A Concise Lecture Note on Basic Mathematics - based on

"A Transition to Advanced Mathematics 8th Edition"

1 Logic and Proofs

1.1 Proposition and Connectives

Definition 1.1. A ***proposition*** is a sentence that has exactly one truth value. It is either true, which we denote by T, or false, which we denote by F.

Example 1.2. $7^2 > 60$ (F), $\pi > 3$ (T)

Example 1.3. Earth is the closest planet to the sun. (F)

Example 1.4. The statement "the north Pacific right whale (露脊鯨) will be extinct species before the year 2525" has one truth value but it takes time to determine the truth value.

Example 1.5. That "Euclid was left-handed" is a statement that has one truth value but may never be known.

Definition 1.6. A ***negation*** of a proposition P, denoted by $\sim$P, is the proposition "not P". The proposition $\sim$P is $\begin{matrix}\text{true}\\ \text{false}\end{matrix}$ exactly when P is $\begin{matrix}\text{false}\\ \text{true}\end{matrix}$.

Definition 1.7. Given propositions P and Q, the $\begin{matrix}\textit{conjunction}\\ \textit{disjunction}\end{matrix}$ of P and Q, denoted by $\begin{matrix}\text{P} \wedge \text{Q}\\ \text{P} \vee \text{Q}\end{matrix}$, is the proposition "P $\begin{matrix}\text{and}\\ \text{or}\end{matrix}$ Q". $\begin{matrix}\text{P} \wedge \text{Q}\\ \text{P} \vee \text{Q}\end{matrix}$ is true exactly when $\begin{matrix}\text{both P and Q are true}\\ \text{at least one of P or Q is true}\end{matrix}$.

Example 1.8. Now we analyze the sentence "either 7 is prime and 9 is even, or else 11 is not less than 3". Let P denote the sentence "7 is a prime", Q denote the sentence "9 is even", and R denote the sentence "11 is less than 3". Then the original sentence can be symbolized by $(\text{P} \wedge \text{Q}) \vee (\sim \text{R})$, and the table of truth value for this sentence is

P	Q	R	$\text{P} \wedge \text{Q}$	$\sim$R	$(\text{P} \wedge \text{Q}) \vee (\sim \text{R})$
T	T	T	T	F	T
T	T	F	T	T	T
T	F	T	F	F	F
F	T	T	F	F	F
T	F	F	F	T	T
F	T	F	F	T	T
F	F	T	F	F	F
F	F	F	F	T	T

Since P is true and Q, R are false, the sentence $(\text{P} \wedge \text{Q}) \vee (\sim \text{R})$ is true.

Definition 1.9. A $\begin{matrix}\textit{tautology}\\ \textit{contradiction}\end{matrix}$ is a propositional form that is $\begin{matrix}\text{true}\\ \text{false}\end{matrix}$ for every assignment of truth values to its component.

Example 1.10. The logic symbol $(P \vee Q) \vee (\sim P \wedge \sim Q)$ is a tautology.

Example 1.11. The logic symbol $\sim(P \vee \sim P) \vee (Q \wedge \sim Q)$ is a contradiction.

Definition 1.12. Two propositional forms are said to be ***equivalent*** if they have the same truth value.

Theorem 1.13. *For propositions* P, Q, R, *we have the following:*

(a) $P \Leftrightarrow \sim(\sim P)$. (**Double Negation Law**)

(b) $P \vee Q \Leftrightarrow Q \vee P$
(c) $P \wedge Q \Leftrightarrow Q \wedge P$ } (**Commutative Laws**)

(d) $P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$
(e) $P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$ } (**Associative Laws**)

(f) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
(g) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ } (**Distributive Laws**)

(h) $\sim(P \wedge Q) \Leftrightarrow (\sim P) \vee (\sim Q)$
(i) $\sim(P \vee Q) \Leftrightarrow (\sim P) \wedge (\sim Q)$ } (**De Morgan's Laws**)

Proof. We prove (g) for example, and the other cases can be shown in a similar fashion. Using the truth table,

P	Q	R	Q∧R	P∨(Q∧R)	P∨Q	P∨R	(P∨Q)∧(P∨R)
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
F	T	T	T	T	T	T	T
T	F	F	F	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

we find that "$P \vee (Q \wedge R)$" is equivalent to that "$(P \vee Q) \wedge (P \vee R)$". □

Definition 1.14. A ***denial*** of a proposition is any proposition equivalent to $\sim P$.

- **Rules for $\sim$, $\wedge$ and $\vee$:**

1. $\sim$ is always applied to the smallest proposition following it.
2. $\wedge$ connects the smallest propositions surrounding it.
3. $\vee$ connects the smallest propositions surrounding it.

Example 1.15. Under the convention above, we have

1. $\sim P \vee \sim Q \Leftrightarrow (\sim P) \vee (\sim Q)$.
2. $P \vee Q \vee R \Leftrightarrow (P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$.
3. $P \wedge \sim Q \vee \sim R \Leftrightarrow \big[P \wedge (\sim Q)\big] \vee (\sim R)$.
4. $R \wedge P \wedge S \wedge Q \Leftrightarrow \big[(R \wedge P) \wedge S\big] \wedge Q$.

1.2 Conditionals and Biconditionals

Definition 1.16. For propositions P and Q, the ***conditional sentence*** $P \Rightarrow Q$ is the proposition "if P, then Q". Proposition P is called the ***antecedent*** and Q is the ***consequence***. The sentence $P \Rightarrow Q$ is true if and only if P is false or Q is true.

Example 1.17. We would like to determine the truth value of the sentence "if $x > 8$, then $x > 5$". Let P denote the sentence "$x > 8$" and Q the sentence "$x > 5$".

1. If P, Q are both true statements, then $x > 8$ which is (exactly the same as P thus) true.
2. If P is false while Q is true, then $5 < x \leqslant 8$ which is (exactly the same as $\sim P \wedge Q$ thus) true.
3. If P, Q are both false statements, then $x \leqslant 5$ which is (exactly the same as $\sim Q$ thus) true.
4. It is not possible to have P true but Q false.

Remark 1.18. In a conditional sentence, P and Q might not have connections. The truth value of the sentence "$P \Rightarrow Q$" only depends on the truth value of P and Q.

• **How to read** $P \Rightarrow Q$ **in English**?

1. If P, then Q.
2. P is sufficient for Q.
3. P only if Q.
4. Q whenever P.
5. Q is necessary for P.
6. Q, if P (or when P).

Definition 1.19. Let P and Q be propositions.

1. The ***converse*** of $P \Rightarrow Q$ is $Q \Rightarrow P$.
2. The ***contrapositive*** of $P \Rightarrow Q$ is $\sim Q \Rightarrow \sim P$.

Example 1.20. We would like to determine the truth value, as well as the converse and the contrapositive, of the sentence "if π is an integer, then 14 is even".

1. Since that π is an integer is false, the implication "if π is an integer, then 14 is even" is true.
2. The converse of the sentence is "if 14 is even, then π is an integer" which is a false statement.
3. The contrapositive of the sentence is "if 14 is not even, then π is not an integer" which is a true statement since the antecedent "14 is not even" is false.

By this example, we know that a sentence and its converse cannot be equivalent.

Theorem 1.21. *For propositions* P *and* Q*, the sentence* $P \Rightarrow Q$ *is equivalent to its contrapositive* $\sim Q \Rightarrow \sim P$.

Proof. Using the truth table

P	Q	$P \Rightarrow Q$	$\sim Q$	$\sim P$	$\sim Q \Rightarrow \sim P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

we conclude that the truth value of $P \Rightarrow Q$ and $\sim Q \Rightarrow \sim P$ are the same; thus they are equivalent sentences. □

Definition 1.22. For propositions P and Q, the ***bi-conditional sentence*** $P \Leftrightarrow Q$ is the proposition "P if and only if Q". The sentence $P \Leftrightarrow Q$ is true exactly when P and Q have the same truth values. In other words, $P \Leftrightarrow Q$ is true if and only if P is equivalent to Q.

Remark 1.23. The notation $\Leftrightarrow$ is a combination of $\Rightarrow$ and its converse $\Leftarrow$, so the notation seems to suggest that $(P \Leftrightarrow Q)$ is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. This is in fact true since

P	Q	$P \Leftrightarrow Q$	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (P \Rightarrow Q)$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

Example 1.24. The proposition "$2^3 = 8$ if and only if 49 is a perfect square" is true because both components are true. The proposition "$\pi = \frac{22}{7}$ if and only if $\sqrt{2}$ is a rational number" is also true (since both components are false). The proposition "$6 + 1 = 7$ if and only if Argentina is north of the equator" is false because the truth values of the components differ.

Remark 1.25. Definitions may be stated with the "if and only if" wording, but it is also common practice to state a formal definition using the word "if". For example, we could say that "a function f is continuous at a number c if $\cdots$" leaving the "only if" part understood.

Example 1.26. A teacher says "If you score 74% or higher on the next test, you will pass the exam". Even though this is a conditional sentence, everyone will interpret the meaning as a biconditional (since the teacher tries to "define" how you can pass the exam).

Theorem 1.27. *For propositions* P*,* Q *and* R*, we have the following:*

(a) $(P \Rightarrow Q) \Leftrightarrow (\sim P \vee Q)$.

(b) $(P \Leftrightarrow Q) \Leftrightarrow (P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

(c) $\sim (P \Rightarrow Q) \Leftrightarrow (P \wedge \sim Q)$.

(d) $\sim(\mathrm{P} \wedge \mathrm{Q}) \Leftrightarrow (\mathrm{P} \Rightarrow \sim \mathrm{Q})$.

(e) $\sim(\mathrm{P} \wedge \mathrm{Q}) \Leftrightarrow (\mathrm{Q} \Rightarrow \sim \mathrm{P})$.

(f) $\mathrm{P} \Rightarrow (\mathrm{Q} \Rightarrow \mathrm{R}) \Leftrightarrow (\mathrm{P} \wedge \mathrm{Q}) \Rightarrow \mathrm{R}$.

(g) $\mathrm{P} \Rightarrow (\mathrm{Q} \wedge \mathrm{R}) \Leftrightarrow (\mathrm{P} \Rightarrow \mathrm{Q}) \wedge (\mathrm{P} \Rightarrow \mathrm{R})$.

(h) $(\mathrm{P} \vee \mathrm{Q}) \Rightarrow \mathrm{R} \Leftrightarrow (\mathrm{P} \Rightarrow \mathrm{R}) \wedge (\mathrm{Q} \Rightarrow \mathrm{R})$.

• **How to read** $\mathrm{P} \Leftrightarrow \mathrm{Q}$ **in English**?

1. P if and only if Q.
2. P if, but only if, Q.
3. P implies Q, and conversely.
4. P is equivalent to Q.
5. P is necessary and sufficient for Q.

• **Rules for** $\sim$, $\wedge$, $\vee$, $\Rightarrow$ **and** $\Leftrightarrow$: These connectives are always applied in the order listed.

Example 1.28.

1. $\mathrm{P} \Rightarrow \sim \mathrm{Q} \vee \mathrm{R} \Leftrightarrow \mathrm{S}$ is an abbreviation for $\big(\mathrm{P} \Rightarrow \big[(\sim \mathrm{Q}) \vee \mathrm{R}\big]\big) \Leftrightarrow \mathrm{S}$.
2. $\mathrm{P} \vee \sim \mathrm{Q} \Leftrightarrow \mathrm{R} \Rightarrow \mathrm{S}$ is an abbreviation for $\big[\mathrm{P} \vee (\sim \mathrm{Q})\big] \Leftrightarrow (\mathrm{R} \Rightarrow \mathrm{S})$.
3. $\mathrm{P} \Rightarrow \mathrm{Q} \Rightarrow \mathrm{R}$ is an abbreviation for $(\mathrm{P} \Rightarrow \mathrm{Q}) \Rightarrow \mathrm{R}$.

1.3 Quantified Statements

Definition 1.29. An ***open sentence*** is a sentence that contains variables. When P is an open sentence with a variable x (or variables $x_1, \cdots, x_n$), the sentence is symbolized by $\mathrm{P}(x)$ (or $\mathrm{P}(x_1, \cdots, x_n)$).

The ***truth set*** of an open sentence is the collection of variables (from a certain universe) that may be substituted to make the open sentence a true proposition.

Remark 1.30.

