My Mathematical Napkin

A Collection of Important Notes

Version 2022-02-28

Contents

1 Metamathematics

§1.1 Introducing a Formal Metamathematical System

Similar to a language, in the study of metamathematics we must first identify the various symbols and grammar rules that we will be operating on. In our study of metamathematics, we are interested in understanding how to manipulate these symbols in a formal manner and outside of any context or interpretation.

Definition 1.1.1 A symbol is a **formal symbol** of the metamathematical language if it is an occurrence of any of the following:

- A propositional connective, namely: $\rightarrow$ (implies), $\wedge$ (and), $\vee$ (or), $\neg$ (not).
- A quantifier, namely: $\forall$ (for all), $\exists$ (there exists).
- $=$(equals)
- $+$ (addition), $\cdot$ (multiplication), $'$ (successor i.e., if $n \in \mathbb{N}, n' = n + 1$)
- 0 (zero)
- $a, b, c, \ldots$ (variables)
- (and) (parentheses).

Definition 1.1.2 A **formal expression,** or simply expression is constructed from a finite sequence of occurrences of formal symbols

Example 1.1.3 The following are examples of formal expressions:

$$a, a + 0, +0()$$

The metamathematical system also allows us to view formal expressions as strings that can be combined with each other by appending one to the other. This operation is called **concatenation.**

For example, we can concatenate the expressions $a + b$ and $= 0$ to produce the new expression: $a + b = 0$

Of course, some formal expressions, while valid, are still meaningless without the introduction of formation rules. In the usual, informal mathematics, for example, $+0()$ is nonsensical. To that end, we introduce the following definitions. These are equivalent to defining what is a grammatical correct English sentence.

Definition 1.1.4 A **term** in the formal system represents the natural numbers (fixed or represented), specifically defined by the following inductive definition.

1. 0 is a term.
2. A variable is a term.
3. If s and t are terms, then $(s) + (t)$ is a term
4. If s and t are terms, then $(s) \cdot (t)$ is a term
5. If s is a term, then s' is a term.
6. The only terms are those given by these rules.

Definition 1.1.5 A **formula** (or **well-formed formula)** is defined by the following inductive definition:

1. If s and t are terms, then $(s) = (t)$ is a formula.
2. If A and B are formulas, then $A \to B$ is a formula.
3. If A and B are formulas, then $A \wedge B$ is a formula.
4. If A and B are formulas, then $A \vee B$ is a formula.
5. If A is a formula, then $\neg A$ is a formula.
6. If x is a variable and A is a formula, then $\forall x(A)$ is a formula.
7. If x is a variable and A is a formula, then $\exists x(A)$ are formulas.
8. The only formulas are those given by these rules.

While we have defined terms and formulas with parentheses enclosing the operands, we will choose to omit these for the sake of readability, unless omission introduces ambiguity. Additionally, for the sake of brevity, we introduce the following abbreviation rules:

$a \neq b$ is an abbreviation for $\neg(a = b)$
$s < t$ is an abbreviation for $\exists x(x' + s = t)$, where x is a variable and s and t are terms not containing x.

Aside from concatenation, we also have another operation on a term in our formal system, which we introduce below. But first, we need to characterize our variables based on where they are in a formula.

Definition 1.1.6 An occurrence of a variable x in a formula A is **bound** if the occurrence is in the scope of a quantifier $\forall x$ or $\exists x$ or is in a quantifier. Otherwise, x is **free.** Binding pertains to the innermost quantifier in the formula.

In terms of interpretation, an expression containing a free variable represents a quantity or proposition dependent on the value of the variable. Otherwise, if the expression contains a bound variable, the expression represents the result of an operation performed over the range of the variable.

Definition 1.1.7 The **substitution** of a term t for a variable x in a term or formula A consists of replacing simultaneously each free occurrence of x by an occuernce in t.

More formally, if we denote $A(x)$ as the term A with x as a free variable (not necessarily in A), then $A(t)$ is the substitution operation and for A_i which are (possibly empty) parts not containing x

$$A(x) = A_0 x A_1 x \dots x A_n$$
$$A(t) = A_0 t A_1 t \dots t A_n$$

The meaning of a formula is preserved when substitution is performed on a free variable. More specifically, this occurs when we substitute for x, the term t, in the formula $A(x)$ where no free occurrence of x occurs in a quantifier bound by a variable of t. In such a case, t is **free at the free occurrences of** x.

Example 1.1.8 Let t be the term $a + b$. Then substitution for x is valid for the first formula, but not the second

$$\forall c(a' + x') = c'$$
$$\forall b(a' + x') = c'$$

Aside from the different symbols and formulae, we introduce a series of postulates for our formal system. These serve as the assumptions within our formal system that we take as true without question.

Axiomatic System 1.1.9

For Postulates 1-8, A, B, C are formulae.
For Postulates 9-13 x is a variable, $A(x)$ is a formla C is a formula which does not contain x free, and t is a term which is free for x in $A(x)$

Postulates for the propositional calculus

Postulate 1a: $A \to (B \to A)$
Postulate 1b: $(A \to B) \to \Big(\big(A \to (B \to C)\big) \to (A \to C)\Big)$
Postulate 2: $A, A \to B \quad \therefore B$
Postulate 3: $A \to (B \to (A \wedge B))$
Postulate 4a: $(A \wedge B) \to A$
Postulate 4b: $(A \wedge B) \to B$
Postulate 5a: $A \to (A \vee B)$
Postulate 5b: $B \to (A \vee B)$
Postulate 6: $(A \to C) \to \Big((B \to C) \to \big((A \vee B) \to C\big)\Big)$
Postulate 7: $(A \to B) \to ((A \to \neg B) \to \neg A)$
Postulate 8: $(\neg\neg A) \to A$

Additional Postulates for the predicate calculus

Postulate 9: $C \to A(x) \quad \therefore C \to \forall x A(x)$
Postulate 10: $\forall x A(x) \to A(t)$
Postulate 11: $\exists x A(x) \to A(t)$
Postulate 12: $A(x) \to C \quad \therefore \exists x A(x) \to C$

Additional Postulates for Number Theory

Postulate 13: $\Big(A(0) \wedge \forall x\big(A(x) \to A(x')\big)\Big) \to A(x)$
Postulate 14: $a' = b' \to a = b$
Postulate 15: $\neg a' = 0$
Postulate 16: $(a = b) \to \big((a = c) \to (b = c)\big)$
Postulate 17: $(a = b) \to (a' = b')$
Postulate 18: $a + 0 = a$
Postulate 19: $a + b' = (a + b)'$
Postulate 20: $a \cdot 0 = 0$

Postulate 21: $a \cdot b' = a \cdot b + a$

These postulates serve as a template for various axioms.

Definition 1.1.10 A formula is an **axiom** if it is one of the forms 1a, 1b, 3—8,10, 11, 13 or if it is of the form 14—21.

Postulates 2, 9, and 12 are **rules of inference,** and give a notion of immediate consequence within our formal system. Namely, for these postulates the last statement is a **conclusion** and the preceding statements are **premises.**

Axioms combined with rules of inference are used to construct proofs, which we also formalize below.

Definition 1.1.11 A formula is **provable** as defined inductively below:

1. If D is an axiom, then D is provable.
2. If E is provable, and D is an immediate consequence of E, then D is provable.
3. If E and F are provable, and D is an immediate consequence of E and F, then D is provable.
4. A formula is provable only as required by 1—3.

Definition 1.1.12 A **formal proof** is a finite sequence of one or more occurrences of formulas such that each formula of the sequence is either an axiom or an immediate consequence of preceding formulas of the sequence. It is said to be the proof of the last formula in the sequence.

Example 1.1.13 The following is an example of a proof within the formal system:

Prove: $(A \to A)$

1. $A \to (A \to A)$ By Postulate 1a.
2. $\big(A \to (A \to A)\big) \to \Big(\big(A \to \big((A \to A) \to A\big)\big) \to (A \to A)\Big)$ By Postulate 1b.
3. $\Big(\big(A \to \big((A \to A) \to A\big)\big) \to (A \to A)\Big)$ By Postulate 2, 1, 2
4. $\big(A \to \big((A \to A) \to A\big)\big)$ By Postulate 1a.
5. $(A \to A)$ By Postulate 2, 3, 4

■

The proof above showcases the rigor provided by our formal system. Each line in the proof is justified based on already established axioms and rules of inference.

§1.2 Formalizing Deduction

Having formally described the metamathematical language, we now seek to apply it to prove various theorems. In theory, we would use only axioms and rules of inference for our proofs,

however in practice, and indeed in informal mathematics, we often abbreviate. The simplest form of abbreviation is through the use of **derived theorems,** those which follow directly from the application of axioms and rules of inference. Reasoning in this manner is referred to as **direct deduction** Of course, some proof techniques such as proof by contradiction require that we set up assumptions of our own outside of the given axiomatic system. Reasoning in this manner is called **subsidiary deduction.**

We now seek to generalize our definition of proofs to apply to deductions as well.

Definition 1.2.1 Given a list $D_1, \dots, D_l$, $l \geq 0$, of occurrences of formulas, referred to as **assumption formulas,** a finite sequence of one or more occurrences of the formulas is called a **formal deduction** if each formula in the sequence is either one of the assumption formulas, or an axiom, or an immediate consequence of preceding formulas in the sequence. It is said to be a **deduction** of the last formula in the sequence.

Abuse of Notation 1.2.2 If we wish to emphasize that a certain variable x or a certain set of variables, $\{x_1, \dots, x_n\}$ occurs in our finite sequence of assumption formulas, we use the notation $\Gamma(x)$ or $\Theta(x_1, \dots, x_n)$, as needed.

Definition 1.2.3 Let $D_1, \dots, D_l, l \geq 0$ be a list of assumption formulas and E be the last formula of some formal deduction under the assumption formulas. Then, E is **deducible** from the assumption formulas, and is referred to as the **conclusion** of the deduction. In symbolic form this is written as:

$$D_1, \dots, D_l \vdash E$$

Abuse of Notation 1.2.4 For chains of deductions, we may write $A \vdash B \vdash C$, to mean $A \vdash B$ and $B \vdash C$.

These definitions allow for the use of any assumption formulas outside of the given postulates in our Axiomatic System[1].

Example 1.2.5 The following is an example of a deduction. Our desired conclusion is C

1.	A	Assumption Formula 1
2.	B	Assumption Formula 2
3.	$(A \wedge B) \rightarrow C$	Assumption Formula 3
4.	$A \rightarrow (B \rightarrow (A \wedge B))$	Postulate 3
5.	$B \rightarrow (A \wedge B)$	Postulate 2, 1, 4
6.	$A \wedge B$	Postulate 2, 2, 5
7.	C	Postulate 2, 3, 6

■

Notice that at each step of the deduction, we write what a brief explanation as to why the formula follows. We refer to such an explanation as an **analysis** of the deduction. This

[1] See 1.1.9

example also serves to highlight the subtle difference between a proof and a deduction, namely deductions allow for assumption formulae to be a part of the sequence of formulae.

In the above example, we proved that C follows from the assumption formulas. In line with the notation introduced in Definition 3.2., we may write our conclusion as:

$$A, B, (A \wedge B) \rightarrow C \vdash C$$

We now seek to characterize deduction as a sequence. The following shows some of these properties.