1. In general, an open sentence is not a proposition. It can be true or false depending on the value of variables.
2. The truth set of an open sentence $\mathrm{P}(x)$ depends on the universe where x belongs to. For example, suppose that $\mathrm{P}(x)$ is the open sentence $x^2 + 1 = 0$. If the universe is $\mathbb{R}$, then $\mathrm{P}(x)$ is false for all x (in the universe). On the other hand, if the universe is $\mathbb{C}$, the complex plane, then $\mathrm{P}(x)$ is true when $x = \pm i$ (which also implies that the truth set for $\mathrm{P}(x)$ is $\{i, -i\}$).

Example 1.31. Let $\mathrm{P}(x)$ be the open sentence "x is a prime number between 5060 and 5090". In this open sentence, the universe is usually chosen to be $\mathbb{N}$, the natural number system, and the truth set for $\mathrm{P}(x)$ is $\{5077, 5081, 5087\}$.

Definition 1.32. With a universe X specified, two open sentences $\mathrm{P}(x)$ and $\mathrm{Q}(x)$ are equivalent if they have the same truth set for all $x \in X$.

Example 1.33. The two sentences "$3x + 2 = 20$" and "$2x - 7 = 5$" are equivalent open sentences in any of the number system, such as $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

Example 1.34. The two sentences "$x^2 - 1 > 0$" and "$(x < -1) \vee (x > 1)$" are equivalent open sentences in $\mathbb{R}$.

Given an open sentence $\mathrm{P}(x)$, the first question that we should ask ourself is "whether the truth set of $\mathrm{P}(x)$ is empty or not".

Definition 1.35. The symbol $\exists$ is called the ***existential quantifier***. For an open sentence $\mathrm{P}(x)$, the sentence $(\exists x)\mathrm{P}(x)$ is read "there exists x such that $\mathrm{P}(x)$" or "for some x, $\mathrm{P}(x)$". The sentence $(\exists x)\mathrm{P}(x)$ is true if the truth set of $\mathrm{P}(x)$ is non-empty.

Remark 1.36. An open sentence $\mathrm{P}(x)$ does not have a truth value, but the quantified sentence $(\exists x)\mathrm{P}(x)$ does.

Example 1.37. The quantified sentence $(\exists\, x)(x^7 - 12x^3 + 16x - 3 = 0)$ is true in the universe of real numbers.

Example 1.38. The quantified sentence $(\exists\, n)(2^{2^n} + 1$ is a prime number$)$ is true in the universe of natural numbers.

Example 1.39. The quantified sentence

$$(\exists\, x, y, z, n)(x^n + y^n = z^n \wedge n \geqslant 3)$$

is true in the universe of integers, but is false in the universe of natural numbers.

Definition 1.40. The symbol $\forall$ is called the ***universal quantifier***. For an open sentence $\mathrm{P}(x)$, the sentence $(\forall\, x)\mathrm{P}(x)$ is read "for all x, $\mathrm{P}(x)$", "for every x, $\mathrm{P}(x)$" or "for every given x (in the universe), $\mathrm{P}(x)$". The sentence $(\forall\, x)\mathrm{P}(x)$ is true if the truth set of $\mathrm{P}(x)$ is the entire universe.

Example 1.41. The quantified sentence $(\forall\, n)(2^{2^n} + 1$ is a prime number$)$ is false in the universe of natural numbers since

$$2^{2^6} + 1 = 641 \times 6700417\,.$$

Remark 1.42. In general, statements of the form "every element of the set A has the property P" and "some element of the set A has property P" may be symbolized as $(\forall\, x \in A)\mathrm{P}(x)$ and $(\exists\, x \in A)\mathrm{P}(x)$, respective. Moreover,

1. "All $\mathrm{P}(x)$ are $\mathrm{Q}(x)$" (所有滿足 P 的 x 都滿足 Q or 只要滿足 P 的 x 就滿足 Q) should be symbolized as "$(\forall\, x)\big(\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)\big)$".

   To see why the sentence should be symbolized like that, we use A and B to denote the truth set of $\mathrm{P}(x)$ and the truth set of $\mathrm{Q}(x)$, respectively. Then "All $\mathrm{P}(x)$ are $\mathrm{Q}(x)$" implies that $A \subseteq B$; that is, if x in A, then x in B. Therefore, by reading the truth table

$x \in A$	$x \in B$	$\mathrm{P}(x)$	$\mathrm{Q}(x)$	$\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)$
T	T	T	T	T
T	F	T	F	F
F	T	F	T	T
F	F	F	F	T

we find that the truth set of the open sentence $\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)$ is the whole universe since the second case $(x \in A) \wedge (x \in B)$ cannot happen.

2. "Some $\mathrm{P}(x)$ are $\mathrm{Q}(x)$" (有些满足 P 的 x 也满足 Q or 有些 x 同時满足 P 和 Q) should be symbolized as "$(\exists\, x)\big(\mathrm{P}(x) \wedge \mathrm{Q}(x)\big)$".

Example 1.43.

1. The sentence "for every odd prime x less than 10, $x^2 + 4$ is prime" can be symbolized as
$$(\forall\, x)\big[(x \text{ is odd}) \wedge (x \text{ is prime}) \wedge (x < 10) \Rightarrow (x^2 + 4 \text{ is prime})\big]\,.$$

2. The sentence "for every rational number there is a larger integer" can be symbolized as
$$(\forall\, x \in \mathbb{Q})\big[(\exists\, z \in \mathbb{Z})(z > x)\big]\,.$$

3. The sentence "some functions defined at 0 are not continuous at 0" can be symbolized as
$$(\exists\, f)\big[(f \text{ is defined at } 0) \wedge (f \text{ is not continuous at } 0)\big]\,.$$

4. The sentence "some integers are even and some integers are odd" can be symbolized as
$$(\exists\, x)(x \text{ is even}) \wedge (\exists\, y)(y \text{ is odd})\,.$$

5. The sentence "some real numbers have a multiplicative inverse (乘法反元素)" can be symbolized as
$$(\exists\, x \in \mathbb{R})\big[(\exists\, y \in \mathbb{R})(xy = 1)\big]\,.$$

To symbolized the sentence "any real numbers have an additive inverse (加法反元素)", it is required that we combine the use of the universal quantifier and the existential quantifier:

$$(\forall\ x \in \mathbb{R})\big[(\exists\, y \in \mathbb{R})(x + y = 0)\big]\,.$$

This is in fact quite common in mathematical statement. Another example is the sentence "some real number does not have a multiplicative inverse" which can be symbolized by

$$(\exists x \in \mathbb{R}) \sim \big[(\exists\, y \in \mathbb{R})(xy = 1)\big]$$

or simply

$$(\exists\, x \in \mathbb{R})\big[(\forall\, y \in \mathbb{R})(xy \neq 1)\big]\,.$$

Example 1.44 (Continuity of functions)**.** By the definition of continuity and using the logic symbol, f is continuous at a number c if

$$\underbrace{(\forall\,\varepsilon)\,(\exists\delta)\,\underbrace{(\forall\,x)\big[(|x-c|<\delta)\Rightarrow(|f\,(x)-f\,(c)|<\varepsilon)\big]}_{\mathrm{Q}(\varepsilon,\delta)}}_{\mathrm{P}(\varepsilon)\equiv(\exists\,\delta)\mathrm{Q}(\varepsilon,\delta)}\,.$$

1. The universe for the variables ε and δ is the collection of positive real numbers. Therefore, sometimes we write

$$(\forall\,\varepsilon>0)(\exists\,\delta>0)(\forall\,x)\big[(|x-c|<\delta)\Rightarrow(|f\,(x)-f\,(c)|<\varepsilon)\big]\,.$$

2. The sentence $\mathrm{P}(\varepsilon)\equiv(\exists\,\delta)\mathrm{Q}(\varepsilon,\delta)$ is always true for any $\varepsilon>0$.

3. Suppose ε is a given positive number. Then the truth set for $\mathrm{Q}(\varepsilon,\delta)$ is non-empty which implies that "there is at least one positive number δ making the sentence $\mathrm{Q}(\varepsilon,\delta)$ true".

Definition 1.45. Two quantified statement are equivalent in a given universe if they have the same truth value in that universe. Two quantified sentences are equivalent if they are equivalent in every universe.

Theorem 1.46. *If* $\mathrm{P}(x)$ *is an open sentence with variable* x*, then*

(a) $\sim(\forall\,x)\mathrm{P}(x)$ *is equivalent to* $(\exists\,x)\sim\mathrm{P}(x)$.

(b) $\sim(\exists\,x)\mathrm{P}(x)$ *is equivalent to* $(\forall\,x)\sim\mathrm{P}(x)$.

Proof. Let X be the universe, and A be the truth set of the open sentence $\mathrm{P}(x)$.

1. The sentence $(\forall\,x)\mathrm{P}(x)$ is true if and only if $A=X$; thus $\sim(\forall\,x)\mathrm{P}(x)$ is true if and only if $A\neq X$. On the other hand, the sentence $(\exists\,x)\sim\mathrm{P}(x)$ is true if and only if the truth set of $\sim\mathrm{P}(x)$ is non-empty; thus $(\exists\,x)\sim\mathrm{P}(x)$ is true if and only if $A\neq X$.

2. Using (a) and the double negation law, $(\exists\,x)\mathrm{P}(x)$ is equivalent to $\sim\big((\forall\,x)\sim\mathrm{P}(x)\big)$; thus

$$\sim(\exists\,x)\mathrm{P}(x)\;\Leftrightarrow\sim\big[\sim\big((\forall\,x)\sim\mathrm{P}(x)\big)\big]\;\Leftrightarrow\;(\forall\,x)\sim\mathrm{P}(x)\,.$$

□

Corollary 1.47.

1. *If* $\mathrm{P}(x,y,z)$ *and* $\mathrm{Q}(x,y,z)$ *are open sentences with variables* x*,* y *and* z*, then the quantified sentence* $\sim\big[(\forall\,x)(\exists\,y)(\forall\,z)\big(\mathrm{P}(x,y,z)\Rightarrow\mathrm{Q}(x,y,z)\big)\big]$ *is equivalent to* $(\exists\,x)(\forall\,y)(\exists\,z)\big(\mathrm{P}(x,y,z)\wedge\sim\mathrm{Q}(x,y,z)\big)$.

2. *If* $\mathrm{P}(x_1,x_2,x_3,x_4)$ *and* $\mathrm{Q}(x_1,x_2,x_3,x_4)$ *are open sentences with variables* x_1*,* x_2*,* x_3 *and* x_4*, then the quantified sentence* $\sim\big[(\exists\,x_1)(\forall\,x_2)(\exists\,x_3)(\forall\,x_4)\big(\mathrm{P}(x_1,x_2,x_3,x_4)\Rightarrow\mathrm{Q}(x_1,x_2,x_3,x_4)\big)\big]$ *is equivalent to* $(\forall\,x_1)(\exists\,x_2)(\forall\,x_3)(\exists\,x_4)\big(\mathrm{P}(x_1,x_2,x_3,x_4)\wedge\sim\mathrm{Q}(x_1,x_2,x_3,x_4)\big)$.

Example 1.48 (Discontinuity of functions)**.** A function f is continuous at c if and only if

$$(\forall\,\varepsilon>0)(\exists\,\delta>0)(\forall\,x)\big[(|x-c|<\delta)\Rightarrow\big(\big|f\,(x)-f\,(c)\big|<\varepsilon\big)\big]\,.$$

Therefore, f is not continuous at c if and only if

$$(\exists\,\varepsilon>0)(\forall\,\delta>0)(\exists\,x)\big[(|x-c|<\delta)\wedge\big(\big|f\,(x)-f\,(c)\big|\geqslant\varepsilon\big)\big]\,.$$

解讀：f 在 c 不連續，則存在一個正數 ε 使得任意正數 δ 所定義的開區間 $(c-\delta,c+\delta)$ 中有 x 會滿足 $\big|f\,(x)-f\,(c)\big|\geqslant\varepsilon$。

Example 1.49 (Non-existence of limits)**.** A function f defined on an interval containing c, except possibly at c, is said to have a limit at c $\big($or $\lim\limits_{x\to c}f(x)$ exists$\big)$ if and only if

$$(\exists\,L\in\mathbb{R})(\forall\,\varepsilon>0)(\exists\,\delta>0)(\forall\,x)\big((0<|x-c|<\delta)\Rightarrow(|f\,(x)-L|<\varepsilon)\big)\,.$$

Therefore, f does not have a limit at c if and only if

$$(\forall\,L\in\mathbb{R})(\exists\,\varepsilon>0)(\forall\,\delta>0)(\exists\,x)\big((0<|x-c|<\delta)\wedge(|f\,(x)-L|\geqslant\varepsilon)\big)\,.$$

解讀：若 f 在 c 極限不存在，則不管對哪個（可能的極限）實數 L 都可以找到一個正數 ε，使得任意正數 δ 所定義的去中心區域 $(c-\delta,c)\cup(c,c+\delta)$ 中都有 x 會滿足 $|f\,(x)-L|\geqslant\varepsilon$。

Definition 1.50. The symbol $\exists!$ is called the ***unique existential quantifier***. For an open sentence $\mathrm{P}(x)$, then sentence $(\exists!x)\mathrm{P}(x)$ is read "there is a unique x such that $\mathrm{P}(x)$". The sentence $(\exists!x)\mathrm{P}(x)$ is true if the truth set of $\mathrm{P}(x)$ has exactly one element.

Theorem 1.51. *If* $\mathrm{P}(x)$ *is an open sentence with variable* x*, then*

(a) $(\exists!x)\mathrm{P}(x)\Rightarrow(\exists x)\mathrm{P}(x)$.

(b) $(\exists!x)\mathrm{P}(x)\Leftrightarrow\big[\big((\exists x)\mathrm{P}(x)\big)\wedge\big((\forall\,y)(\forall\,z)(\mathrm{P}(y)\wedge\mathrm{P}(z)\Rightarrow y=z)\big)\big]$.

1.4 Basic Proof Methods I (Direct Proof)

Mathematical Theorem: A statement that describes a pattern or relationship among quantities or structures, usually of the form $\mathrm{P}\Rightarrow\mathrm{Q}$.
Proofs of a Theorem: Justifications of the truth of the theorem that follows the principle of logic.
Lemma: A result that serves as a preliminary step to prove the main theorem.
Axiom (公設): Some facts that are used to develop certain theory and **cannot** be proved.
Undefined terms: Not everything can/have to be defined, and we have to treat them as known.

Remark 1.52. 1. To validate a conditional sentence $\mathrm{P}\Rightarrow\mathrm{Q}$, by definition you only need to shown that there is **no** chance that P is true but at the same time Q is false. Therefore, you often show that if P is true then Q is true, if Q is false then P is false or that P is true and Q is false leads to a contradiction (always false).

2. Sometimes it is difficult to identify the antecedent of a mathematical theorem. Usually it is because the antecedent is too trivial to be stated. For example, "$\sqrt{2}$ is an irrational number" is a mathematical theorem and it can be understood as "**if you know what an irrational number is**, then $\sqrt{2}$ is an irrational number".

• **General format of proving** P ⇒ Q **directly**:

> **Direct proof of** P ⇒ Q
> **Proof.**
> Assume P. (可用很多方式取代，主要是看 P 的內容)
> ⋮
> Therefore, Q.
> Thus, P ⇒ Q. □

Basic Rules: In any proof at any time you may

1. state an axiom (by the axiom of ⋯⋯), an assumption (assume that ⋯⋯), or a previously proved result (by the fact that ⋯⋯).
2. state a sentence whose symbolic translation is a tautology.
3. state a sentence (or use a definition) equivalent to any statement earlier in the proof.
4. use the *modus ponens rule*: after statements P and P ⇒ Q appear in a proof, state Q.

Example 1.53. Prove that if x is odd, then $x+1$ is even.

Proof. Assume that x is an odd number.
Then $x = 2k+1$ for some integer k; thus $x+1 = 2k+1+1 = 2(k+1)$ which shows that $x+1$ is a multiple of 2.
Therefore, $x+1$ is even. □

Example 1.54. Let a, b, c be integers. If a divides b and b divides c, then a divides c.

Proof. Let a, b, c be integers.
Assume that a divides b and b divides c.
Then $b = am$ for some integer m, and $c = bn$ for some integer n; thus $c = (am)n = a(mn)$ which shows that c is an multiple of a.
Therefore, a divides c. □

Alternative way of proving. Let a, b, c be integers.
Assume that a divides b. Then $b = am$ for some integer m.
Assume that b divides c. Then $c = bn$ for some integer n.
Thus, $c = (am)n = a(mn)$ which shows that c is an multiple of a.
Therefore, a divides c. □

Example 1.55. Show that $(\forall\, x \in \mathbb{R})(x^2 + 1 > 0)$.
翻譯成 $\mathrm{P} \Rightarrow \mathrm{Q}$ 的句型：**Show that if $x \in \mathbb{R}$, then $x^2 + 1 > 0$.**

Proof. Assume that x is a real number.
Then either $x > 0$, $x = 0$ or $x < 0$.

1. If $x > 0$, then $x^2 = x \cdot x > 0$.
2. If $x = 0$, then $x^2 = 0$.
3. If $x < 0$, then $(-x) > 0$; thus $x^2 = (-x) \cdot (-x) > 0$.

In either cases, $x^2 \geqslant 0$; thus $x^2 + 1 > 0$.
Therefore, $x^2 + 1 > 0$. □

Example 1.56. Show that $(\forall\, \varepsilon > 0)\left(\#\left\{n \in \mathbb{N} \,\middle|\, \frac{1}{n} > \varepsilon\right\} < \infty\right)$.
翻譯成 $\mathrm{P} \Rightarrow \mathrm{Q}$ 的句型：**Show that if $\varepsilon > 0$, then the collection $\left\{n \in \mathbb{N} \,\middle|\, \frac{1}{n} > \varepsilon\right\}$ has only finitely many elements.**

Proof. Assume that $\varepsilon > 0$. Then $\frac{1}{\varepsilon} < \infty$.
Note that $\left\{n \in \mathbb{N} \,\middle|\, \frac{1}{n} > \varepsilon\right\}$ is identical to the set $\left\{n \in \mathbb{N} \,\middle|\, n < \frac{1}{\varepsilon}\right\}$, while the later is the collection of natural numbers that are less than $\frac{1}{\varepsilon}$.
Therefore, $\#\left\{n \in \mathbb{N} \,\middle|\, \frac{1}{n} > \varepsilon\right\} \leqslant \frac{1}{\varepsilon} < \infty$. □

Example 1.57. Show that $(\forall\, x \in \mathbb{R})(\exists\, y \in \mathbb{R})(x + y = 0)$.
翻譯成 $\mathrm{P} \Rightarrow \mathrm{Q}$ 的句型：**Show that "if $x \in \mathbb{R}$, then the truth set of the open sentence $\mathrm{P}(y) \equiv (x + y = 0)$ is non-empty" or "if $x \in \mathbb{R}$, then there exists $y \in \mathbb{R}$ such that $x + y = 0$".**

Proof. Assume that x is a real number.
Then $y = -x$ is a real number and $x + y = 0$.
Thus, there exists $y \in \mathbb{R}$ such that $x + y = 0$.
Therefore, for each $x \in \mathbb{R}$, there exists $y \in \mathbb{R}$ such that $x + y = 0$. □

Remark 1.58. The sentence "Assume that x is a real number" in the proof above is often replaced by "Let x be a real number" or "Let $x \in \mathbb{R}$ be given".

1.5 Basic Proof Methods II (Indirect Proof)

Recall that a conditional sentence is equivalent to its contrapositive; that is,

$$(\mathrm{P} \Rightarrow \mathrm{Q}) \Leftrightarrow (\sim \mathrm{Q} \Rightarrow \sim \mathrm{P}).$$

Therefore, to prove the conditional sentence $\mathrm{P} \Rightarrow \mathrm{Q}$, one can instead prove that $\sim \mathrm{Q} \Rightarrow \sim \mathrm{P}$. This way of proving $\mathrm{P} \Rightarrow \mathrm{Q}$ is called "proved by contraposition".

• **General format of proving P ⇒ Q by contraposition**:

> **Proof of P ⇒ Q by Contraposition**
> **Proof.**
> Assume ∼Q. (可用很多方式取代，主要是看 ∼Q 的內容)
> ⋮
> Therefore, ∼P.
> Thus, ∼Q ⇒∼P.
> Therefore, P ⇒ Q. □

Example 1.59. Let m be an integer. Show that if m^2 is even, then m is even.

Proof. Assume (the contrary) that m is odd.
Then $m = 2k + 1$ for some integer k. Therefore, $m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ which is an odd number.
Thus, if m is odd, then m^2 is odd.
Therefore, if m^2 is even, then m is even. □

Example 1.60. Let x and y be real numbers such that $x < 2y$. Show that if $7xy \leqslant 3x^2 + 2y^2$, then $3x \leqslant y$.

Proof. Let x and y be real numbers such that $x < 2y$.
Assume the contrary that $3x > y$.
Then $2y - x > 0$ and $3x - y > 0$. Therefore, $(2y - x)(3x - y) > 0$. Expanding the expression, we find that $7xy - 3x^2 - 2y^2 > 0$. Therefore, $7xy > 3x^2 + 2y^2$.
Thus, if $3x > y$, then $7xy > 3x^2 + 2y^2$.
Therefore, if $7xy \leqslant 3x^2 + 2y^2$, then $3x \leqslant y$. □

• **General format of proving P ⇒ Q by contradiction**:

> **Proof of P ⇒ Q by Contradiction**
> **Proof.**
> Assume P and ∼Q. (可用很多方式取代，主要是看 P 與 ∼Q 的內容)
> ⋮
> Therefore, ∼P.
> Thus, P∧∼P, a contradiction.
> Therefore, P ⇒ Q. □

or simply

> **Proof of P ⇒ Q by Contradiction**
> **Proof.**
> Assume P and ∼Q. (可用很多方式取代，主要是看 P 與 ∼Q 的內容)
> ⋮
> Therefore, ∼P, a contradiction.
> Therefore, P ⇒ Q. □

As mentioned before, there are cases that the antecedent of a theorem is unclear. This kind of theorems are of the form Q.

• **General format of proving Q by contradiction**:

Proof of Q by Contradiction
Proof.
Assume $\sim$Q. (可用很多方式取代，主要是看 $\sim$Q 的內容)
⋮ (通常是敘述公設或是定義的過程)
Therefore, P.
⋮ (由 P$\wedge\sim$Q 進行邏輯推演)
Therefore, $\sim$P.
Thus, P$\wedge\sim$P, a contradiction.
Therefore, P $\Rightarrow$ Q. □

Example 1.61. Show that $\sqrt{2}$ is an irrational number.

Proof. Assume (the contrary) that $\sqrt{2}$ is a rational number.
Then $\sqrt{2} = \frac{q}{p}$ for some positive integers p, q satisfying $(p, q) = 1$. Thus, q^2 is an even number since $q^2 = 2p^2$. By Example 1.59, q is even; thus $q = 2k$ for some integer k. Then p^2 is an even number since $p^2 = \frac{q^2}{2} = 2k^2$. Example 1.59 again implies that p is an even number.
Thus, $(p, q) \neq 1$, a contradiction.
Therefore, $\sqrt{2}$ is an irrational number. □

Example 1.62. Show that the collection of primes is infinite.

Proof. Assume the contrary that there are only finitely many primes.
Suppose that $p_1 < p_2 < \cdots < p_k$ are all the prime numbers. Let $n = p_1 p_2 \cdots p_k + 1$. Then $n > p_k$ and n is not a prime. Therefore, n has a prime divisor (質因數) q; that is, q is a prime and $q|n$. Since q is a prime, $q = p_j$ for some $1 \leqslant j \leqslant k$.
However, $q = p_j$ does not divide n, a contradiction.
Therefore, the collection of primes is infinite. □

Example 1.63. There are n people ($n \geqslant 2$) at a party, some of whom are friends. Prove that there exists someone at the party who is friends with the same number of party-goers as another person.
中文解釋：證明在一個宴會中，至少有兩個人在宴會中的朋友數一樣多。

Proof. Assume the contrary that no two party-goers have the same number of friends. Note that the number of friends should range from 0 to $n-1$; thus by the assumption that no two party-goers have the same number of friends, there must be one party-goer who has no friend, while there must be one party-goer who has $n-1$ friends. This is impossible because the one who has $n-1$ friends is a friend of the one who has no friend. □

Some mathematical theorems are of the form $\mathrm{P} \Leftrightarrow \mathrm{Q}$. As explained before, this means $\mathrm{P} \Rightarrow \mathrm{Q}$ and $\mathrm{Q} \Rightarrow \mathrm{P}$; thus one should establish these two implication separately.