Proposition 1.2.6. Given lists of assumption formulas Γ, Δ, assumption formulas C and D, and conclusion E

i. $E \vdash E$
ii. If $\Gamma \vdash E$, then E is in the list Γ
iii. If $\Gamma \vdash E$, then $\Delta, \Gamma \vdash E$
(Extraneous assumptions do not affect the conclusion if it is deducible).
iv. If $\Delta, C, D, \Gamma \vdash E$, then $\Delta, D, C, \Gamma \vdash E$
(The order of assumptions does not affect the conclusion if it is deducible).
v. If $\Delta \vdash C$, and $C, \Gamma \vdash E$, then $\Delta, \Gamma \vdash E$
(Assumptions which are derived from previous assumptions can be rederived in the deduction as needed without affecting the conclusion).

An important result within Metamathematics is the following Theorem. It allows us to verify that abbreviating proofs is, indeed, valid.

Theorem 1.2.7. **(The Deduction Theorem for Propositional Calculus)**
For the propositional calculus, if $\Gamma, A \vdash B$, then $\Gamma \vdash (A \rightarrow B)$

In other words, if B is deducible from $\Gamma \cup \{A\}$, then there exists a deduction using Γ where the final element in the sequence is $A \rightarrow B$.

Idea of the Proof:
Show the following is true by strong induction:
$P(\Gamma, A, k)$*: For every formula* B*, if there is a deduction of* B *from* Γ, A *of length* k*, then there can be found a deduction of* $A \rightarrow B$ *from* Γ

Consider the following base cases and show that $A \rightarrow B$ follows from Γ:

a. B is one of the formulas of Γ
b. B is A.
c. B is an axiom.

In addition to the above cases, for the inductive case, consider when B is the consequence of two preceding formulas in the deduction applying Postulate 2. Namely, there exists P and $P \rightarrow B \in \Gamma$.

■

If we apply the Deduction Theorem to the metamathematical statement $\Gamma, A \vdash B$ to obtain $\Gamma \vdash (A \to B)$, we say that we **discharge** A. The resulting metamathematical statement is referred to as a direct type since we only apply axioms and rules of inference on our assumptions to arrive at the conclusion.

Earlier, we introduced the notion of a subsidiary deduction. We formalize such a deduction through the definition below

Definition 1.2.8 A **subsidiary deduction rule** is a metamathematical theorem which has one or more hypotheses of the form $\Delta_i \vdash E_i$ and a conclusion of the form $\Delta \vdash E$. Each of the $\Delta_i \vdash E_i$ are **subsidiary deductions**, and the conclusion is the **resulting deduction.**

Example 1.2.9 The following is an example of a subsidiary deduction rule:
If $\Gamma, A \vdash C$ and $\Gamma, B \vdash C$, then $\Gamma, A \vee B \vdash C$.

$\Gamma, A \vdash C$ and $\Gamma, B \vdash C$ are the subsidiary deductions, and $\Gamma, A \vee B \vdash C$ is the resulting deduction.

We may note that the Deduction Theorem has only been stated for the Propositional Calculus. Indeed, this is because the Predicate Calculus introduces additional rules of inference, which may affect the deductions that we formulate. However, it turns out we can extend the theorem to accommodate these formal systems if we consider additional cases in our proof.

Definition 1.2.10 Given a deduction specified as a sequence of formulae $A_1, \dots, A_k$ with assumption formulas $D_1, \dots, D_l$, we say that A_i **depends** on D_j if and only if one of the following holds:[1]

1. A_i is an occurrence of D_j (informally, D_j is dependent on itself).
2. A_i is an immediate consequence of A_{i_1} and A_{i_2} which depend on D_j (informally, formulae that were derived from D_j are dependent on D_j).

Definition 1.2.11 A variable y is **varied** in a given deduction with a given analysis for a given assumption formula D_i if (1) y occurs free in D_i, and (2) The deduction contains an application of Postulate 9 or 12 with respect to y to a formula depending on D_i. Otherwise, we say y is held **constant.**

Theorem 1.2.12. **(The Deduction Theorem for the Predicate Calculus and the Full Number Theoretic Formal System)**
If $\Gamma, A \vdash B$, with the free variables held constant for the last assumption formula A, then $\Gamma \vdash (A \to B)$

Idea of the Proof:

[1] For the Predicate Calculus, it is helpful to remember that Postulates 9 and 12 are only dependent on premises of the form $C \to A(x)$. This means that as long as that premise is not derived from an assumption formula, Postulates 9 and 12 are dependent on no assumption formula.

The proof is similar to 1.2.7 except we consider the following as additional cases and show by induction that the theorem holds:

a. B is the immediate consequence of a preceding formula by the application of Rule 9 of the form $C \to A(x)$, where C does not contain x free, and B is $C \to \forall x A(x)$. Then:
   i. $C \to A(x)$ does not depend on A.[1]
   ii. $C \to A(x)$ depends on A.
b. B is the immediate consequence of a preceding formula by the application of Rule 12 of the form $A(x) \to C$, where C does not contain x free, and B is $\exists x A(x) \to C$. Then:
   i. $A(x) \to C$ does not depend on A.
   ii. $A(x) \to C$ depends on A.

§1.3 Introducing and Eliminating Logical Symbols

In §1.2 we formalized the notion of a deduction and arrived at the Deduction Theorems--1.2.7 and 1.2.12. In this section we introduce rules that, coupled with the Deduction Theorem, will let us prove theorems in a more succinct manner without needing to worry about the validity of these proofs.

Theorem 1.3.1 Let A, B, C or $x, A(x)$, C, and t be subject to the corresponding stipulations in the Postulates of Axiomatic System 1.1.9. Additionally, let Γ denote a list of assumption formulae.

	Introduction	Elimination
Implication	If $\Gamma, A \vdash B$, then $\Gamma \vdash (A \to B)$ **(Deduction Theorem)**	$A, A \to B \vdash B$ **(Modus Ponens)**
Conjunction	$A, B \vdash A \wedge B$	$A \wedge B \vdash A$ $A \wedge B \vdash B$
Disjunction	$A \vdash A \vee B$ $B \vdash A \vee B$	If $\Gamma, A \vdash C$ and $\Gamma, B \vdash C$, then $\Gamma, A \vee B \vdash C$ **(Proof By Cases)**
Negation	If $\Gamma, A \vdash B$, and $\Gamma, A \vdash \neg B$, then $\Gamma \to \neg A$ **(Proof by Contradiction)** [2]	$\neg\neg A \vdash A$ **(Discharge of Double Negation)**
Generality	$A(x) \vdash^{x} \forall x A(x)$	$\forall x A(x) \vdash A(t)$
Existence	$A(t) \vdash \exists x A(x)$[3]	If $\Gamma(x), A(x) \vdash C$, then $\Gamma(x), \exists x A(x) \vdash^{x} C$

Proof:
Apply the Deduction Theorem as well as the corresponding Postulates listed in 1.1.9. Most of the Postulates (such as Postulate 8) directly correspond to a rule listed in 1.3.1.

[1] The following observation may help: A given variable is always held constant for each assumption formula in which it does not occur free.
[2] Also called Reductio ad Absurdum
[3] Note that $A(t)$ really denotes the result of replacing every free occurrence of x in $A(x)$ with t.

■

An additional rule can be derived if we apply Generality Introduction and then Generality Elimination in succession, namely if x is a variable, $A(x)$ a formula and t a term which is free for x, then

$$A(x) \vdash^{x} A(t)$$

We can also derive an additional rule that allows a change of variables for generality introduction and existence elimination given by the following:

Corollary 1.3.2

i. **Strong Generality Introduction** $A(b) \vdash^{b} \forall x A(x)$
ii. **Strong Existential Elimination** If $\Gamma(b), A(b) \vdash C$, then $\Gamma(b), \exists x A(x) \vdash^{b} C$

Idea of the Proof: The above statements only require us to modify the proof for 1.3.1. Instead of using our Postulates, we instead use the deduction: $C \to A(b) \vdash^{b} C \to \forall x A(x)$

§1.4 Dependence and Variation

In §1.2 we introduced the notion of variables that depend on other variables, and variables that may vary or be held constant. This section aims to provide additional rigor to our metamathematical system by introducing facts about dependencies and variations introduced in our deductions.

Proposition 1.4.1 In the subsidiary deduction rules of 1.3.1, if the conclusion depends on a given assumption formula in the resulting deduction, then the conclusion depends on the same assumption formula in the given deduction.

Proof: We show the contrapositive, if the conclusion does not depend on some chosen assumption formula in the given deduction, we can then introduce the assumption formula by 1.2.6 iii. In such a case, the subsidiary deduction in the resulting deduction also does not depend on the chosen assumption formula.

■

Proposition 1.4.2 In the subsidiary deduction rules of 1.3.1 with the exception of Existence Elimination, if a variable is varied in the resulting deduction for a given assumption formula, then the variable is varied in the same assumption formula in the given deduction.

For Existential Elimination, the x is varied in $\Gamma(x), \exists x A(x) \vdash^{x} C$ only for those deductions in $\Gamma(x)$ which contain x free and on which the C depends in the given deduction $\Gamma(x), A(x) \vdash C$.

Proof: It suffices to show that the proposition holds for the Deduction Theorem. To show this we simply examine the cases we needed to show for the proof of the Deduction Theorem. If the resulting deduction, in this case $C \to A(x)$ depends on $A(x)$, then x is not varied since it is not free. Otherwise, $C \to A(x)$ does not depend on $A(x)$, and therefore if x is varied in the

conclusion derived by applying Postulate 1, then so will the x in $C \to A(x)$, and so will the x in $A(x)$ since C does not contain x free.

The special case is when we consider existential elimination. If we consider the proof of existential elimination, we see that we can eliminate any assumption formula (by 1.2.6 iii) that the conclusion does not depend on and where x is varied similar to 1.4.1[1].

■

Intuitively speaking, Propositions 1.4.1 and 1.4.2 are saying that the dependence of a formula to an assumption formula, and the variation of a variable in an assumption formula is preserved when we apply our subsidiary deduction rules.

§1.5 The Propositional Calculus

In this section we investigate the Propositional Calculus, specifically that which can be derived from Postulates 1—8 in 1.1.9. In this context we restrict our definition of formula to only allow for →, ¬, ∧ and ∨ as our operators. We will also refer to the formulae within this narrowed context as **propositional letter formulae.**

We introduce the following theorem formalizing the notion of substitution within the Propositional Calculus specifically.

Theorem 1.5.1 Let Γ be propositional letter formulae and E be a propositional formula in the distinct propositional letters $P_1, \dots, P_n$. Let $A_1, \dots, A_n$ be formulas. Let Γ^* and E^* be the result of substituting $A_1, \dots, A_n$ for $P_1, \dots, P_n$ in Γ and E respectively. Then $\Gamma^* \vdash E^*$ if and only if $\Gamma \vdash$ E.

In brief, what the theorem tells us is that deducibility is preserved under substitution from formulae to propositional letters and vice versa. The result should make intuitive sense, but we seek to prove that this is indeed the case.

Idea of the Proof: First we show that if $\Gamma \vdash E$ then $\Gamma^* \vdash E^*$. We show that applying the substitution to each of the assumption formulae, as well as any additional formulae within the deduction does not change our analysis in the resulting deduction.