• **General format of proving** $\mathrm{P} \Leftrightarrow \mathrm{Q}$:

> **Proof of** $\mathrm{P} \Leftrightarrow \mathrm{Q}$
> **Proof.**
> (i) Show that $\mathrm{P} \Rightarrow \mathrm{Q}$ using the methods mentioned above.
> (ii) Show that $\mathrm{Q} \Rightarrow \mathrm{P}$ using the methods mentioned above.
> Therefore, $\mathrm{P} \Leftrightarrow \mathrm{Q}$. □

Example 1.64. Let m, n be integers. Show that m and n have the same parity (同奇同偶) if and only if $m^2 + n^2$ is even.

Proof. ($\Rightarrow$) If m and n are both even, then $m = 2k$ and $n = 2\ell$ for some integers k and ℓ. Therefore, $m^2 + n^2 = 2(2k^2 + 2\ell^2)$ which is even. If m and n are both odd, then $m = 2k+1$ and $n = 2\ell+1$ for some integers k and ℓ. Therefore, $m^2 + n^2 = 2(2k^2 + 2\ell^2 + 2k + 2\ell + 1)$ which is even. Therefore, if m and n have the same parity, $m^2 + n^2$ is even.

($\Leftarrow$) Assume the contrary that there are m and n having opposite parity. W.L.O.G. we can assume that m is even and n is odd. Then $m = 2k$ and $n = 2\ell+1$ for some integers k and ℓ. Therefore, $m^2 + n^2 = 2(2k^2 + 2\ell^2 + 2\ell) + 1$ which is odd. Thus, if m and n have opposite parity, then $m^2 + n^2$ is odd. Therefore, if $m^2 + n^2$ is even, then m and n have the same parity. □

Remark 1.65. 1. Sometimes it requires intermediate equivalent proposition to show $\mathrm{P} \Leftrightarrow \mathrm{Q}$; that is, one might establish

$$(\mathrm{P} \Leftrightarrow \mathrm{R}_1) \wedge (\mathrm{R}_1 \wedge \mathrm{R}_2) \wedge \cdots \wedge (\mathrm{R}_{n-1} \Leftrightarrow \mathrm{R}_n) \wedge (\mathrm{R}_n \Leftrightarrow \mathrm{Q})$$

to prove $\mathrm{P} \Leftrightarrow \mathrm{Q}$.

2. Often times it is more efficient to show a theorem of the form "$\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_n$ are equivalent" (which means $\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_n$ have the same truth value) by showing that $\mathrm{P}_1 \Rightarrow \mathrm{P}_2$, $\mathrm{P}_2 \Rightarrow \mathrm{P}_3$, $\cdots$, and $\mathrm{P}_n \Rightarrow \mathrm{P}_1$. In other words, one uses the following relation

$$\big[(\mathrm{P}_1 \Leftrightarrow \mathrm{P}_2) \wedge (\mathrm{P}_2 \Leftrightarrow \mathrm{P}_3) \wedge \cdots \wedge (\mathrm{P}_{n-1} \Leftrightarrow \mathrm{P}_n)\big] \Leftrightarrow \big[(\mathrm{P}_1 \Rightarrow \mathrm{P}_2) \wedge (\mathrm{P}_2 \Rightarrow \mathrm{P}_3) \wedge \cdots \wedge (\mathrm{P}_n \Rightarrow \mathrm{P}_1)\big]$$

to prove this kind of theorems.

Example 1.66. Let x, y be non-negative real numbers such that $x - 4y < y - 3x$. Prove that if $3x > 2y$, then $12x^2 + 10y^2 < 24xy$.

Direct proof. Let x, y be non-negative real numbers such that $x - 4y < y - 3x$. Suppose that $3x > 2y$. Then $4x - 5y < 0$ and $3x - 2y > 0$. Therefore,

$$0 > (4x - 5y)(3x - 2y) = 12x^2 + 10y^2 - 23xy$$

or equivalently, $12x^2 + 10y^2 < 23xy$. Since x, y are non-negative real numbers, $23xy \leqslant 24xy$; thus $12x^2 + 10y^2 < 24xy$. □

Proof by contraposition. Let x, y be non-negative real numbers such that $x-4y < y-3x$. Assume the contrary that $12x^2 + 10y^2 \geqslant 24xy$. Since x, y are non-negative real numbers,

$$12x^2 + 10y^2 \geqslant 24xy \geqslant 23xy\,;$$

thus $(4x - 5y)(3x - 2y) = 12x^2 + 10y^2 - 23xy \geqslant 0$. Since $x - 4y < y - 3x$, we find that $4x - 5y < 0$; thus $3x - 2y \leqslant 0$. □

Proof by contradiction. Let x, y be non-negative real numbers such that $x-4y < y-3x$. Assume that $3x > 2y$ and $12x^2 + 10y^2 \geqslant 24xy$. Then $4x - 5y < 0$ and $3x - 2y > 0$; thus

$$0 > (4x - 5y)(3x - 2y) = 12x^2 + 8y^2 - 23xy \geqslant 24xy - 23xy = xy \geqslant 0\,,$$

where the last inequality follows from the fact that x, y are non-negative real numbers. Thus, we reach a contradiction $0 > 0$. □

1.6 Proofs Involving Quantifiers

- **General format of proving $(\forall\, x)\mathrm{P}(x)$ directly**:

  Note that to establish $(\forall\, x)\mathrm{P}(x)$ is the same as proving that "if x is in the universe, then $\mathrm{P}(x)$ is true".

> **Direct Proof of $(\forall\, x)\mathrm{P}(x)$**
> **Proof.**
> Let x be given in the universe. (可用很多方式取代，主要是看宇集是什麼)
> ⋮
> Hence $\mathrm{P}(x)$ is true.
> Therefore, $(\forall\, x)\mathrm{P}(x)$ is true. □

- **General format of proving $(\forall\, x)\mathrm{P}(x)$ by contradiction**:

  To prove "if x is in the universe, then $\mathrm{P}(x)$ is true" by contradiction is to show that "an x in the universe so that $\mathrm{P}(x)$ is false leads to a contradiction".

> **Proof of $(\forall\, x)\mathrm{P}(x)$ by contradiction**
> **Proof.**
> Assume (the contrary) that $\sim(\forall\, x)\mathrm{P}(x)$.
> Then $(\exists\, x) \sim \mathrm{P}(x)$.
> Let x be an element in the universe such that $\sim \mathrm{P}(x)$.
> ⋮
> Therefore, $\mathrm{Q} \wedge \sim \mathrm{Q}$, a contradiction.
> Thus $(\exists\, x) \sim \mathrm{P}(x)$ is false, so $(\forall\, x)\mathrm{P}(x)$ is true. □

or simply

Proof of $(\forall\, x)\mathrm{P}(x)$ by contradiction
Proof.
Assume (the contrary) that $(\exists\, x) \sim \mathrm{P}(x)$.
Let x be an element in the universe such that $\sim \mathrm{P}(x)$.
$\vdots$
Therefore, $\mathrm{Q} \wedge \sim \mathrm{Q}$, a contradiction.
Thus $(\exists\, x) \sim \mathrm{P}(x)$ is false, so $(\forall\, x)\mathrm{P}(x)$ is true. □

Example 1.67. Show that for all $x \in \left(0, \frac{\pi}{2}\right)$, $\sin x + \cos x > 1$.

Proof. Assume that there exists $x \in \left(0, \frac{\pi}{2}\right)$ such that $\sin x + \cos x \leqslant 1$. Then $0 < \sin x + \cos x \leqslant 1$; thus

$$0 < (\sin x + \cos x)^2 \leqslant 1\,.$$

Expanding the square and using the identity $\sin^2 x + \cos^2 x = 1$, we find that

$$0 < 1 + 2\sin x \cos x \leqslant 1$$

which shows $\sin x \cos x \leqslant 0$. On the other hand, since $x \in \left(0, \frac{\pi}{2}\right)$, we have $\sin x > 0$ and $\cos x > 0$ so that $\sin x \cos x > 0$, a contradiction.
Therefore, $\sin x + \cos x > 1$ for all $x \in \left(0, \frac{\pi}{2}\right)$. □

- **General format of proving $(\exists\, x)\mathrm{P}(x)$ directly**: Method 1.

The easiest way to show that $(\exists\, x)\mathrm{P}(x)$ is to give a precise x in the universe and show that $\mathrm{P}(x)$ is true; however, this usually requires that you make some effort to find out which x suits this requirement.

Constructive Proof of $(\exists\, x)\mathrm{P}(x)$
Proof.
Specify one particular element a.
If necessary, verify that a is in the universe.
$\vdots$
Therefore, $\mathrm{P}(a)$ is true.
Thus $(\exists\, x)\mathrm{P}(x)$ is true. □

Example 1.68. Show that between two different rational numbers there is a rational number.
翻譯成數學語言，即證明 "If $a, b \in \mathbb{Q}$ and $a < b$, then there exists $c \in \mathbb{Q}$ such that $a < c < b$".

Proof. Let a, b be rational numbers and $a < b$. Let $c = \dfrac{a+b}{2}$. Then $c \in \mathbb{Q}$ and $a < c < b$. □

Example 1.69. Show that there exists a natural number whose fourth power is the sum of other three fourth power.

Proof. 20615693 is one such number because it is a natural number and

$$20615673^4 = 2682440^4 + 1536539^4 + 18796760^4\,.$$ □

• **General format of proving $(\exists\, x)\mathrm{P}(x)$ directly: Method 2.**

To show $(\exists\, x)\mathrm{P}(x)$, often times it is almost impossible to provide a precise x so that $\mathrm{P}(x)$ is true. Proving $(\exists\, x)\mathrm{P}(x)$ directly (not proving by contradiction) then usually requires a lot of abstract steps.

Non-Constructive Proof of $(\exists\, x)\mathrm{P}(x)$
Proof.
$\vdots$
Therefore, $\mathrm{P}(a)$ is true.
Thus $(\exists\, x)\mathrm{P}(x)$ is true. □

Example 1.70. Let $f : [0,1] \to [0,1]$ be continuous. Show that $(\exists\, x \in [0,1])\big(x = f(x)\big)$.

Proof. 1. If $f(0) = 0$, then $(\exists\, x \in [0,1])\big(x = f(x)\big)$.

2. If $f(0) \neq 0$ and $f(1) \neq 1$, then $0 < f(0), f(1) < 1$. Define $g : [0,1] \to \mathbb{R}$ by $g(x) = x - f(x)$. Then g is continuous on $[0,1]$. Moreover, $g(0) < 0$ and $g(1) > 0$. Thus, the intermediate value theorem implies that there exists x such that $0 < x < 1$ and $g(x) = 0$ (which is the same as $x = f(x)$).

In either cases, there exists $x \in [0,1]$ such that $x = f(x)$. □

• **General format of proving $(\exists\, x)\mathrm{P}(x)$ by contradiction**:

Proof of $(\exists\, x)\mathrm{P}(x)$ by contradiction
Proof.
Suppose the contrary that $\sim(\exists\, x)\mathrm{P}(x)$.
If necessary, verify that a is in the universe.
$\vdots$
Therefore, $\mathrm{P}(a)$ is true.
Thus $(\exists\, x)\mathrm{P}(x)$ is true. □

Example 1.71. Let S be a set of 6 positive integers, each less than or equal to 10. Prove that there exists a pair of integers in S whose sum is 11.

Proof. Suppose the contrary that every pair of integers in S has a sum different from 11. Then S contains at most one element from each of the sets $\{1,10\}$, $\{2,9\}$, $\{3,8\}$, $\{4,7\}$ and $\{5,6\}$. Thus, S contains at most 5 elements, a contradiction. We conclude that S contains a pair of numbers whose sum in 11. □

• **General format of proving $(\exists\, !x)\mathrm{P}(x)$**:

Proof of $(\exists\, !x)\mathrm{P}(x)$
Proof.
(i) Prove that $(\exists\, x)\mathrm{P}(x)$ is true using the methods mentioned above.
(ii) Prove that $(\forall\, y)(\forall\, z)\big[\big(P(y) \wedge P(z)\big) \Rightarrow (y = z)\big]$:
Assume that y and z are elements in the universe such that $\mathrm{P}(y)$ and $\mathrm{P}(z)$ are true.
$\vdots$
Therefore, $y = z$.
From (i) and (ii) we conclude that $(\exists\, !x)\mathrm{P}(x)$ is true. □

Example 1.72. Prove that every non-zero real number has a unique multiplicative inverse.