To show that $\Gamma^* \vdash E^*$ implies $\Gamma \vdash E$, we apply similar reasoning. Within each formula in the deduction, it may be possible to extract components we refer to as prime (i..e, those not connected by the propositional connectives). We substitute propositional letters for each of these prime formulae, and such a substitution would not change the analysis.

■

[1] In brief, the idea for this proof is as follows:

(1)	$\Gamma(x), A(x) \vdash C$	Hypothesis
(2)	$\exists x A(x), \exists x A(x) \to C \vdash C$	Modus Ponens
(3)	$\Gamma(x) \vdash A(x) \to C \vdash^x \exists x A(x) \to C$	Deduction Theorem, Postulate 12
(4)	$\Gamma(x), \exists x A(x) \to C$	2, 3 by 1.2.6 v.

In addition to the operators mentioned before, we introduce a new operator for equivalence, shown in the definition below

Definition 1.5.2 If A and B are formulas, then $A \leftrightarrow B$ abbreviates $(A \to B) \wedge (B \to A)$. We say A and B are **equivalent formulas.**

Similar to what we have done in 1.3.1, we can establish additional rules that apply within our propositional calculus. The following Theorem serves to catalog these new rules.

Theorem 1.5.3 Let A, B and C be formulae, we then have

1	Principle of Identity	$\vdash A \to A$
2	Chain Inference	$A \to B, B \to C \vdash A \to C$
3	Interchange of Premises	$A \to (B \to C) \vdash B \to (A \to C)$
4	Importation	$A \to (B \to C) \vdash (A \wedge B) \to C$
5	Exportation	$(A \wedge B) \to C \vdash A \to (B \to C)$
6	Introduction of conclusion	$A \to B \vdash (B \to C) \to (A \to C)$
7	Introduction of premise	$A \to B \vdash (C \to A) \to (C \to B)$
8a	Introduction of a conjunctive member	$A \to B \vdash (A \wedge C) \to (B \wedge C)$
8b		$A \to B \vdash (C \wedge A) \to (C \wedge B)$
9a	Introduction of a disjunctive member	$A \to B \vdash (A \vee C) \to (B \vee C)$
9b		$A \to B \vdash (C \vee A) \to (C \vee B)$
10a	Refutation of the premise	$\neg A \vdash A \to B$
10b		$A \vdash \neg A \to B$
11	Proving the conclusion	$B \vdash A \to B$
12	Contraposition	$A \to B \vdash \neg B \to \neg A$
13		$A \to \neg B \vdash B \to \neg A$
14	Contraposition with Negation Suppressed[1]	$\neg A \to B \vdash \neg B \to A$
15		$\neg A \to \neg B \vdash B \to A$
16	Basic Equivalence	$A \to B, B \to A \vdash A \leftrightarrow B$
17a		$A \leftrightarrow B \vdash A \to B$
17b		$A \leftrightarrow B \vdash B \to A$
18a		$A \leftrightarrow B, A \vdash B$
18b		$A \leftrightarrow B, B \vdash A$
19	Reflexivity of Equivalence	$\vdash A \leftrightarrow A$
20	Symmetry of Equivalence	$A \leftrightarrow B \vdash B \leftrightarrow A$
21	Transitivity of Equivalence	$A \leftrightarrow B, B \leftrightarrow C \vdash A \leftrightarrow C$
22	Intuitionistic Results	$A \to (B \to C), \neg\neg A, \neg\neg B \vdash \neg\neg C$
23		$\neg\neg(A \to B) \vdash \neg\neg A \to \neg\neg B$
24		$\neg\neg(A \to B), \neg\neg(B \to C) \vdash \neg\neg(A \to C)$
25a		$\vdash \neg\neg(A \wedge B) \leftrightarrow \neg\neg A \wedge \neg\neg B$
25b		$\vdash \neg\neg(A \leftrightarrow B) \leftrightarrow \neg\neg(A \to B) \wedge \neg\neg(B \to A)$

[1] Applies to the intuitionist system

Idea of the Proof: We simply use the derived rules and the postulates from 1.1.9 and 1.3.1 to show a derivation.

■

2 Set Theory

§2.1 The Set

The mathematical object that is the central focus of Set Theory is of course the set. This section introduces different definitions that are relevant within Set Theory.

Definition 2.1.1 A **set** is defined as a collection of objects called the **elements** of the set. If x is a member of X, then we denote it as $x \in X$

We can specify what elements are members of a set through different methods. We can manually list each element (i.e., $A = \{Alice, Bob\}$, or we may wish to give an explicit rule for membership in the set (i.e., $B = \{x | x \in \mathbb{R}, x \geq 1\}$). We will not be selective in what method we use to specify the elements of the sets we are studying.

Unless otherwise stated, we will treat sets as collections of distinct elements.

Sets are inherently recursive structures, which is apparent in the following definition.

Definition 2.1.2 A set A is a **subset** of B, denoted $A \subseteq B$, if all elements of A are also elements of B. More symbolically:

$$x \in A \rightarrow x \in B$$

Likewise, we say that B is a **superset** of A, denoted $B \supseteq A$.

Of course, by this definition, we can see that for any set X, $X \subseteq X$. The following definitions seeks to distinguish trivial from non-trivial subsets.

Definition 2.1.3 Sets A and B are **equal,** denoted $A = B$, if and only if $A \subseteq B$ and $B \subseteq A$. Otherwise, they are unequal, denoted $A \neq B$.

Definition 2.1.4 A set A is a **proper subset** of B, denoted $A \subset B$, if $A \subseteq B$ and $A \neq B$.[1]

Our definition of $A = B$ requires that all elements of B are also elements of A and vice versa. However, we may also wish to note another way in which the elements of two sets can be related. This is given by the definition below.

Definition 2.1.5 Sets A and B are **equivalent,** denoted $A \sim B$, if there exists a bijective mapping that maps each element of A to an element of B.

Finally, we introduce special sets that are the extremal cases in terms of the number of elements they contain.

[1] Some authors prefer to use $\subset$ to denote subsets, proper or not. We choose not to do this to avoid ambiguity.

Definition 2.1.6 The **null set (or empty set)** is the set containing no elements. It is denoted as $\emptyset$.

Definition 2.1.7 The **universal set**[1] is the set containing all elements, including itself. It is denoted as U.

§2.2 Operations of Set Algebra

We now introduce some familiar operations on sets.

Definition 2.2.1 The **union** of two sets A and B, denoted as $A \cup B$ is the set
$$\{x | x \in A \; or \; x \in B\}$$
If we are dealing with a sequence of sets, $A_1, \ldots, A_n$, we denote their union using this operation:
$$\bigcup_{i=1}^{n} A_i$$

Definition 2.2.2 The **intersection** of two sets A and B, denoted as $A \cap B$ is the set
$$\{x | x \in A \; and \; x \in B\}$$
If we are dealing with a sequence of sets, $A_1, \ldots, A_n$, we denote their intersection using this operation:
$$\bigcap_{i=1}^{n} A_i$$

Definition 2.2.3 The **complement**[2] of the set A, denoted A^c is defined as
$$\{x | x \notin A\}$$

Definition 2.2.4 The **difference**[3] of the set A and B, denoted $A - B$ is defined as
$$\{x | x \in A \; and \; x \notin B\}$$

Notice that if we allow for a universal set U, we can express the complement as
$$A^c = U - A$$

We may also wish to note that there is a natural correspondence between the set operations and the typical logical operators. Intersection corresponds with conjunction. Union corresponds to disjunction. And complement corresponds to negation. The correspondence should be immediately apparent if we investigate how we have defined each set operation.

---

[1] It is interesting to note that not all variations of Set Theory do not allow the formulation of the Universal Set as it can give rise to various paradoxes. We choose to include the notion of a universal set here anyway should it be useful to identify such a concept within a certain context (i.e., probability).

[2] Other commonly used notations are A' and $\bar{A}$

[3] Another commonly used notation is $A \backslash B$

We now present some fundamental properties that can be found within Set Algebra.

Proposition 2.2.5 (**Properties of Set Operations**)

Commutativity	$A \cup B = B \cup A$ $A \cap B = B \cap A$
Associativity	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$
Distributivity	$A \cup (B \cap C) = (A \cup B) \cap (B \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (B \cap C)$
Identity	$A \cup \emptyset = A$ $A \cap U = A$
Complement	$A \cup A^c = U$ $A \cap A^c = \emptyset$
Idempotent	$A \cup A = A$ $A \cap A = A$
Domination	$A \cup U = U$ $A \cap \emptyset = \emptyset$
Absorption	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$
De Morgan' Law	$(A \cup B)^c = A^c \cap B^c$ $(A \cap B)^c = A^c \cup B^c$
Involution	$A^{cc} = A$
Complement Laws for Universe and Empty Set	$\emptyset^C = U$ $U^c = \emptyset$

Idea of the Proof: The proof follows immediately from the properties of the logical operators corresponding to each set operator.[1]

■

We can also give properties related to the difference operator

Proposition 2.2.6 (**Properties of Differences of Sets**) Let $A, B, C \subseteq U$. The following identities hold:

i. $C - (A \cap B) = (C - A) \cup (C - B)$
ii. $C - (A \cup B) = (C - A) \cap (C - B)$
iii. $C - (B - A) = (A \cap C) \cup (C - B)$
iv. $(B - A) \cap C = (B \cap C) - A = B \cap (C - A)$
v. $(B - A) \cup C = (B \cup C) - (A - C)$
vi. $(B - A) - C = B - (A \cup C)$
vii. $A - A = \emptyset$

[1] Alternatively, we can treat these properties as Fundamental and not require a proof completely. Whether the reader wishes to do so is up to them.

viii. $\emptyset - A = \emptyset$
ix. $A - \emptyset = A$
x. $B - A = A^c \cap B$
xi. $(B - A)^c = A \cup B^c$
xii. $U - A = A^c$
xiii. $A - U = \emptyset$

Idea of the Proof: We can observe that (x) can be derived directly from the definition of the difference operation. The rest of the statements can be proven by substituting (x) for $B - A$. ■

§2.3 Relations

Another common theme within Mathematics is the use of mappings, typically from one domain of discourse to another. For example, functions typically map a domain to a corresponding codomain. Of course, functions are simply one type of mathematical object known as a relation, which we define in this section.

First, we introduce an operator that can be used to create tuples from elements of sets.

Definition 2.3.1 Let A and B be sets. Then the **Cartesian Product** of A and B, written as $A \times B$ is defined as the set of all ordered pairs formed from elements of A and B. In set-builder notation, it can be elaborated as:

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

We can, of course, chain multiple Cartesian Products together, which may be written as:

$$A_1 \times A_2 \times \ldots \times A_n$$

An element of this set is what we will refer to as an **ordered n-tuple.**

Additionally, if we are simply dealing with a single set (i.e., $A \times A$), we may abbreviate the notation as A^2 (or A^n for n-fold Cartesian products).

We are now ready to define a relation.

Definition 2.3.2 Let A and B be sets. Then a **relation** R between A and B is a subset of $A \times B$. If two objects are in a relation, we may denote it as $(a, b) \in R$, which we read as a is R-related to b. It may also be denoted as aRb.

Note that in a relation, the order of the elements within the tuple is important.[1]

§2.4 Equivalence Relations

[1] Unless the relation is symmetric.