Proof. Let x be a non-zero real number.

1. Let $y = \dfrac{1}{x}$. Since $x \neq 0$, y is a real number. Moreover, $xy = 1$; thus $(\exists\, y \in \mathbb{R})(xy = 1)$.
2. Suppose that y and z are real numbers such that $xy = xz = 1$. Then $x(y - z) = xy - xz = 0$. By the fact that $x \neq 0$, we must have $y = z$.

Therefore, $(\forall\, x \neq 0)(\exists\, !y)(xy = 1)$. □

Some manipulations of quantifiers that permit valid deductions:

$$(\forall\, x)(\forall\, y)\mathrm{P}(x, y) \Leftrightarrow (\forall\, y)(\forall\, x)\mathrm{P}(x, y)\,, \tag{1.1a}$$

$$(\exists\, x)(\exists\, y)\mathrm{P}(x, y) \Leftrightarrow (\exists\, y)(\exists\, x)\mathrm{P}(x, y)\,, \tag{1.1b}$$

$$(\forall\, x)\mathrm{P}(x) \vee (\forall\, x)\mathrm{Q}(x) \Rightarrow (\forall\, x)\big[\mathrm{P}(x) \vee \mathrm{Q}(x)\big]\,, \tag{1.1c}$$

$$(\forall\, x)\big[\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)\big] \Rightarrow \big[(\forall\, x)\mathrm{P}(x) \Rightarrow (\forall\, x)\mathrm{Q}(x)\big]\,, \tag{1.1d}$$

$$(\forall\, x)\big[\mathrm{P}(x) \wedge \mathrm{Q}(x)\big] \Leftrightarrow \big[(\forall\, x)\mathrm{P}(x) \wedge (\forall\, x)\mathrm{Q}(x)\big]\,, \tag{1.1e}$$

$$(\exists\, x)(\forall\, y)\mathrm{P}(x, y) \Rightarrow (\forall\, y)(\exists\, x)\mathrm{P}(x, y)\,. \tag{1.1f}$$

Counter-examples for the non-equivalence in (1.1c), (1.1d) and (1.1f):

1. the "if" direction in (1.1c): Let the universe be all the integers, $\mathrm{P}(x)$ be the statement "x is an even number" and $\mathrm{Q}(x)$ be the statement "x is an odd number". Then clearly $(\forall\, x)\big[\mathrm{P}(x) \vee \mathrm{Q}(x)\big]$ but we do not have $(\forall\, x)\mathrm{P}(x) \vee (\forall\, x)\mathrm{Q}(x)$.
2. the "if" direction in (1.1d): Let the universe be all the animals, $\mathrm{P}(x)$ be the statement "x has wings" and $\mathrm{Q}(x)$ be the statement "x is a bird". Then clearly the implication $\big[(\forall\, x)\mathrm{P}(x) \Rightarrow (\forall\, x)\mathrm{Q}(x)\big]$ is true (since the antecedent is false) while the statement $(\forall\, x)\big[\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)\big]$ is false.
3. the "if" direction in (1.1f): Let the universe be all the non-negative real numbers, and $\mathrm{P}(x, y)$ be the statement "$y = x^2$". Clearly $(\forall\, y)(\exists\, x)\mathrm{P}(x, y)$ but we do not have $(\exists\, x)(\forall\, y)\mathrm{P}(x, y)$.

1.7 Strategies for Constructing Proofs

Summary of strategies you should try when you begin to write a proof:

1. **Understand the statement to be proved**: make sure you know the **definitions** of all terms that appear in the statement.
2. **Identify the assumption(s) and the conclusion**, and **determine the logical form of the statement**.

3. **Look for the key ideas**: Ask yourself what is needed to reach the conclusion. Find relationships among the terms, the equations, and formulas involved. Recall known facts and previous results about the antecedent and consequence.

- Proof of $(\mathrm{P} \Rightarrow \mathrm{Q}_1 \vee \mathrm{Q}_2)$: Note that

$$(\mathrm{P} \Rightarrow \mathrm{Q}_1 \vee \mathrm{Q}_2) \;\Leftrightarrow\; \big[(\mathrm{P} \wedge \sim \mathrm{Q}_1) \Rightarrow \mathrm{Q}_2\big].$$

Example 1.73. If (x, y) is inside the circle $(x-6)^2 + (y-3)^3 = 8$, then $x > 4$ or $y > 1$.

Proof. Suppose that (x, y) is inside the circle $(x-6)^2+(y-3)^2 = 8$ and $x \leqslant 4$. Then $(x-6)^2+(y-3)^2 < 8$ and $6 - x \geqslant 2$. Therefore,

$$(y-3)^2 < 8 - (6-x)^2 \leqslant 8 - 4 = 4$$

which implies that $|y-3| < 2$; thus $-2 < y - 3 < 2$ which further shows $1 < y < 5$. □

1.8 Proofs from Number Theory

Theorem 1.74 (The Division Algorithm)**.** *For all integers a and b, with $a \neq 0$, there exist unique integer q and r such that $b = aq + r$ and $0 \leqslant r < |a|$.*

1. The integer a is the **divisor** (除數), b is the **divident** (被除數), q is the **quotient** (商), and r is the **remainder** (餘數).
2. a is said to divide b if $b = aq$ for some integer q.
3. A **common divisor** (公因數) of nonzero integers a and b is an integer that divides both a and b.

Definition 1.75. Let a and b be non-zero integers. We say the integer d is the **greatest common divisor (gcd)** of a and b, and write $d = \gcd(a, b)$, if

1. d is a common divisor of a and b.
2. every common divisor c of a and b is not greater than d.

Theorem 1.76. *Let a and b be non-zero integers. The gcd of a and b is the smallest positive linear combination of a and b; that is,*

$$\gcd(a, b) = \min\big\{am + bn \,\big|\, am + bn > 0\,, m, n \in \mathbb{Z}\big\}\,.$$

Proof. Let $d = am + bn$ be the smallest positive linear combination of a and b. We show that d satisfies (1) and (2) in the definition of the greatest common divisor.

1. **First we show that d divides a.** By the Division Algorithm, there exist integers q and r such that $a = dq + r$, where $0 \leqslant r < d$. Then

$$r = a - dq = a - (am + bn)q = a(1 - m) + b(-nq)\,;$$

thus r is a linear combination of a and b. Since $0 \leqslant r < d$ and d is the smallest positive linear combination, we must have $r = 0$. Therefore, $a = dq$; thus d divides a. Similarly, d divides b (replacing a by b in the argument above); thus d is a common divisor of a and b.

2. **Next we show that all common divisors of a and b is not greater than d.** Let c be a common divisor of a and b. Then c divides d since $d = am + bn$. Therefore, $c \leqslant d$.

By (1) and (2), we find that $d = \gcd(a, b)$. ▫

Theorem 1.77 (Euclid's Algorithm (輾轉相除法))**.** *Let a and b be positive integers with $a \leqslant b$. Then there are two lists of positive integers $q_1, q_2, \cdots, q_{k-1}, q_k, q_{k+1}$ and $r_1, r_2, \cdots, r_{k-1}, r_k, r_{k+1}$ such that*

1. $a > r_1 > r_2 > \cdots > r_{k-1} > r_k > r_{k+1} = 0$.
2. $b = aq_1 + r_1$, $a = r_1q_2 + r_2$, $r_1 = r_2q_3 + r_3$, $\cdots$, $r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}$, $r_{k-2} = r_{k-1}q_k + r_k$, $r_{k-1} = r_kq_{k+1}$ *(that is, $r_{k+1} = 0$).*

Furthermore, $\gcd(a, b) = r_k$, the last non-zero remainder in the list.

Proof. Let a and b be positive integers with $a \leqslant b$. By the Division Algorithm, there exists positive integer q_1 and non-negative integer r_1 such that $b = aq_1 + r_1$ and $0 \leqslant r_1 < a$. If $r_1 = 0$, the lists terminate; otherwise, for $0 < r_1 < a$, there exists positive integer q_2 and non-negative integer r_2 such that $a = r_1q_2 + r_2$ and $0 \leqslant r_2 < r_1$. If $r_2 = 0$, the lists terminate; otherwise, for $0 < r_2 < r_1$, there exists positive integer q_3 and non-negative integer r_3 such that $r_1 = r_2q_3 + r_3$ and $0 \leqslant r_3 < r_2$.

Continuing in this fashion, we obtain a strictly decreasing sequence of non-negative integers $r_1, r_2, r_3, \cdots$. This lists must end, so there is an integer k such that $r_{k+1} = 0$. Thus we have

$$\begin{aligned} &r_0 \equiv a > r_1 > r_2 > \cdots > r_k > r_{k+1} = 0\,, \\ &r_{j-1} = r_jq_{j+1} + r_{j+1} \quad \text{for all } 1 \leqslant j \leqslant k\,, \\ &b = r_0q_1 + r_1\,. \end{aligned}$$

We now show that $r_k = d \equiv \gcd(a, b)$.

1. The remainder r_k divides r_{k-1} since $r_{k-1} = r_kq_{k+1}$. Also, r_k divides r_{k-2} since

$$r_{k-2} = r_{k-1}q_k + r_k = r_kq_{k+1}q_k + r_k = r_k(q_kq_{k+1} + 1)\,.$$

Therefore, by the fact that $r_{j-1} = r_jq_{j+1} + r_{j+1}$ for all $1 \leqslant j \leqslant k$, we find that r_k divides r_j for all $0 \leqslant j \leqslant k - 1$; thus r_k divides linear combinations of r_j; thus r_k divides a (which is r_0) and b (which is $r_0q_1 + r_1$).

2. On the other hand, d divides r_1 since $r_1 = b - aq_1$. Also, d also divides r_2 since

$$r_2 = r_1 - aq_2 = b - aq_1 - aq_2 = b - a(q_1 + q_2)\,.$$

Therefore, by the fact that $r_{j+1} = r_{j-1} - r_j q_{j+1}$ for all $1 \leqslant j \leqslant k$, we find that d divides r_k for all $0 \leqslant j \leqslant k$.

By (1), r_k is a common divisor of a and b. By (2), the greatest common divisor of a and b must divide r_k; thus we conclude that $r_k = \gcd(a, b)$. □

Example 1.78. Using Euclid's algorithm to compute the greatest common divisor of 12 and 32:

$$\begin{aligned} 32 &= 12 \times 2 + 8\,, \\ 12 &= 8 \times 1 + 4\,, \\ 8 &= 4 \times 2 + 0\,. \end{aligned}$$

Therefore, $4 = \gcd(12, 32)$. Moreover, by working backward,

$$4 = 12 - 8 \times 1 = 12 - (32 - 12 \times 2) \times 1 = 12 \times 3 + 32 \times (-1)\,.$$

Definition 1.79. We say that non-zero integers a and b are **relatively prime** (互質) or **coprime**, if $\gcd(a, b) = 1$.

Lemma 1.80 (Euclid's Lemma)**.** *Let a, b and p be integers. If p is a prime and p divides ab, then p divides a or p divides b.*

Proof. Let a, b be integers, and p be a prime. Suppose that p divides ab, and p does not divides a. Then $\gcd(p, a) = 1$; thus there exist integers m and n such that $1 = am + pn$. Therefore, $b = abm + apn$. Since p divides ab, we conclude that p divides b (since b is a linear combination of ab and p). □

Remark 1.81. The same proof of Euclid's Lemma can be applied to shown a more general case:

Let a, b, p be integers such that p divides ab. If a and p are relatively prime, then p divides b.

2 Sets and Induction

2.1 Basic Concept of Set Theory

Definition 2.1. A ***set*** is a collection of objects called ***elements*** or ***members*** of the set. To denote a set, we make a complete list $\{x_1, x_2, \cdots, x_N\}$ or use the notation

$$\{x : \mathrm{P}(x)\} \quad \text{or} \quad \{x \,|\, \mathrm{P}(x)\}\,,$$

where the sentence $\mathrm{P}(x)$ describes the property that defines the set (the set $\{x \,|\, \mathrm{P}(x)\}$ is in fact the truth set of the open sentence $\mathrm{P}(x)$). A set A is said to be a ***subset*** of S if every member of A is also a member of S. We write $x \in A$ (or A contains x) if x is a member of A, write $x \notin A$ if x is not a member of A, and write $A \subseteq S$ (or S includes A) if A is a subset of S. The empty set, denoted $\varnothing$, is the set with no member.