The notion of equivalence was touched on in 2.1.5. In Mathematics, this relation is powerful as it allows us to talk about representatives of classes within a particular domain of discourse. For example, within Number Theory, we may speak of numbers that are odd and even (i.e., 0 or 1 modulo 2), and in operations and proofs concerning parity, we may simply choose to use one representative for each parity.

We provide the following definitions:

Definition 2.4.1 An **equivalence relation** is a relation R on the set X such that the following properties are true $\forall x, y, z \in X$

i. **Reflexivity:** $(x, x) \in R$
ii. **Symmetry:** $(x, y) \in R$ if and only if $(y, x) \in R$
iii. **Transitivity:** $(x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R$.

Definition 2.4.2 An **equivalence class** of a with respect to an equivalence relation R on the set X is a set A such that $A = \{x \in X | (x, a) \in R\}$.

§2.5 Cardinality and Counting

In our study of sets, it may also be important to establish a measure for how many elements are there in a set. We introduce this through the cardinality of the set, defined below:

Definition 2.5.1 The **cardinality** of a set A, denoted $|A|$ refers to the number of elements of the set.

Of course, as is apparent with the set of all natural numbers, we may deal with finite or infinitely many elements in each set. While we could assign the "number" ∞ to be the cardinality for all infinite sets, it has been shown that there are different levels of infinities.

Theorem 2.5.2 There are more Real Numbers than there are Natural Numbers

We hold off the proof of this theorem for now in favor of being more specific with what we mean when we say that two sets have the same cardinality or size.

Definition 2.5.3 (**Order Relation of Cardinalities)** Let A and B be sets. We say that

i. $|A| = |B|$ if and only if there exists a bijection $f: A \rightarrow B$.
ii. $|A| < |B|$ if there exists an injective function and no bijective function $f: A \rightarrow B$
iii. $|A| > |B|$ if there exists an injective function and no bijective function $f: B \rightarrow A$

The notion of cardinality allows us to establish a notion of counting (in the typical sense that we would count objects). When we count the number of elements of A, we are actually mapping each element to a distinct natural number. We have made mention of finite and infinite sets, and we now define these as well.

Definition 2.5.4 A **finite set** is a set which has a bijective mapping to the set of natural numbers $\{1,2,\dots,n\}, n \in \mathbb{N}$. Otherwise, we say that the set is **infinite**. A **countably infinite**[1] set is a set which has a bijective mapping with the natural numbers. Otherwise, the set is **uncountably infinite**.

Our definition of finite and infinite sets allows us to discuss some seemingly peculiar examples.

Proposition 2.5.5 There are as many even numbers as there are natural numbers.

Proof: Indeed for $n \in \mathbb{N}$, $n \mapsto 2n$ is a valid bijective mapping since each natural number is mapped to an even natural number, and each even number is mapped to n.

■

2.5.5 holds despite the fact the set of even numbers is clearly a subset of the set of natural numbers.

We now present a proof to 2.5.2, which we will restate below using the ordering of cardinalities.

Theorem 2.5.2 $|\mathbb{N}| < |\mathbb{R}|$.

Proof: The proof is due to Cantor's diagonalization argument. Consider a finite list of real numbers, and for simplicity, we suppose these numbers are between 0 and 1, and that the only digits are 0 and 1.

List the numbers in some order. The following illustration should help

$$1 \mapsto 0.010001 \dots 11010$$
$$2 \mapsto 0.101000 \dots 00101$$
$$3 \mapsto 0.011101 \dots 01111$$
$$\vdots$$

Suppose by this point we claim that all the real numbers between 0 and 1 have been created, then we construct a new real number by considering the i^{th} item in the list and taking the i^{th} decimal place and changing it to the other digit (so that 0 becomes 1 and vice versa). In the example above we may get

$$0.110\cdots$$

Furthermore, since this item is different to each of the other items in the list by at least one decimal point (as stated in how we defined its construction), then this item is a new real number not on the list, contradicting our assumption that the list was exhaustive.

■

Given our definition of what it means for two sets to be the same size, we give the following important theorem.

[1] Also called enumerable.

Theorem 2.5.6 **(Schroder-Bernstein Theorem)** Let X and Y be sets. If there exist injective mappings $f: X \to Y$ and $g: Y \to X$, then there exists a bijective mapping $h: X \to Y$.

Idea of the Proof 1:

i. Consider $A_1 = X - g(Y)$, and the inductive definition $A_n = g \circ f(A_{n-1})$. Show that the sequence $A_1, \dots, A_n$ is pairwise disjoint.
ii. Do the same for $f(A_n)$ for all $n \in \mathbb{N}$. The argument is similar to i.
iii. Define $A = \bigcup_{n=1}^{\infty} A_n$ and $B = \bigcup_{n}^{\infty} f(A_n)$. Show that $f: A \to B$ is bijective.
iv. Define $A' = X - A$ and $B' = Y - B$ (refer to iii). Show that $g: B' \to A'$ is bijective.
v. Finish the proof by constructing a bijective function $h: A \to B$ using the results from iii and iv.

■

Idea of the Proof 2 (Konig's Proof):

i. Consider X and Y to be disjoint sets such that common elements are repeated twice.
ii. Consider the sequence for $x \in X$ and $y \in Y$.

$$\dots, f^{-1}g^{-1}(x), g^{-1}(x), x, f(x), g\big(f(x)\big), \cdots$$

And show that each $x \in X$ and $y \in Y$ appears exactly once in this sequence. Call such a sequence the family of x.
iii. ii implies that it suffices to consider only each family of x and construct a bijective mapping h for that family.
iv. Define h by considering how each element appears in the sequence. Consider these cases in particular,
   a. The sequence in (ii) has an element in X as its endpoint.
   b. The sequence in (ii) has an element in Y as its endpoint.
   c. The sequence in (ii) has the same endpoints. More specifically, repeatedly composing by f and g will lead back to x multiple times.
   d. The sequence in (ii) is infinite.

   The mapping, then, is based on successors and predecessors, whichever is defined.

■

§2.6 Power Sets

The results from 2.5.2 insinuate that there is a hierarchy of "infinities", starting from the natural numbers. Naturally, we may wish to ask if there is an infinity that is above the real numbers. To that end, we introduce sets that are seeded from other sets.

Definition 2.6.1 Given a set A, the **power set** $P(A)$ refers to the collection of all subsets of A.

The power set is a central idea in Cantor's Theorem.

Theorem 2.6.2 **(Cantor's Theorem).** Given a set A, there is no onto mapping from A to $P(A)$.

Proof: We argue by contradiction. Suppose there is a mapping $f: A \to P(A)$. Then each element of $P(A)$ must be mapped to by an element of A. Note that the elements of $P(A)$ are subsets of A.

By construction, consider the set:

$$B = \{a \mid a \notin f(a)\}$$

So that $B \subseteq A$ and $B \in P(A)$. Now, suppose $b \in A$, $f(b) = B$. The contradiction is that b must both be and not be in B. If $b \in B$, then $b \notin f(b)$, then $b \notin f(B)$. If $b \notin f(B)$, then $b \notin f(b)$, and $b \in B$.

■

3 Elementary Functions

This chapter serves to catalog important functions that are relevant in different mathematical theories, and which merit their own section to explore the different properties of these functions.

§3.1 What are functions?

To begin, we formally define what we mean by a function

Definition 3.1.1 A **function** is a mapping between two sets X and Y that associates each element in X to one element in Y. We denote it as $f: X \to Y$.

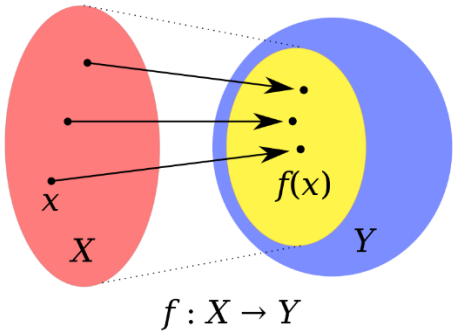


Figure 3.1.1. Illustration of Function. Obtained from https://commons.wikimedia.org/wiki/File:Codomain2.SVG

Definition 3.1.2 Given a function $f: X \to Y$, the set X is referred to as the **domain,** and the set Y is referred to as the **codomain.**

We denote x to be an element of X, and $f(x)$ to be an element of Y such that $x \mapsto f(x)$ (read x maps to $f(x)$).

Definition 3.1.3 Given a function $f: X \to Y$, the **range or image** of f under a subset $A \subseteq X$ is defined as the set $\{f(x) \in Y | x \in A\}$.

We denote the image of f under a subset A as $f(A)$[1]. If the subset only contains a single element x, we say $f(x)$ is the image of x.

Note that by the above definition, the range and the codomain are not necessarily the same. Similarly, we may introduce a corresponding subset for the domain of f

Definition 3.1.4 Given a function $f: X \to Y$, the **pre-image** of f under a subset $B \subseteq Y$ is defined as the set $\{x \in X | f(x) \in B\}$.

[1] An alternative notation to this is $f^{\to}$ However, for the sake of readability, we will prefer the notation specified.

We denote the pre-image of f under a subset B as $f^{-1}(B)$[1]. If the subset only contains a single element x, we say x is the pre-image of $f(x)$.

As an abbreviation, for the function $f: X \to Y$, when we say "the pre-image of a function", we are really saying $f^{-1}(Y)$. Similarly, when we say "the range of a function", we are really saying $f(X)$.

§3.2 Injections, Surjections, and Bijections

We may also wish to classify each function based on the images of every element in the codomain. We present the following set of definitions to introduce this classification.

Definition 3.2.1 A function $f: X \to Y$ is **injective** (is an injection)[2] if every element of the domain is mapped to at most one element in the codomain. Symbolically, it is defined as $\forall x_1, x_2 \in X, f(x_1) = f(x_2) \to x_1 = x_2$.

Definition 3.2.2 A function $f: X \to Y$ is **surjective** (is a surjection)[3] if every element of the codomain is the image of at least one element in the domain. Symbolically, it is defined as $\forall y \in Y, \exists x \in X, f(x) = y$.

Definition 3.2.3 A function $f: X \to Y$ is **bijective** (is a bijection)[4] if it is both injective and surjective. Specifically, every element in the domain is mapped to one and only one element in the codomain.

It should be noted that it is entirely possible for a function to neither be injective nor surjective. For example, consider the function that maps a person to their oldest brother. Certainly, not all people have a brother so the function is not surjective, and certainly the youngest and middle child of a family with three sons are mapped to the same person, so the function is not injective.

§3.3 The Absolute Value Function

The **absolute value function** is a special function, defined as $|x|: \mathbb{R} \to \mathbb{R}$, where

$$|x| = \begin{cases} -x, & x < 0 \\ x, & x \geq 0 \end{cases}$$

Geometrically, the absolute value function represents the unsigned distance between a number x on the real number line, and 0.

---

[1] This is not to be confused with finding the inverse of a function. Indeed, it is not necessarily the case that the function is invertible within the specified set B.

[2] May also be called a one-to-one function

[3] May also be called an onto function

[4] May also be called a one-to-one correspondence.

We now examine some important properties of the absolute value function. For the following, we let $a, b, c \in \mathbb{R}$.

Proposition 3.3.1 $|ab| = |a||b|$.