Example 2.2. The set $A = \{1, 3, 5, 7, 9, 11, 13\}$ may also be written as

$$\big\{x \,\big|\, x \in \mathbb{N}, x \text{ is odd, and } x < 14\big\} \quad \text{or} \quad \big\{x \in \mathbb{N} \,\big|\, x \text{ is odd, and } x < 14\big\}.$$

Remark 2.3. Beware of the distinction between "is an element of" and "is a subset of". For example, let $A = \big\{1, \{2, 4\}, \{5\}, 8\big\}$. Then $4 \notin A$, $\{5\} \in A$, $\big\{1, \{5\}\big\} \subseteq A$ and $\big\{\{5\}\big\} \subseteq A$, but $\{5\} \nsubseteq A$.

Remark 2.4. Not all open sentences $\mathrm{P}(x)$ can be used to defined sets. For example, $\mathrm{P}(x) \equiv$ "x is a set" is not a valid open sentence to define sets for otherwise it will lead to the construction of a set which violates the axiom of regularity.

- **Direct proof of** $A \subseteq B$: $(\forall\, x)\big[(x \in A) \Rightarrow (x \in B)\big]$.

> **Direct proof of $A \subseteq B$**
> **Proof.**
> Let x be an element in A.
> $\vdots$
> Thus, $x \in B$.
> Therefore, $A \subseteq B$. □

- **Proof of** $A \subseteq B$ **by contraposition**: $\sim(x \in B) \Rightarrow \sim(x \in A)$ or $(\forall\, x)\big[(x \notin B) \Rightarrow (x \notin A)\big]$.

> **Proof of $A \subseteq B$ by contraposiction**
> **Proof.**
> Let x be an element.
> Suppose that $x \notin B$; that is, x is not an element of B.
> $\vdots$
> Thus, $x \notin A$.
> Therefore, $A \subseteq B$. □

- **Proof of** $A \subseteq B$ **by contradiction**: $\sim(\exists\, x)\big[(x \in A) \wedge \sim(x \in B)\big]$.

> **Proof of $A \subseteq B$ by contradiction**
> **Proof.**
> Assume that there exists $x \in A$ but $x \notin B$.
> $\vdots$
> Thus, $\mathrm{P} \wedge \sim\mathrm{P}$, a contradiction.
> Therefore, $A \subseteq B$. □

Theorem 2.5. (a) For every set A, $\varnothing \subseteq A$.

(b) For every set A, $A \subseteq A$.

(c) For all sets A, B and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof. (a) Note that since there is no element in $\varnothing$, the open sentence $\mathrm{P}(x) \equiv \big[(x \in \varnothing) \Rightarrow (x \in A)\big]$ is always true (since the antecedent $(x \in \varnothing)$ is always false) for all x.

(b) This follows from that the conditional sentence $\mathrm{P} \Rightarrow \mathrm{P}$ is a tautology (always true).

(c) This follows from that $\big[(\mathrm{P} \Rightarrow \mathrm{Q}) \wedge (\mathrm{Q} \Rightarrow \mathrm{R})\big] \Rightarrow (\mathrm{P} \Rightarrow \mathrm{R})$. □

Definition 2.6. Two sets A and B are said to be ***equal***, denoted by $A = B$, if $(\forall\, x)(x \in A \Leftrightarrow x \in B)$; that is $(A \subseteq B) \wedge (B \subseteq A)$. A set B is said to be a ***proper subset*** of a set A, denoted by $B \subsetneq A$, if $B \subseteq A$ but $A \neq B$.

• **Proof of** $A = B$:

> **Two-part proof of** $A = B$
> **Proof.**
> (i) Prove that $A \subseteq B$ (by any method.)
> (ii) Prove that $B \subseteq A$ (by any method).
> Therefore, $A = B$. □

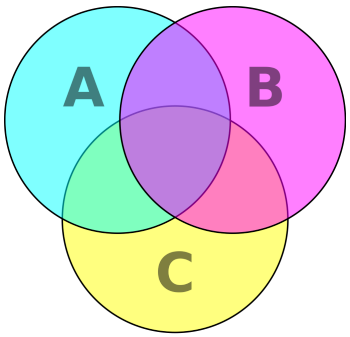
Theorem 2.7. *If A and B are sets with no elements, then $A = B$.*

Proof. Let A, B be set. If A has no element, then $A = \varnothing$; thus by the fact that empty set is a subset of any set, $A \subseteq B$. Similarly, if B has no element, then $B \subseteq A$. □

Theorem 2.8. *For any sets A and B, if $A \subseteq B$ and $A \neq \varnothing$, then $B \neq \varnothing$.*

Proof. Let A, B be sets, $A \subseteq B$, and $A \neq \varnothing$. Then there is an element x such that $x \in A$. By the assumption that $A \subseteq B$, we must have $x \in B$. Therefore, $B \neq \varnothing$. □

• **Venn diagrams**:



Definition 2.9. Let A be a set. The ***power set*** of A, denoted by $\mathscr{P}(A)$ or 2^A, is the colloection of all subsets of A. In other words, $\mathscr{P}(A) \equiv \big\{B \,\big|\, B \subseteq A\big\}$.

Example 2.10. If $A = \{a, b, c, d\}$, then

$$\mathscr{P}(A) = \Big\{\varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\},$$
$$\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b, c, d\}\Big\}.$$

We note that $\#(A) = 4$ and $\#(\mathscr{P}(A)) = 16 = 2^{\#(A)}$.

Theorem 2.11. *If A is a set with n elements, then $\mathscr{P}(A)$ is a set with 2^n elements.*

Proof. Suppose that A is a set with n elements.

1. If $n = 0$, then $A = \varnothing$; thus $\mathscr{P}(A) = \{\varnothing\}$ which shows that $\mathscr{P}(A)$ has $2^0 = 1$ element.
2. If $n \geqslant 1$, we write A as $\{x_1, x_2, \cdots, x_n\}$. To describe a subset B of A, we need to know for each $1 \leqslant i \leqslant n$ whether x_i is in B. For each x_i, there are two possibilities (either $x_i \in B$ or $x_i \notin B$). Thus, there are exactly 2^n different ways of making a subset of A. Therefore, $\mathscr{P}(A)$ has 2^n elements. □

Theorem 2.12. *Let A, B be sets. Then $A \subseteq B$ if and only if $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.*

Proof. Let A, B be sets.

($\Rightarrow$) Suppose that $A \subseteq B$ and $C \in \mathscr{P}(A)$. Then C is a subset of A; thus the fact that $A \subseteq B$ implies that $C \subseteq B$. Therefore, $C \in \mathscr{P}(B)$.

($\Leftarrow$) Suppose that $A \nsubseteq B$. Then there exists $x \in A$ but $x \notin B$. Then $\{x\} \subseteq A$ but $\{x\} \nsubseteq B$ which shows that $\mathscr{P}(A) \nsubseteq \mathscr{P}(B)$. □

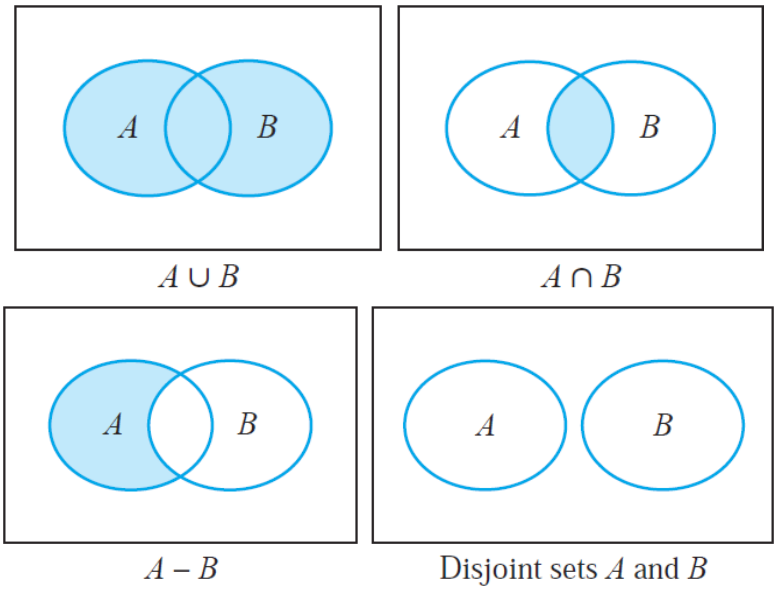
2.2 Set Operations

Definition 2.13. Let A and B be sets.

1. The **union of A and B**, denoted by $A \cup B$, is the set $\{x \mid (x \in A) \vee (x \in B)\}$.
2. The **intersection of A and B**, denoted by $A \cap B$, is the set $\{x \mid (x \in A) \wedge (x \in B)\}$.
3. The **difference of A and B**, denoted by $A - B$ or $A \backslash B$, is the set $\{x \mid (x \in A) \wedge (x \notin B)\}$.

Definition 2.14. Two sets A and B are said to be ***disjoint*** if $A \cap B = \varnothing$.

- Venn diagrams:



Theorem 2.15. *Let A, B and C be sets. Then*

(a) $A \subseteq A \cup B$; (b) $A \cap B \subseteq A$; (c) $A \cap \varnothing = \varnothing$; (d) $A \cup \varnothing = A$;

(e) $A \cap A = A$; (f) $A \cup A = A$; (g) $A \backslash \varnothing = A$; (h) $\varnothing \backslash A = \varnothing$;

(i) $A \cup B = B \cup A$;
(j) $A \cap B = B \cap A$;
} **(commutative laws)**

(k) $A \cup (B \cup C) = (A \cup B) \cup C$;
(ℓ) $A \cap (B \cap C) = (A \cap B) \cap C$;
} **(associative laws)**

(m) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
(n) $A \cup (B \cap C) = (A \cap B) \cup (A \cap C)$;
} **(commutative laws)**

(o) $A \subseteq B$ *if and only if* $A \cup B = B$; (p) $A \subseteq B$ *if and only if* $A \cap B = A$;

(q) *If* $A \subseteq B$, *then* $A \cup C = B \cup C$; (r) *If* $A \subseteq B$, *then* $A \cap C \subseteq B \cap C$.

Note: $(A \cup B) \cap C \neq A \cup (B \cap C)$ in general!

Proof of Theorem 2.15. We only prove (m) and (n).

(m) Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. Thus,

(a) if $x \in B$, then $x \in A \cap B$.

(b) if $x \in C$, then $x \in A \cap C$.

Therefore, $x \in A \cap B$ or $x \in A \cap C$ which shows $x \in (A \cap B) \cup (A \cap C)$; thus we establish that

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)\,.$$

On the other hand, suppose that $x \in (A \cap B) \cup (A \cap C)$.

(a) if $x \in A \cap B$, then $x \in A$ and $x \in B$.

(b) if $x \in A \cap C$, then $x \in A$ and $x \in C$.

In either cases, $x \in A$; thus if $x \in (A \cap B) \cup (A \cap C)$, then $x \in A$ but at the same time $x \in B$ or $x \in C$. Thus, $x \in A$ and $x \in B \cup C$ which shows that $x \in A \cap (B \cup C)$. Therefore,

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)\,.$$

(p) ($\Rightarrow$) Suppose that $A \subseteq B$. Let x be an element in A. Then $x \in B$ since $A \subseteq B$; thus $x \in A \cap B$ which implies that $A \subseteq A \cap B$. On the other hand, it is clear that $A \cap B \subseteq A$, so we conclude that $A \cap B = A$.