Proof: This should be apparent if we do an exhaustive proof considering the four cases when a is positive or negative, and b is positive or negative.

■

Proposition 3.3.2 $|a - b| = |b - a|$.

Proof: The intuitive notion of the absolute value representing distance between two numbers should make this trivial. For formality's sake, we can use 3.3.1 and express $|b - a|$ as $|(-1)(a - b)|$

■

Proposition 3.3.3[1] **(Triangle Inequality)** $|a + b| \leq |a| + |b|$.

Proof: We can do an exhaustive proof, considering the four cases when a is positive or negative, and b is positive or negative.

■

Proposition 3.3.4 **(Reverse Triangle Inequality)** $\big||a| - |b|\big| \leq |a - b|$.

Proof: Express $|a|$ and $|b|$ as $|(a - b) + b|$ and $|(b - a) + b|$, respectively, and apply 3.3.2 and the Triangle Inequality to obtain an inequality with an upper and lower bound. Conclude based on the intuitive interpretation of $|a|$ that the proposition holds.

■

Proposition 3.3.5 $|a - b| \leq |a - c| + |c - b|$.

Proof: It follows directly from applying the Triangle Inequality to: $|(a - c) + (c - b)|$

■

[1] As it turns out, this inequality has a geometric interpretation if we imagine $|a + b|$ as the hypotenuse of a right triangle with legs of length $|a|$ and $|b|$. If the triangle is indeed a triangle in Euclidean space, then the Triangle Inequality must be satisfied.

4 Real Analysis

§4.1 Constructing $\mathbb{R}$

In real world applications such as those in the realm of Physics and Engineering, we often deal with quantities whose values span a continuum. In that sense, it no longer suffices to use $\mathbb{N}$, $\mathbb{Z}$, or even $\mathbb{Q}$ as the domain in which to define our values since doing so introduces discontinuities in our supposedly continuous domain. This shall serve as our primary, application-oriented, motivation for introducing a superset of the rationals that can "fill in the gaps" between the rational numbers. Such a set is what we refer to as the set of real numbers or $\mathbb{R}$.

More precisely, when we say we wish to "fill in the gaps" we are really invoking the following axiom[1]:

Axiom 4.1.1 (**Axiom of Completeness**) Every nonempty set of real numbers that is bounded above has a least upper bound.

We can dissect what the Axiom of Completeness is stating by looking at two keywords: bounded and least upper bound. The following definitions are provided.

Definition 4.1.2 A set $A \subseteq \mathbb{R}$ is **bounded above** if there exists a number $b \in \mathbb{R}$ such that $a \leq b$ for all $a \in A$. The number b is called an **upper bound** for A.

Similarly, the set A is **bounded below** if there exists a **lower bound** $l \in \mathbb{R}$ satisfying $l \leq a$ for every $a \in A$.

Definition 4.1.3 A real number s is the **least upper bound (or the supremum)** for a set $A \subseteq \mathbb{R}$ if it meets the following criteria:

i. s is an upper bound for A;
ii. If b is any upper bound for A, then $s \leq b$.

We denote the least upper bound as $s = \sup A$.

Definition 4.1.4 A real number s is the **greatest lower bound (or the infimum)** for a set $A \subseteq \mathbb{R}$ if it meets the following criteria:

i. s is a lower bound for A;
ii. If b is any lower bound for A, then $b \leq s$.

We denote the greatest lower bound as $s = \inf A$.

[1] While we have stated that this is an axiom, in reality it is entirely possible to prove the Axiom of Completeness as a Theorem. The proof is done via construction using Dedekind cuts.

By 4.1.3 and 4.1.4 we can guarantee that the supremum and infimum of a set is unique. Additionally, it should be noted that $\sup A$ and $\inf A$ are not necessarily elements of the set of real numbers A. To that end, we provide additional definition:

Definition 4.1.5 A real number x is a **maximum** of the set A if $a_0 \in A$ and $a_0 \geq a$ for all $a \in A$. Similarly, a_1 is a **minimum** of A if $a_1 \in A$ and $a_1 \leq a$ for all $a \in A$.

Example 4.1.6 Consider the set $A = \{x \in \mathbb{R} | 0 < x < 1\}$. The Axiom of Completeness suggests that we ought to find a least upper bound for A. Indeed, we find that $\sup A = 1$ since $\forall a \in A, a \leq 1$. However, the set does not have a maximum. Informally speaking, this is due to the fact that for any upper bound $x \in A$, it is possible to find $x' \in A$ such that $x < x'$.

§4.2 Properties of $\mathbb{R}$

With the Axiom of Completeness in mind, we can catalog some interesting properties of $\mathbb{R}$.

Theorem 4.2.1**(Nested Interval Property)** For each $n \in \mathbb{N}$, assume we have a closed interval $I_n = [a_n, b_n]$. Assume further that each of the intervals are nested, i.e.

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

Then, the intersection of these intervals has a nonempty intersection

$$\bigcap_{n=1}^{\infty} I_n \neq \emptyset$$

Proof: Consider the sequence of real numbers formed by the a_n's. Call this sequence A. By the Axiom of Completeness, we know that $a_n \leq \sup A$. By the fact each interval is a superset of the next one in the sequence, the b_n's are also upper bounds. By the definition of supremum $\sup A \leq b_n$. Thus, $\forall n, a_n \leq \sup A \leq b_n$

■

The following property aims to determine a relation between the real numbers and the natural numbers. Specifically, we show that introducing the real numbers as a superset of the natural numbers does not introduce an upper bound for the natural numbers.

Theorem 4.2.2**(Archimedean Property)**

i. Given any real number $x \in \mathbb{R}$, there exists $n \in \mathbb{N}$ satisfying $n > x$.
ii. Given any real number $y \in \mathbb{R}$, there exists $n \in \mathbb{N}$ satisfying $\frac{1}{n} < y$.

Proof: For (i) we argue by contradiction. Another way to phrase the property is that the natural numbers do not have a real number upper bound. Suppose that $\mathbb{N}$ has an upper bound. Since $N \subset \mathbb{R}$, the Axiom of Completeness applies. Let $\alpha = \sup A$, then by definition of supremum, $\alpha - 1$ is no longer an upper bound. Hence $\alpha - 1 < n$[1], for some $n \in \mathbb{N}$. But this also means that $\alpha < n + 1$, contradicting the assumption that α is an upper bound.

[1] This follows from the fact that if no such n exists, then $\alpha - 1$ would also be an upper bound.

For (ii), simply set x to be $1/y$ in the inequality $n > x$.

■

In the same manner as above, we can also propose a theorem relating the rationals with the reals.

Theorem 4.2.3

i. Given $x, y \in \mathbb{R}$, where $x < y$, there exists $r \in \mathbb{Q}$ such that $x < r < y$.
ii. Given $x, y \in \mathbb{R} - \mathbb{Q}$, where $x < y$, there exists $r \in \mathbb{R} - \mathbb{Q}$ such that $x < r < y$.

In other words, it is always possible to find another rational or another irrational number between two real numbers (regardless if both endpoints are rational or irrational).

Idea of the Proof:

(i) The challenge is to find $p, q \in \mathbb{Z}$ such that $x < \frac{p}{q} < y$. First, justify using the Archimedean Property that there exists a q such that, $\frac{p-1}{q} \leq x$ does not imply $\frac{p}{q} \geq y$. Then express the inequality as

$$qx < p < qy$$

And suppose p is the smallest integer bigger than qx. Finish the proof by showing the above inequality holds.

■

(ii) The result follows from (i) by considering the shifted interval $a - \sqrt{2}$ and $b - \sqrt{2}$. It may be helpful to convince ourselves that if $a \in \mathbb{Q}$ and $t \notin \mathbb{Q}$, then $a + t \notin \mathbb{Q}$.

■

5 Graph Theory

§5.1 Introducing Graphs

In Graph Theory the central object of study is the graph. Essentially graphs are used to model systems of objects which exhibit a pairwise relationship with one another. For example, we may wish to use graphs to model a network of computers or a system of roads and paths. We introduce a formal definition of the graph below.

Definition 5.1.1 A **graph** G is defined as an ordered triple $(V(G), E(G), \phi)$. $V(G)$ denotes the **vertex set** of the graph, $E(G)$ denotes the **edge set** of the graph, and ϕ is an **incidence relation**, defined as $\phi: E(G) \to V(G) \times V(G)$, which associates an element of the edge set with a pair of elements in the vertex set[1].

Accordingly, we refer to elements of the edge and vertex sets as **edges** and **vertices (or nodes,** respectively. The incidence function maps edges to a pair of vertices corresponding to its endpoints.

We introduce a classic example to illustrate the use of graphs as models for systems of objects[2].

Example 5.1.2 **(Seven Bridges of Konigsberg)** The following diagram shows a system of islands, each connected by two-way bridges.

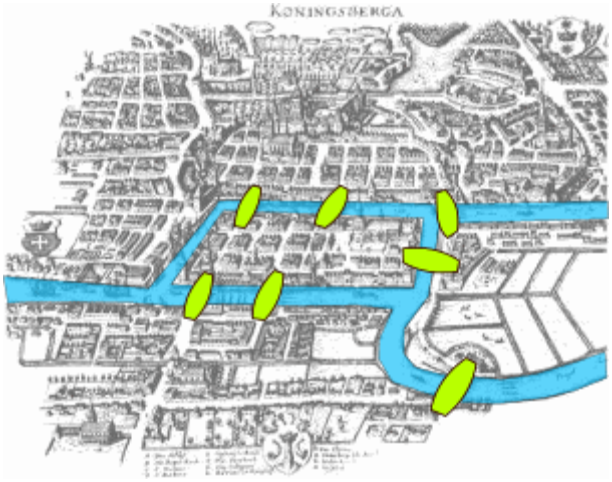
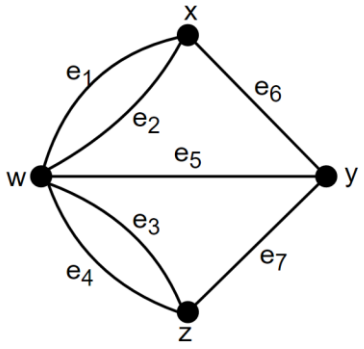


Figure 5.1.1 The Seven Bridges of Konigsberg
By Bogdan Giuşcă - Public domain (PD), based on the image, CC BY-SA 3.0,
https://commons.wikimedia.org/w/index.php?curid=112920

[1] Some definitions omit the incidence relation. We choose to include it to allow for discussion on non-simple graphs—graphs with multiple edges or loops.
[2] This example is courtesy of Euler, and was the first problem where Graph Theory was used on.

We can use graphs to model the relationship between the islands, in particular if we let the islands be our vertices and the bridges connecting them be the edges. We can construct the following visual representation of the graph.



Here, the graph G has a vertex set $V(G) = \{w, x, y, z\}$ and edge set $E(G) = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$. The incidence function of the graph can also be given as

$$\phi(e_1) = \phi(e_2) = (w, x)$$
$$\phi(e_3) = \phi(e_4) = (w, z)$$
$$\phi(e_5) = (w, y)$$
$$\phi(e_6) = (x, y)$$
$$\phi(e_7) = (y, z)$$

We may notice that ϕ in 5.1.2 is not injective (i.e., two distinct edges map to the same pair of vertices). We provide the following definitions to distinguish such a case

Definition 5.1.3 A **loop** is an edge whose endpoints are equal. **Multiple edges** are edges that have the same pair of endpoints. A **simple graph** is a graph that has no loops or multiple edges.