($\Leftarrow$) Suppose that $A \cap B = A$.Let x be an element in A. Then $x \in A \cap B$ which shows that $x \in B$. Therefore, $A \subseteq B$. □

Remark 2.16. Theorem 1.13 can be applied to show (k), (ℓ), (m) and (n). For example, to show (m), we let x be an element in the universe, and P, Q and R denote the propositions $x \in A$, $x \in B$ and $x \in C$, respectively. Note that Theorem 1.13 provides that

$$\mathrm{P} \wedge (\mathrm{Q} \vee \mathrm{R}) \Leftrightarrow \big[(\mathrm{P} \wedge \mathrm{Q}) \vee (\mathrm{P} \wedge \mathrm{R})\big] .$$

(1) Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$; thus the proposition $\mathrm{P} \wedge (\mathrm{Q} \vee \mathrm{R})$ is true. Therefore, the proposition $\big[(\mathrm{P} \wedge \mathrm{Q}) \vee (\mathrm{P} \wedge \mathrm{R})\big]$ is also true which implies that $x \in A \cap B$ or $x \in A \cap C$; thus $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

(2) Working conversely, we find that if $x \in A \cap B$ or $x \in A \cap C$, then $x \in A \cap (B \cup C)$. Therefore, $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

From (1) and (2), we conclude that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Definition 2.17. Let U be the universe and $A \subseteq U$. The ***complement*** of A, denoted by $A^{\complement}$, is the set $U \backslash A$.

Theorem 2.18. *Let U be the universe, and $A, B \subseteq U$. Then*

(a) $(A^{\complement})^{\complement} = A$.

(b) $A \cup A^{\complement} = U$.

(c) $A \cap A^{\complement} = \varnothing$.

(d) $A \backslash B = A \cap B^{\complement}$.

(e) $A \subseteq B$ *if and only if* $B^{\complement} \subseteq A^{\complement}$.

(f) $A \cap B = \varnothing$ *if and only if* $A \subseteq B^{\complement}$

(g) $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$.
(h) $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$. } **(De Morgan's Law)**

Proof. We only prove (a), (e) and (g), and the others are left as exercises.

(a) By the definition of the complement, $x \in (A^{\complement})^{\complement}$ if and only if $x \notin A^{\complement}$ if and only if $x \in A$.

(e) By the equivalence of $\mathrm{P} \Rightarrow \mathrm{Q}$ and $\sim \mathrm{Q} \Rightarrow \sim \mathrm{P}$, we conclude that

$$(\forall\, x)\big[(x \in A) \Rightarrow (x \in B)\big] \quad \Leftrightarrow \quad (\forall\, x)\big[(x \notin B) \Rightarrow (x \notin A)\big]$$

and the bi-directional statement is identical to that

$$A \subseteq B \Leftrightarrow B^{\complement} \subseteq A^{\complement} .$$

(e) (Alternative proof) Using (a), it suffices to show that $A \subseteq B \Rightarrow B^{\complement} \subseteq A^{\complement}$. Suppose that $A \subseteq B$, and $B^{\complement} \nsubseteq A^{\complement}$. Then there exists $x \in B^{\complement}$ and $x \in A$; however, by the fact that $A \subseteq B$, x has to belong to B, a contradiction.

(g) By the equivalence of $\sim(\mathrm{P} \vee \mathrm{Q})$ and $(\sim\mathrm{P}) \wedge (\sim\mathrm{Q})$, we find that

$$(\forall\, x) \sim \big[(x \in A) \vee (x \in B)\big] \quad \Leftrightarrow \quad (\forall\, x)\big[(x \notin A) \wedge (x \notin B)\big]$$

and the bi-directional statement is identical to that

$$(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}\,.$$

(g) (Alternative proof) Let x be an element in the universe.

$$\begin{aligned} x \in (A \cup B)^{\complement} \;& \text{ if and only if } x \notin A \cup B \\ & \text{if and only if it is not the case that } x \in A \text{ or } x \in B \\ & \text{if and only if } x \notin A \text{ and } x \notin B \\ & \text{if and only if } x \in A^{\complement} \text{ and } x \in B^{\complement} \\ & \text{if and only if } x \in A^{\complement} \cap B^{\complement}\,. \end{aligned}$$

□

Definition 2.19. An ***ordered pair*** (a, b) is an object formed from two objects a and b, where a is called the ***first coordinate*** and b the ***second coordinate***. Two ordered pairs are equal whenever their corresponding coordinates are the same.

An ***ordered n-tuples*** $(a_1, a_2, \cdots, a_n)$ is an object formed from n objects a_1, a_2, $\cdots$, a_n, where a_j is called the j-th coordinate. Two n-tuples $(a_1, a_2, \cdots, a_n)$, $(c_1, c_2, \cdots, c_n)$ are equal if $a_i = c_i$ for $i \in \{1, 2, \cdots, n\}$.

Definition 2.20. Let A and B be sets. The product of A and B, denoted by $A \times B$, is

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

The product of three or more sets are defined similarly.

Example 2.21. Let $A = \{1, 3, 5\}$ and $B = \{\star, \diamond\}$. Then

$$A \times B = \big\{(1, \star), (3, \star), (5, \star), (1, \diamond), (3, \diamond), (5, \diamond)\big\}\,.$$

Theorem 2.22. *If A, B, C and D are sets, then*

(a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

(c) $A \times \varnothing = \varnothing$.

(d) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

(e) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

(f) $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$.

2.3 Indexed Families of Sets

Definition 2.23. Let $\mathscr{F}$ be a family of sets.

1. The ***union*** of the family $\mathscr{F}$ or the ***union*** over $\mathscr{F}$, denoted by $\bigcup_{A\in\mathscr{F}} A$, is the set $\{x \mid x \in A \text{ for some } A \in \mathscr{F}\}$. Therefore,
$$x \in \bigcup_{A\in\mathscr{F}} A \quad \text{if and only if} \quad (\exists\, A \in \mathscr{F})(x \in A).$$

2. The ***intersection*** of the family $\mathscr{F}$ or the ***intersection*** over $\mathscr{F}$, denoted by $\bigcap_{A\in\mathscr{F}} A$, is the set $\{x \mid x \in A \text{ for all } A \in \mathscr{F}\}$. Therefore,
$$x \in \bigcap_{A\in\mathscr{F}} A \quad \text{if and only if} \quad (\forall\, A \in \mathscr{F})(x \in A).$$

Example 2.24. Let $\mathscr{F}$ be the collection of sets given by
$$\mathscr{F} = \left\{ \left[\frac{1}{n}, 2 - \frac{1}{n}\right] \,\middle|\, n \in \mathbb{N} \right\}.$$
Then $\bigcup_{A\in\mathscr{F}} A = (0,2)$ and $\bigcap_{A\in\mathscr{F}} A = \{1\}$. In this kind of cases, we also write $\bigcup_{A\in\mathscr{F}} A$ and $\bigcap_{A\in\mathscr{F}} A$ as $\bigcup_{n=1}^{\infty} \left[\frac{1}{n}, 2 - \frac{1}{n}\right]$ and $\bigcap_{n=1}^{\infty} \left[\frac{1}{n}, 2 - \frac{1}{n}\right]$, respectively.

Example 2.25. Let $\mathscr{F}$ be the collection of sets given by
$$\mathscr{F} = \left\{ \left(-\frac{1}{n}, 2 + \frac{1}{n}\right) \,\middle|\, n \in \mathbb{N} \right\}.$$
Then $\bigcup_{A\in\mathscr{F}} A = (-1,3)$ and $\bigcap_{A\in\mathscr{F}} A = [0,2]$. In this kind of cases, we also write $\bigcup_{A\in\mathscr{F}} A$ and $\bigcap_{A\in\mathscr{F}} A$ as $\bigcup_{n=1}^{\infty} \left(-\frac{1}{n}, 2 + \frac{1}{n}\right)$ and $\bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, 2 + \frac{1}{n}\right)$, respectively.

Theorem 2.26. *Let $\mathscr{F}$ be a family of sets.*

(a) *For every set B in the family $\mathscr{F}$, $\bigcap_{A\in\mathscr{F}} A \subseteq B$.*

(b) *For every set B in the family $\mathscr{F}$, $B \subseteq \bigcup_{A\in\mathscr{F}} A$.*

(c) *If the family $\mathscr{F}$ is non-empty, then $\bigcap_{A\in\mathscr{F}} A \subseteq \bigcup_{A\in\mathscr{F}} A$.*

(d) $\left(\bigcap_{A\in\mathscr{F}} A\right)^{\complement} = \bigcup_{A\in\mathscr{F}} A^{\complement}$.

(e) $\left(\bigcup_{A\in\mathscr{F}} A\right)^{\complement} = \bigcap_{A\in\mathscr{F}} A^{\complement}$.

(De Morgan's Law)

Proof. We only prove (d). Let x be an element in the universe. Then

$$\begin{aligned} x \in \Big(\bigcap_{A\in\mathscr{F}} A\Big)^{\complement} &\text{ if and only if } x \notin \bigcap_{A\in\mathscr{F}} A \\ &\text{if and only if } \sim\big(x \in \bigcap_{A\in\mathscr{F}} A\big) \\ &\text{if and only if } \sim(\forall\, A \in \mathscr{F})(x \in A) \\ &\text{if and only if } (\exists\, A \in \mathscr{F}) \sim (x \in A) \\ &\text{if and only if } (\exists\, A \in \mathscr{F})(x \notin A) \\ &\text{if and only if } (\exists\, A \in \mathscr{F})(x \in A^{\complement}) \\ &\text{if and only if } x \in \bigcup_{A\in\mathscr{F}} A^{\complement}. \end{aligned}$$

□

Theorem 2.27. *Let $\mathscr{F}$ be a non-empty family of sets and B a set.*

(a) *If $B \subseteq A$ for all $A \in \mathscr{F}$, then $B \subseteq \bigcap_{A\in\mathscr{F}} A$.*

(b) *If $A \subseteq B$ for all $A \in \mathscr{F}$, then $\bigcup_{A\in\mathscr{F}} A \subseteq B$.*

Proof. (a) Suppose that $B \subseteq A$ for all $A \in \mathscr{F}$, and $x \in B$. Then $x \in A$ for all $A \in \mathscr{F}$. Therefore, $(\forall\, A \in \mathscr{F})(x \in A)$ or equivalently, $x \in \bigcap_{A\in\mathscr{F}} A$.

(b) Suppose that $A \subseteq B$ for all $A \in \mathscr{F}$, and $x \in \bigcup_{A\in\mathscr{F}} A$. Then $x \in A$ for some $A \in \mathscr{F}$. By the fact that $A \subseteq B$, we find that $x \in B$. □

Example 2.28. Let $\mathscr{F} = \big\{[-r, r^2+1) \,\big|\, r \in \mathbb{R} \text{ and } r \geqslant 0\big\}$. Then $\bigcup_{A\in\mathscr{F}} A = \mathbb{R}$ and $\bigcap_{A\in\mathscr{F}} = [0, 1)$. $\Big($We also write $\bigcup_{A\in\mathscr{F}} A$ and $\bigcap_{A\in\mathscr{F}} A$ as $\bigcup_{r\geqslant 0}[-r, r^2+1)$ and $\bigcap_{r\geqslant 0}[-r, r^2+1)$, respectively.$\Big)$

Proof. 1. If $x \in \mathbb{R}$, then $x \in [-r, r^2+1)$ with $r = |x|$ since $-|x| \leqslant x \leqslant x^2+1$. Therefore, $\mathbb{R} \subseteq \bigcup_{A\in\mathscr{F}} A$.

2. If $x \in [0, 1)$, then $x \in [-r, r^2+1)$ for all $r \geqslant 0$; thus $[0, 1) \subseteq \bigcap_{A\in\mathscr{F}} A$. If $x \in \bigcap_{A\in\mathscr{F}} A$, then $x \in [-r, r^2+1)$ for all $r \geqslant 0$; thus $x \geqslant -r$ and $x < r^2+1$ for all $r \geqslant 0$. In particular, $x \geqslant 0$ and $x < 1$. □

Definition 2.29. Let Δ be a non-empty set such that for each $\alpha \in \Delta$ there is a corresponding set A_α. The family $\big\{A_\alpha \,\big|\, \alpha \in \Delta\big\}$ is an ***indexed family*** of sets, and Δ is called the ***indexing set*** of this family and each $\alpha \in \Delta$ is called an ***index***.

Remark 2.30. 1. The indexing set of an indexed family of sets may be finite or infinite, the member sets need not have the same number of elements, and different indices need not correspond to different sets in the family.

2. If $\mathscr{F} = \{A_\alpha \,|\, \alpha \in \Delta\}$ is an indexed family of sets, we also write $\bigcup_{A\in\mathscr{F}} A$ as $\bigcup_{\alpha\in\Delta} A_\alpha$ and write $\bigcap_{A\in\mathscr{F}} A$ as $\bigcap_{\alpha\in\Delta} A_\alpha$.