Abuse of Notation 5.1.4 Often defining a graph in the manner presented in 5.1.2 may be too long. To abbreviate, we may wish to write edges as a pair of vertices, also indicative of the incidence function. For instance, in 5.1.2, we may write e_4 as (w, y) or simply wy. When order is important, we will treat the first vertex in the pair as the source vertex.

§5.2 Elementary Subsets and Relations of Edges and Vertices

In this section, we define elementary relationships between edges and vertices of a graph.

Firstly, we define relations that are introduced by the incidence function of a graph.

Definition 5.2.1 Let u, v be vertices of a graph G. u and v are **adjacent vertices** if there is an edge in $E(G)$ whose endpoints are u and v. We denote adjacency by $u \leftrightarrow v$.

Definition 5.2.2 An edge $e \in E(G)$ is an **incident edge** to its endpoints.

An important metric based on incidence is the degree of a vertex.

Definition 5.2.3 The **degree** of a vertex v, denoted $\deg v$, is the number of edges that are incident to the vertex. Loops contribute 2 to the degree. As shorthand, we say that a vertex is **odd** if it has odd degree and **even** if it has even degree. If a graph is **odd** then all its vertices are odd, and if a graph is **even** then all its vertices are even.

We can also define elementary objects that can be derived from graphs. These are given below.

Definition 5.2.4 The **complement** of a graph G, denoted $\bar{G}$, is defined as a graph with the same vertex set as G and whose edges are not in G. More symbolically $V(\bar{G}) = V(G)$ and $e \in E(\bar{G})$ if and only if $e \notin E(G)$.

Definition 5.2.5 A graph is **self-complementary** if $G \cong \bar{G}$

Definition 5.2.6 A **clique** of a graph is a set of pairwise adjacent vertices. More formally, every vertex v in the clique is adjacent to every other vertex in the clique.

Definition 5.2.7 An **independent set** of a graph is a set of pairwise non-adjacent vertices. More formally, there are no edges in the graph which has both of its endpoints as elements of the independent set.

Analogous to set theory, we can find notions of subgraphs and partitions. These are introduced in the following definitions

Definition 5.2.8 The graph H is a **subgraph** of a graph G, if and only if $V(H) \subseteq V(G)$, $E(H) \subseteq E(H)$, and the incidence relation of H and G restricted on $V(H)$ and $E(H)$ are the same ($\phi_H = \phi_G$) . We denote H being a subgraph of G as $H \subseteq G$.

Definition 5.2.9 The **decomposition** of a graph is a list of subgraphs such that each edge appears in exactly one subgraph in the list.

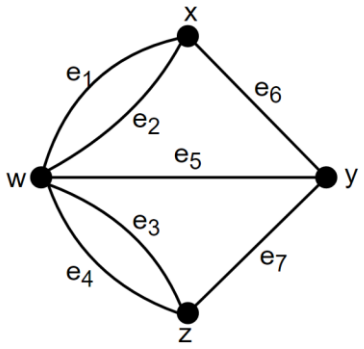
§5.3 Graph Representations

In our study of graphs, it often helps to be able to represent a particular graph. One such representation was provided in 5.1.2 using a picture. However, we may be able to see how limiting this is especially if the graph has multiple edges that can be confusing to the viewer. Additionally, if we were representing a graph for a computer to handle, we cannot simply expect the computer to use the drawing of the graph.

The following approaches serve to remedy this problem.

Definition 5.3.1 Let G be a graph with vertex set $V(G) = \{v_1, \dots, v_n\}$ and edge set $E(G) = \{e_1, \dots, e_m\}$. The **adjacency matrix** of G (which we write as $A(G)$) is an $n \times n$ matrix in which the entry a_{ij} is the number of edges in G with endpoints $\{v_1, v_j\}$ (in that order).

Example 5.3.2 The Seven Bridges of Konigsberg (defined in 5.1.2) has the following adjacency matrix (the graph is also shown again for convenience).



$$A(G) = \begin{pmatrix} 0 & 2 & 1 & 2 \\ 2 & 0 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 2 & 2 & 1 & 0 \end{pmatrix}$$

The order of the columns and the rows is w, x, y, z.

We may also wish to use an alternative to adjacency matrices, particularly because the number of entries is proportional to the square of the number of vertices.

Definition 5.3.3 Let G be a graph with vertex set $V(G) = \{v_1, \dots, v_n\}$ and edge set $E(G) = \{e_1, \dots, e_m\}$. The **incidence matrix,** denoted $M(G)$, is the $n \times m$ matrix where the a_{ij} entry is computed by

$$a_{ij} = \begin{cases} 1, & if\ e_j\ has\ v_i\ as\ an\ endpoint \\ 0, & otherwise \end{cases}$$

Example 5.3.4 The Seven Bridges of Konigsberg graph has the following incidence matrix.

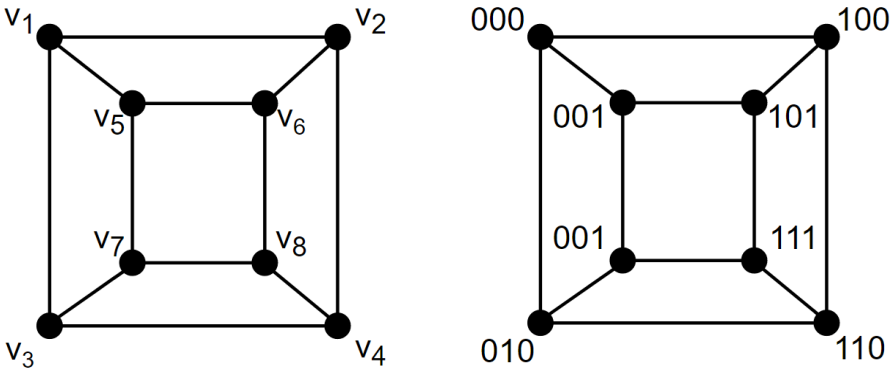
$$M(G) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Where the vertices are ordered as w, x, y, z, and the edges in sequence of their subscripts.

§5.4 Graph Isomorphisms

We can imagine that drawing graphs or representing them as a matrix can yield seemingly different results if we either renamed the vertices or if we rearranged the rows and columns of the adjacency or incidence matrix. Still, despite alterations such as these that involve reordering or renaming the vertices, we do not actually change the structure of the graph. Intuitively, we can see this because we do not add or remove vertices and edges in our graph.

Perhaps another motivation for studying the "renaming" of graphs is that it allows us to look at the structure of seemingly different graphs. It may not be obvious, for example that the net of a cube has the same structure as the graph that you would get by considering all possible bit strings as vertices (000, 001, 010, … 111), and adding an edge between vertices which are different by 1 character.



We establish a notion of similarity between graphs using the following definition:

Definition 5.4.1 An **isomorphism** from G to H is a bijection f that maps $V(G)$ to $V(H)$ and $E(G)$ to $E(H)$ such that each edge of G with endpoints u and v is mapped to an edge with endpoints $f(u)$ and $f(v)$. Two graphs are **isomorphic**, written as $G \cong H$ if there is an isomorphism between them.

Isomorphisms allow us to establish equivalence classes of graphs. However, we first show that isomorphism is, in fact, an equivalence relation[1].

Proposition 5.4.2 $G \cong H$ is an equivalence relation.

Proof: To show that it is an equivalence relation, we show it satisfies three properties. Let F, G, H be graphs.

Firstly, the relation is reflexive since $G \cong G$. The isomorphism is simply the identity function that maps each vertex and edge to itself.

Second, the relation is symmetric since $G \cong H$ implies that there exists a bijective mapping f, by the definition of isomorphism. Since f is bijective, f^{-1} is well defined and it maps $V(H)$ to $V(G)$, and $E(H)$ to $E(G)$ while preserving incidence between edges. Hence $G \cong H$ implies $H \cong G$.

[1] What we really mean is that the relation defined by two graphs being isomorphic is an equivalence relation.

Finally, the relation is transitive. If we have $F \cong G$ and $G \cong H$, then there exist bijective mappings f and g that map from F to G, and which maps from G to H, respectively. Taking the composition $f \circ g$ gives a new mapping from F to H. Since the composition of bijections is a bijection, $F \cong H$.

■

Consequently, we have the following definition

Definition 5.4.3 An **isomorphism class** is an equivalence class of graphs under an isomorphism relation.

The process of determining whether or not two graphs are isomorphic can be tedious, and no "fast" algorithm has been found to exist for this problem. In line with this, however, we may observe some of the following as true for two graphs if we are to test for isomorphism

Proposition 5.4.4 $G \cong H$ if and only if $\bar{G} \cong \bar{H}$.

Proof: We need only show the forward relation is true. Since an isomorphism is simply a renaming of the vertices such that adjacency is preserved, it also preserves nonadjacency.

■

§5.5 Families of Graphs

In this section we catalog some important classes of graphs. We will elaborate on these in throughout our study of Graph Theory.

From the definition of a graph, it should be apparent that it is a recursive structure, namely because it consists of an edge and vertex set which we can add elements to or remove elements from. Induction can, therefore, be applied in proving some theorems concerning graphs. To that end, we introduce for formality's sake, a graph that is the "base case" of all other graphs. It is analogous to the empty set in Set Theory.

Definition 5.5.1 The **null graph** is the graph whose edge set and vertex set are empty.

We will unlikely use the null graph to model any real world system. Of course, this is not the only interesting family or type of graph that we will encounter.

Definition 5.5.2 The **bipartite graph** is a graph G whose vertex set $V(G)$ can be expressed as the union of two disjoint, possibly empty independent sets.

We can, of course, generalize the bipartite graph.

Definition 5.5.3 The **k-partite graph** is a graph G whose vertex set $V(G)$ can be partitioned into k disjoint, possibly empty, independent sets

Another common graph we are likely to find involves traversal along a graph. More specifically, we have the following definition.

Definition 5.5.4 A **path** is a simple graph whose vertices can be ordered into a list such that consecutive vertices are adjacent.

More specifically, if we have a list of n vertices in the path, it is possible to order them as $v_1, v_2, \dots, v_n$ such that $v_1 \leftrightarrow v_2, v_2 \leftrightarrow v_3, \dots, v_{n-1} \leftrightarrow v_n$.

If a path has n vertices, we say that it is an ***n*-path**, which we may also write symbolically as P_n. This defines an isomorphism class for all paths that have n vertices.

Definition 5.5.5 A **cycle** is a graph whose vertices can be ordered into a list such that consecutive vertices are adjacent, and the first and last vertices are adjacent.

More specifically, if we have a list of n vertices in the cycle, it is possible to order them as $v_1, v_2, \dots, v_n$ such that $v_1 \leftrightarrow v_2, v_2 \leftrightarrow v_3, \dots, v_{n-1} \leftrightarrow v_n, v_n \leftrightarrow v_1$.

If a cycle has n vertices, we say that it is an ***n*-cycle**, which we may also write symbolically as C_n. This defines an isomorphism class for all cycles that have n vertices.

We may also wish to define simple graphs that have as many edges as possible. We provide two important isomorphism classes of such below:

Definition 5.5.6 A **complete graph** is a simple graph whose vertices are pairwise adjacent (i.e., every vertex is connected to every other vertex). We write the isomorphism class for the complete graph with n vertices as K_n

Definition 5.5.7 A **complete bipartite graph** is a simple bipartite graph where two vertices are adjacent if and only if they are from different independent sets (i.e., every vertex from one set is connected to every vertex in the other). We write the isomorphism class for the complete bipartite graph with r, s vertices for the two respective independent sets as $K_{r,s}$

§5.6 Graph Connectivity

A natural question to ask in the context of graphs is whether or not the graph is connected. In the context of a road network, for example, are all cities accessible via roads or is there some set of cities cut off from the rest.

Definition 5.6.1 A graph G is said to be **connected** if $\forall u, v \in V(G)$, there exists a path that includes u, v. Otherwise, the graph is **disconnected.**

Graph theory features a plethora of terms concerning the traversal of a graph. We provide them all in the following definition.

Definition 5.6.2 A **walk** is a list $v_0, e_1, \dots, e_k, v_k$ of alternating vertices and edges where each edge, e_i has endpoints v_{i-1} and v_i. A **trail** is a walk with no repeated edges.

If we are particular with the endpoints, we say that we have a u, v-walk, u, v-trail, or u, v-path. The other vertices in such a walk, trail or path are called **internal vertices.** The **length** of a walk, path, trail, or cycle is the number of edges present.

A walk or trail is **closed** if the endpoints are the same.

One basic property of connectivity within a graph is stated below. This property implies that to check if a graph is connected, it suffices to show that there is a u, v-path from each vertex starting from a particular vertex.

Proposition 5.6.3 The connection relation is an equivalence relation.

Proof: It is most certainly the case that a vertex is connected to itself. It is also the case (if direction is irrelevant), that a path can be directed one way to go from u to v or the other way to go to v to u. Finally, it is also apparent that if we have a path from u to v and another from v to w, then we have a u, w-path that passes through v. We have shown reflexivity, symmetry and transitivity.

■

Another consequence of note from 5.6.3 is that we can form an equivalence class for each vertex based on the connectivity relation. We introduce this notion in the definition below.

Definition 5.6.4 A **component** of a graph is a maximally connected subgraph of a particular graph. A component is **trivial** if it has no edges. An **isolated vertex** is a vertex with degree 0.

We can naturally add or remove components from a graph if we introduce the following operation.

Definition 5.6.5 A **cut-edge** or a **cut-vertex** is an edge or vertex in a graph that increases the number of components. We denote this by writing $G - e$, or $G - M$ if we are removing a vertex or edge, or a set of vertices and edges respectively.

An **induced subgraph** is a subgraph obtained by deleting a set of vertices. This is denoted as $G[T]$, where G is a graph and T is a set of vertices. We say that G is induced by T.

In 5.1.2, we introduced the very first problem where Graph Theory was applied. Although, we never explicitly stated what the problem was beyond modelling the connections between islands through graphs. Here we lay out the actual problem that was being solved.

Example 5.6.6 **(Seven Bridges of Konigsberg Continued)** Given the graph shown in 5.1.2, is there a walk that includes all the bridges exactly once.

We now explore how Euler solved this problem using the following definitions and theorems.

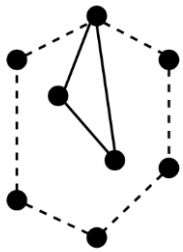
Definition 5.6.7 A **Eulerian** graph is a graph that contains a closed trail containing all edges.

Theorem 5.6.8 A graph is Eulerian if and only if all the vertices have even degree and it has at most one nontrivial component.

Idea of the Proof: To show necessity, we see that if there is a walk visiting all edges, then each edge must be crossed an even number of times (one incoming and one outgoing), hence it must have even degree, and clearly the graph must be connected.

Otherwise, argue by induction. The base case of 0 edges is trivial. In the inductive case, assume each vertex has even degree. Show first that this implies a cycle must exist[1]. In the inductive case, consider such a cycle and delete it, removing either degree 0 or 2 from a subset of the vertex. The induction hypothesis applies and we are done.

The graph below illustrates the induction step. The dashed lines show a cycle that can be removed from the graph. The remaining graph is smaller and strong induction applies.



■

Therefore, to answer the problem in 5.6.6, it is not Eulerian since we have vertices that are odd degree.

§5.7 Bipartite Graphs

Bipartite Graphs arise when we need to model mappings between two sets. The following section is dedicated to these types of graphs.

Proposition 5.7.1 A graph is bipartite if and only if it has no odd cycle.

Proof: If a graph is bipartite, then it takes an even number of steps to go from a partite set to itself.

Otherwise, if the graph has no odd cycle, then consider each nontrivial component of the graph and partition the vertices into subsets X and Y, such that for some chosen vertex in the component, u, and with $f_u(v)$ being the length of the shortest path from u to v, we have

$$X = \{v | f(v) is\ odd\}$$

[1] The Pigeonhole principle should make this obvious.

$$Y = \{v | f(v)\ is\ even\}$$

Argue by contradiction and without loss of generality, suppose that if two vertices $v, v' \in X$ are connected. Then there is an odd length walk $uvv'u$, which must contain an odd length cycle, contradicting the assumption.

■

This page intentionally left blank

Challenges

The following section consists of a list of exercises to test understanding on material. Solutions to the problems presented here are shown in the next section.

1. Prove $(A \wedge B) \to C \vdash A \to (B \to C)$.

2. Show that $\sqrt{2}$ is irrational. Does a similar argument apply to $\sqrt{4}$?

3. Given a function $f: X \to Y$ investigate when the following are true for all subsets $A, B \subseteq X$:
   e. $f(A \cap B) = f(A) \cap f(B)$
   f. $f(A \cup B) = f(A) \cup f(B)$

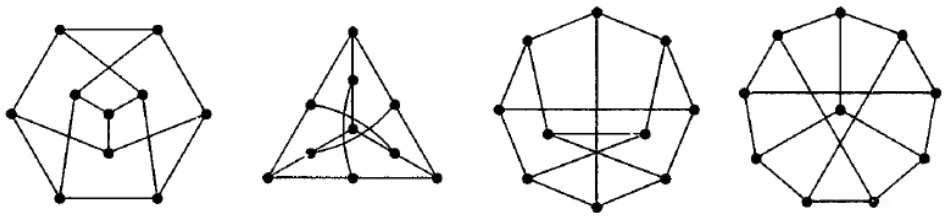
4. Prove the following:
   Assume $s \in \mathbb{R}$ is an upper bound for a set $A \subseteq \mathbb{R}$. Then, $s = \sup A$ if and only if, for every choice of $\epsilon > 0$, there exists an element $a \in A$ satisfying $s - \epsilon < a$.

5.
   a. Let $D_1, \dots, D_n$ be assumption formulae where for $j = 1, \dots, n$ only the distinct variables $y_1, \dots, y_{p_j}$ are varied for D_j (but if $j \neq k$, then $y_{j_1}, \dots, y_{j_{p_j}}$ need not be distinct from $y_{k_1}, \dots, y_{k_{p_k}}$). Show that
   $$D_1, \dots, D_n \vdash E$$
   If and only if
   $$\vdash \forall y_{11} \dots \forall y_{1p_1} D_1 \to \left(\forall y_{21} \dots \forall_{2p_2} D_2 \to \cdots \left(\forall y_{n1} \dots \forall y_{np_n} D_n\right) \dots\right)$$

   b. Given a deduction of E from $D_1, \dots, D_l$, show that another deduction from E from $D_1, \dots, D_l$ can be found in which for $j = 1, \dots, l$, Postulate 9 is applied to premises dependent on D_j only with respect to variables which are varied for D_j in the given deduction, and Postulate 2 is applied to no postulate dependent on an assumption formula.

   c. Show that a variable y is varied for a given one of the assumption formulae in Δ in the resulting deduction $\Delta, \Gamma \vdash E$, where $\Delta, \Gamma \vdash C$ and $C, \Gamma \vdash E$ only (a) if y is varied for the same assumption formula in Δ or (b) if y is varied for C in the second given deduction, and C depends on the assumption formula in Δ and that assumption formula contains y free.

6. Show that the following graphs are Isomorphic to each other. The illustration is courtesy of West, 2001.



7. Prove that K_n decomposes into 3 isomorphic subgraphs if and only if $n + 1$ is not divisible by 3.

8. Present an alternate proof to 2.5.2 (the set of real numbers is uncountable) that uses the Nested Interval Property.

9. Show that $|P(N)| = \mathbb{R}$.

Solutions

The following section consists of answers to the problems presented in previous sections

1. Prove $(A \wedge B) \to C \vdash A \to (B \to C)$.
   Solution:
   We apply the Deduction Theorem (1.2.7). Observe that the target metamathematical statement follows from the Theorem applied to:
   $$(A \wedge B) \to C, A \vdash\!\!\to (B \to C)$$
   Which also follows from the Deduction Theorem applied to:
   $$(A \wedge B) \to C, A, B \vdash\!\!\to C$$

   To finish the solution, we prove the above equation using Axiomatic System 1.1.9:

1.	$(A \wedge B) \to C$	First Assumption Formula
2.	A	Second Assumption Formula
3.	B	Third Assumption Formula
4.	$A \to (B \to (A \wedge B))$	Postulate 3
5.	$B \to (A \wedge B)$	Postulate 2, 2, 4
6.	$(A \wedge B)$	Postulate 2, 3, 5
7.	C	Postulate 2, 1, 6

   Therefore $(A \wedge B) \to C, A, B \vdash C$, and by the argument using the Deduction Theorem presented above $(A \wedge B) \to C \vdash A \to (B \to C)$

   ■

2. Show that $\sqrt{2}$ is irrational. Does a similar argument apply to $\sqrt{4}$?
   Solution:
   We argue by contradiction. Suppose $\sqrt{2} = \frac{p}{q}$ where p and q are coprime. Then
   $$2 = \frac{p^2}{q^2}$$
   $$2q^2 = p^2$$
   Certainly, p^2 is even, hence p is even, that is for some $k \in \mathbb{Z}$, $p = 2k$.

   Substituting we get:
   $$2q^2 = 4k^2$$
   $$q^2 = 2k^2$$
   By a similar argument, q^2 is even, hence q is even, but we assumed p and q were coprime.

   The argument fails for $\sqrt{4} = \frac{p}{q}$ when we argue that p^2 must only be divisible by 4 since this is not the only possibility. Indeed if p is divisible by 2, then p^2 is divisible by 4, and we get
   $$4q^2 = (2k)^2 = 4k^2$$
   $$q = k$$

Which gives us

$$\sqrt{4} = \frac{2q}{q} = 2$$

■

3. Given a function $f: X \to Y$ investigate when the following are true for all subsets $A, B \subseteq X$:
   a. $f(A \cap B) = f(A) \cap f(B)$
   Solution:
   We show that this is true for any arbitrary A and B as long as the function is injective. First, we show $f(A \cap B) \subseteq f(A) \cap f(B)$. Consider $x \in A \cap B$, which implies $x \in A$ and $f(x) \in A$, and $x \in B$ and $f(x) \in B$. Therefore $f(x) \in f(A) \cap f(B)$, whenever $x \in A \cap B$, thus $f(A \cap B) \subseteq f(A) \cap f(B)$.

   Going the other way, if $f(x) \in f(A)$, then $x \in A$, likewise if $f(x) \in f(B)$, then $x \in B$. However, if the function is not injective, then there exists $x_1, x_2 \in X$ such that $x_1 \neq x_2$ $f(x_1) = f(x_2)$. Let $x_1 \in A - B$, and $x_2 \in B - A$. Then $x_1, x_2 \notin A \cap B$, so that $f(x_1) \notin f(A \cap B)$, but $f(x_1) = f(x_2)$ so $f(x_1) \in f(A)$ and $f(x_1) \in f(B)$, so $f(x_1) \in f(A) \cap f(B)$.

   ■

   b. $f(A \cup B) = f(A) \cup f(B)$
   We show that this is always true. If $x \in A \cup B$, then $x \in A$ or $x \in B$, so that either $f(x) \in f(A)$ or $f(x) \in f(B)$. This establishes that $f(A \cup B) \subseteq f(A) \cup f(B)$.

   Going the other way, if $f(x) \in f(A) \cup f(B)$, then either $f(x) \in f(A)$ or $f(x) \in f(B)$. Hence, either $x \in A$ or $x \in B$. It doesn't matter if $x \in A \cap B$ or $x \in A - B$ as these are still part of the union. This establishes that $f(A) \cup f(B) \subseteq f(A \cup B)$, which completes the proof.

   ■

4. Prove the following:
   Assume $s \in \mathbb{R}$ is an upper bound for a set $A \subseteq \mathbb{R}$. Then, $s = \sup A$ if and only if, for every choice of $\epsilon > 0$, there exists an element $a \in A$ satisfying $s - \epsilon < a$.
   Solution:
   We first show that if $s = \sup A$, then for every choice of $\epsilon > 0$, there exists $a \in A$ such that $s - \epsilon < a$. Since s is the least upper bound $s - \epsilon < s$ cannot be an upper bound, and therefore there must be some element $a \in A$ such that $s - \epsilon < a$.

   Conversely, if we suppose that $\forall \epsilon > 0$, there exists $a \in A$ such that $s - \epsilon < a$, where s is an upper bound. We verify that s is the least upper bound. Suppose $b < s$, then take $\epsilon = s - b$. By the hypothesis, there must exist $a \in A$ such that $s - (s - b) < a$, in other words, $b < a$, hence b cannot be an upper bound, b cannot exist and $s = \sup A$

   ■

5.

a. Let $D_1, \dots, D_n$ be assumption formulae where for $j = 1, \dots, n$ only the distinct variables $y_1, \dots, y_{p_j}$ are varied for D_j (but if $j \neq k$, then $y_{j_1}, \dots, y_{j_{p_j}}$ need not be distinct from $y_{k_1}, \dots, y_{k_{p_k}}$). Show that

$$D_1, \dots, D_n \vdash E$$

If and only if

$$\vdash \forall y_{11} \dots \forall y_{1p_1} D_1 \to \left(\forall y_{21} \dots \forall_{2p_2} D_2 \to \cdots \left(\forall y_{n1} \dots \forall y_{np_n} D_n \to E\right) \dots\right)$$

Solution:

The following deduction using Eliminations and Introductions shows both necessary and sufficient conditions (to go the other way, simply reverse the order of statements in the proof and change all Eliminations to Introductions and all Introductions to Eliminations).

1. $D_1 \dots D_n \vdash E$ Given
2. $\forall y_{11} \dots \forall y_{1p_1} D_1 \vdash D_1$ Universal elimination

   …

   $\forall y_{n1} \dots \forall y_{np_n} D_n \vdash D_n$ Universal elimination
3. $\forall y_{11} \dots \forall y_{1p_1} D_1, \dots, \forall y_{n1} \dots \forall y_{np_n} D_n \vdash E$ 1.2.6 v.
4. $\forall y_{11} \dots \forall y_{1p_1} D_1, \dots, \forall y_{n-11} \dots \forall y_{np_{n-1}} D_{n-1} \vdash \forall y_{n1} \dots \forall y_{np_n} D_n \to E$ Deduction Theorem

…

$\vdash \forall y_{11} \dots \forall y_{1p_1} D_1 \to \left(\forall y_{21} \dots \forall_{2p_2} D_2 \to \cdots \left(\forall y_{n1} \dots \forall y_{np_n} D_n \to E\right) \dots\right)$ Deduction Theorem

■

b. Given a deduction of E from $D_1, \dots, D_l$, show that another deduction of E from $D_1, \dots, D_l$ can be found in which for $j = 1, \dots, l$, Postulate 9 is applied to premises dependent on D_j only with respect to variables which are varied for D_j in the given deduction, and Postulate 2 is applied to no premise dependent on an assumption formula.

Solution:

Consider from (a) $D_1, \dots, D_l \vdash E$, and consider the proof for converting it to $\vdash \forall y_{11} \dots \forall y_{1p_1} D_1 \to \left(\forall y_{21} \dots \forall_{2p_2} D_2 \to \cdots \left(\forall y_{n1} \dots \forall y_{np_n} D_n \to E\right) \dots\right)$, and then back to $D_1, \dots, D_l \vdash E$ using a different deduction. For brevity, call the former the forward deduction and the latter the backward deduction. By (a) we only apply Universal elimination (and hence Postulate 9) to those premises which are D_j or which are derived from D_j (hence dependent on D_j) since variables stay varied (1.4.2), and only on those variables that are varied in D_j.

In the backward deduction, we can choose to apply either Postulate 9 or 12 depending on the quantifiers within each assumption formula. However, note that in such a case, the new premise is

$$\forall y_{11} \dots \forall y_{1p_1} D_1 \to \left(\forall y_{21} \dots \forall_{2p_2} D_2 \to \cdots \left(\forall y_{n1} \dots \forall y_{np_n} D_n \to E\right) \dots\right)$$

Which is not dependent on any of the assumption formulae $D_1, \dots, D_n$.

■

c. Show that a variable y is varied for a given one of the assumption formulae in Δ in the resulting deduction $\Delta, \Gamma \vdash E$, where $\Delta, \Gamma \vdash C$ and $C, \Gamma \vdash E$ only (a) if y is varied for the same assumption formula in Δ or (b) if y is varied for C in the second given deduction, and C depends on the assumption formula in Δ and that assumption formula contains y free.

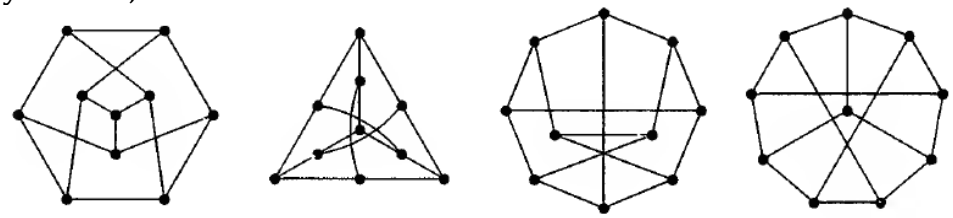
Solution:

Case (a) follows immediately from 1.4.2. Case (b) also immediately follows by first observing that varied variables for a formula dependent on one of the assumption formulae remain varied in the assumption formula for the given deduction (follows from 1.4.1 and 1.4.2). We require y be free by the definition of dependence so that y is varied in the resulting deduction.

Note that a special case arises when we consider $C, \Gamma \vdash E$ where we have an application of Postulate 9 or 12 with respect to y on a premise dependent on C. In such a case, however, we use (b) to create a new deduction where neither Postulate 9 nor Postulate 12 are applied to any dependent formula.

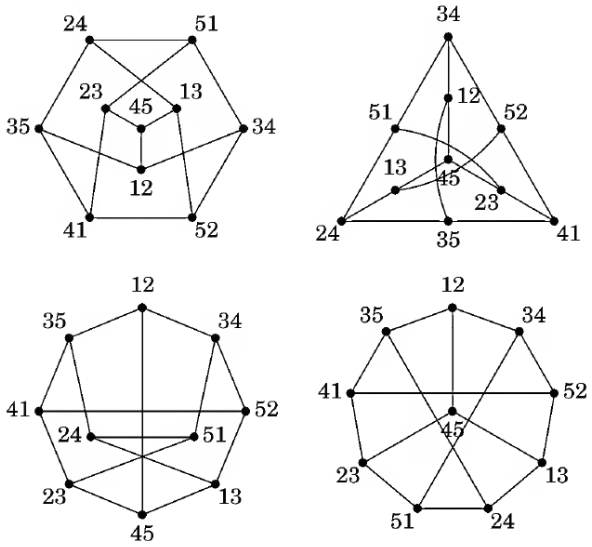
■

6. Show that the following graphs are Isomorphic to each other. The illustration is courtesy of West, 2001.



Solution:

The following labelling shows the graphs are from the same isomorphism class (Illustration can be found in West, 2001).



■

7. Prove that K_n decomposes into 3 isomorphic subgraphs if and only if $n+1$ is not divisible by 3.

Solution:

We first show that if K_n decomposes into 3 isomorphic subgraphs, then $n+1$ is not divisible by 3 (or $n \not\equiv 1 \ mod\ 3$). We have $\binom{n}{2}$ edges in K_n, so

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

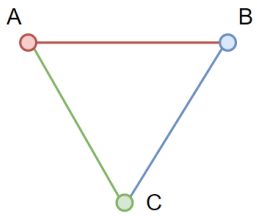
Since we have 3 isomorphic subgraphs, we have to partition the edges evenly, so

$$\frac{n(n-1)}{2} \equiv 0 \ mod\ 3$$

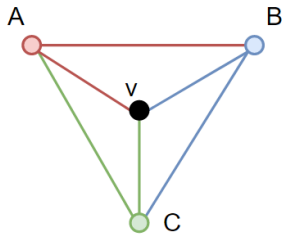
So that either $n \equiv 0 \ mod\ 3$ or $n-1 \equiv 0 \ mod\ 3$, and in either case $n+1 \not\equiv 0 \bmod 3$.

Now suppose $n \equiv 0 \ mod\ 3$ or $n-1 \equiv 0 \ mod\ 3$. We provide an explicit form for the subgraph. In the graphs that follow, suppose A, B, C are subgraphs which are complete graphs containing the same number of vertices (specifically $\lfloor n/3 \rfloor$). Let v be a single vertex, and let each edge between subgraphs represent a set of edges connecting all vertices from one subgraph to all vertices of another. Then the following decompositions of K_n use 3 copies of the same graph.

For $n \equiv 0 \ mod\ 3$



For $n \equiv 1 \; mod \; 3$



■

8. Present an alternate proof to 2.5.2 (the set of real numbers is uncountable) that uses the Nested Interval Property.
   Solution:
   We argue by contradiction. Suppose we have a list of real numbers $\{r_1, r_2, . r_3, \dots\}$. Consider the sequence of nested intervals constructed such that for the n^{th} interval I_n, we have

   $$r_k \in I_n, k \geq n$$

   And such that $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$

   By our assumption that the real numbers are countable, $\bigcap_n^\infty I_n = \emptyset$. By the nested interval property, we have $\bigcap_n^\infty I_n \neq \emptyset$. Hence, our assumption was false and the real numbers are uncountable

   ■

9. Show that $|P(N)| = \mathbb{R}$.
   Solution:
   TO-DO

10. Bla*