3. Another way for the union and intersection of indexed family of sets whose indexing set is $\mathbb{N}$ or $\mathbb{Z}$ is

$$\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n=1}^{\infty} A_n \quad \text{and} \quad \bigcap_{n\in\mathbb{N}} A_n = \bigcap_{n=1}^{\infty} A_n$$

and

$$\bigcup_{n\in\mathbb{Z}} A_n = \bigcup_{n=-\infty}^{\infty} A_n \quad \text{and} \quad \bigcap_{n\in\mathbb{N}} A_n = \bigcap_{n=-\infty}^{\infty} A_n\,.$$

Also, the union and intersection of sets A_4, A_5, A_6, $\cdots$, A_{100} can be written as

$$\bigcup_{4\leqslant n\leqslant 100} A_n = \bigcup_{n=4}^{100} A_n \quad \text{and} \quad \bigcap_{4\leqslant n\leqslant 100} A_n = \bigcap_{n=4}^{100} A_n$$

and etc.

Definition 2.31. The indexed family $\mathscr{F} = \{A_\alpha \,|\, \alpha \in \Delta\}$ of sets is said to be ***pairwise disjoint*** if for all $\alpha, \beta \in \Delta$, either $A_\alpha = A_\beta$ or $A_\alpha \cap A_\beta = \varnothing$.

Definition 2.32. The indexed family $\mathscr{F} = \{A_k \,|\, k \in \mathbb{N}\}$ of sets is said to be a ***nested family*** of sets if for all $i, j \in \mathbb{N}$, $i \leqslant j$, then $A_j \subseteq A_i$.

2.4 Mathematical Induction

• **Peano's Axiom for natural numbers**:

1. 1 is a natural number.
2. Every natural number has a unique successor which is a natural number (+1 is defined on natural numbers).
3. No two natural numbers have the same successor ($n + 1 = m + 1$ implies $n = m$).
4. 1 is not a successor for any natural number (1 is the "smallest" natural number).
5. If a property is possessed by 1 and is possessed by the successor of every natural number that possesses it, then the property is possessed by all natural numbers. (如果某個被自然數 1 所擁有的性質，也被其它擁有這個性質的自然數的下一個自然數所擁有，那麼所有的自然數都會擁有這個性質)

The 5th statement in the Peano Axiom for natural numbers can be restated as the famous

• **Principle of Mathematical Induction (PMI)**: If $S \subseteq \mathbb{N}$ has the property that

$$(1)\ 1 \in S, \text{ and} \quad (2)\ n + 1 \in S \text{ whenever } n \in S\,,$$

then $S = \mathbb{N}$.

Definition 2.33. A set $S \subseteq \mathbb{N}$ is said to be ***inductive*** if it has the property that $n+1 \in S$ whenever $n \in S$.

Note: There are many inductive sets, but only one inductive set contains 1 (which is $\mathbb{N}$).

• **Inductive definition**: Inductive definition is a way to define some "functions" $f(n)$ for all natural numbers n. It is done by describe the first object $f(1)$, and then the $(n+1)$-th object $f(n+1)$ is defined in terms of the n-th object $f(n)$. We remark that in this way of defining f, **PMI** ensures that the collection of all n for which the corresponding object $f(n)$ is defined is $\mathbb{N}$.

Example 2.34. The notation $\sum_{k=1}^{n} x_k$ can be defined by

1. $\sum_{k=1}^{1} x_k = x_1$; 2. For all $n \in \mathbb{N}$, $\sum_{k=1}^{n+1} x_k = \sum_{k=1}^{n} x_k + x_{n+1}$.

Example 2.35. The notation $\prod_{k=1}^{n} x_k$ can be defined by

1. $\sum_{k=1}^{1} x_k = x_1$; 2. For all $n \in \mathbb{N}$, $\prod_{k=1}^{n+1} x_k = \left(\prod_{k=1}^{n} x_k\right) \cdot x_{n+1}$.

Example 2.36. The **factorial** $n!$ can be defined by

1. $1! = 1$; For all $n \in \mathbb{N}$, $(n+1)! = n! \times (n+1)$.

PMI can provide a powerful method for proving statements that are true for all natural numbers.

Suppose that $\mathrm{P}(n)$ is an open sentence concerning the natural numbers.

Proof of $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ by mathematical induction
Proof.
Let S denote the truth of P.
(i) **Basis Step**. Show that $1 \in S$.
(ii) **Inductive Step**. Show that S is inductive by showing that
if $n \in S$, then $n+1 \in S$.
Therefore, **PMI** ensures that the truth set of P is $\mathbb{N}$. □

or

Proof of $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ by mathematical induction
Proof.
(i) **Basis Step**. Show that $\mathrm{P}(1)$ is true.
(ii) **Inductive Step**. Suppose that $\mathrm{P}(n)$ is true.
⋮
Therefore, $\mathrm{P}(n+1)$ is true.
Therefore, **PMI** ensures that $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ is true. □

Example 2.37. Prove that for every natural number n,

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

Proof. Let $\mathrm{P}(n)$ be the open sentence $1 + 3 + 5 + \cdots + (2n-1) = n^2$.

1. $\mathrm{P}(1)$ is true since $1 = 1^2$.

2. Suppose that $\mathrm{P}(n)$ is true. Then

$$1+3+5+\cdots+(2n-1)+(2n+1)=n^2+(2n+1)=(n+1)^2$$

which shows that $\mathrm{P}(n+1)$ is true.

Therefore, **PMI** ensures that $(\forall\, n\in\mathbb{N})\mathrm{P}(n)$ is true. □

Example 2.38 (De Moivre's formula)**.** Let θ be a real number. Prove that for every $n\in\mathbb{N}$,

$$(\cos\theta+i\sin\theta)^n=\cos(n\theta)+i\sin(n\theta)\,.$$

Proof. Let $\theta\in\mathbb{R}$ and $\mathrm{P}(n)$ be the open sentence $(\cos\theta+i\sin\theta)^n=\cos(n\theta)+i\sin(n\theta)$.

1. Obviously $\mathrm{P}(1)$ is true.

2. Suppose that $\mathrm{P}(n)$ is true. Then

$$\begin{aligned}(\cos\theta+i\sin\theta)^{n+1}&=(\cos\theta+i\sin\theta)^n\cdot(\cos\theta+i\sin\theta)=\big[\cos(n\theta)+i\sin(n\theta)\big]\cdot(\cos\theta+i\sin\theta)\\&=\big[\cos(n\theta)\cos\theta-\sin(n\theta)\sin\theta\big]+i\big[\cos(n\theta)\sin\theta+\sin(n\theta)\cos\theta\big]\\&=\cos(n+1)\theta+i\sin(n+1)\theta\end{aligned}$$

which shows that $\mathrm{P}(n+1)$ is true.

Therefore, **PMI** ensures that $(\forall\, n\in\mathbb{N})\mathrm{P}(n)$ is true. □

Theorem 2.39 (Archimedean Property)**.** *For all natural numbers a and b, there exists a natural number s such that $sb>a$.*

Proof. We fix b and make induction on a.

1. If $a=1$, then the choice of $s=2$ ensures that $2b>1$. Therefore, the Archimedean property holds for $a=1$ (with fixed b).

2. Suppose that if $a=k$, there exists $s=s^*\in\mathbb{N}$ such that $s^*b>k$. Then the choice of $s=s^*+1$ ensures that $sb=(s^*+1)b>k+b\geqslant k+1$; thus Archimedean property holds for $a=k+1$ (with fixed b).

Therefore, **PMI** implies that Archimedean property holds for all $a\in\mathbb{N}$ (with fixed b) and the theorem is concluded. □

• **Generalized Principle of Mathematical Induction (GPMI)**: If $S\subseteq\mathbb{N}$ has the property that

$$(1)\ k\in S,\text{ and}\quad (2)\ n+1\in S\text{ whenever }n\in S\,,$$

then $S=\{k,k+1,k+2,\cdots\}=\big\{n+k-1\,\big|\,n\in\mathbb{N}\big\}$.

Theorem 2.40. PMI *implies* **GPMI**, *and vice versa.*

Proof. It suffices to show that **PMI** implies **GPMI**. Let $T = \{n \in \mathbb{N} \,|\, k + n - 1 \in S\}$. Then $T \subseteq \mathbb{N}$. Moreover,

1. $1 \in T$ since $k \in S$ if and only if $1 \in T$.

2. If $n \in T$, then $k + n - 1 \in S$; thus $k + n \in S$ which implies that $n + 1 \in T$.

Therefore, **PMI** ensures that $T = \mathbb{N}$ which shows that $S = \{n \in \mathbb{N} \,|\, n \geqslant k\}$. □

Example 2.41. Prove that $n^2 - n - 20 > 0$ for all $n > 5$.

Proof. Let $S = \{n \in \mathbb{N} \,|\, n^2 - n - 20 > 0\}$.

1. $6 \in S$ since $6^2 - 6 - 20 = 10 > 0$.

2. Suppose that $n \in S$. Then

$$(n+1)^2 - (n+1) - 20 > n^2 + 2n + 1 - n - 1 - 20 > 2n > 0\,.$$

Therefore, **GPMI** ensures that $S = \{n \in \mathbb{N} \,|\, n \geqslant 6\}$. □

2.5 Equivalent Forms of Induction

In this section, we establish the equivalence among **PMI** and the other two principles: the Well-Ordering Principle and the Principle of Complete Induction.

• **Well-Ordering Principle (WOP)**: Every nonempty subset of $\mathbb{N}$ has a smallest element.

Theorem 2.42. PMI *implies* **WOP**.

Proof. Assume the contrary that there exists a non-empty set $S \subseteq \mathbb{N}$ such that S does not have the smallest element. Define $T = \mathbb{N} \backslash S$, and $T_0 = \{n \in \mathbb{N} \,|\, \{1, 2, \cdots, n\} \subseteq T\}$. Then we have $T_0 \subseteq T$. Also note that $1 \notin S$ for otherwise 1 is the smallest element in S, so $1 \in T$ (thus $1 \in T_0$).

Assume $k \in T_0$. Since $\{1, 2, \cdots, k\} \subseteq T$, $1, 2, \cdots k \notin S$. If $k + 1 \in S$, then $k + 1$ is the smallest element in S. Since we assume that S does not have the smallest element, $k + 1 \notin S$; thus $k + 1 \in T \Rightarrow k + 1 \in T_0$.

Therefore, by **PMI** we conclude that $T_0 = \mathbb{N}$; thus $T = \mathbb{N}$ (since $T_0 \subseteq T$) which further implies that $S = \varnothing$ (since $T = \mathbb{N} \backslash S$). This contradicts to the assumption $S \neq \varnothing$. □

• **Principle of Complete Induction (PCI)**: If $S \subseteq \mathbb{N}$ has the property

$$\forall\, n \in \mathbb{N},\ n \in S \text{ whenever } \{1, 2, \cdots, n-1\} \subseteq S\,, \tag{2.1}$$

then $S = \mathbb{N}$.

We note that the set $\{1, 2, \cdots, n-1\}$ denotes the collection of natural numbers that are not greater than $n - 1$.

Theorem 2.43. WOP *implies* **PCI**.

Proof. Assume the contrary that for some $S \neq \mathbb{N}$, S has the property (2.1). Define $T = \mathbb{N}\backslash S$. Then T is a non-empty subset of $\mathbb{N}$; thus **WOP** implies that T has a smallest element k. Then $1, 2, \cdots, k-1 \notin T$ which is the same as saying that $\{1, 2, \cdots, k-1\} \subseteq S$. By property (2.1), $k \in S$ which implies that $k \notin T$, a contradiction. ▫

To establish the equivalent among **PMI**, **WOP** and **PCI**, it suffices to establish the following

Theorem 2.44. PCI *implies* **PMI**.

Proof. Let $S \subseteq \mathbb{N}$ has the property

$$\text{(a) } 1 \in S, \text{ and} \quad \text{(b) } n+1 \in S \text{ whenever } n \in S\,.$$

We show that $S = \mathbb{N}$ by verifying that $k \in S$ whenever $\{1, 2, \cdots, k-1\} \subseteq S$.

1. (a) implies $1 \in S$; thus the statement "$\{1, 2, \cdots, k-1\} = \varnothing \subseteq S \Rightarrow 1 \in S$" is true.

2. Suppose that $\{1, 2, \cdots, k-1\} \subseteq S$. Then $k-1 \in S$. Using (b) we find that $k \in S$; thus the statement "$\{1, 2, \cdots, k-1\} \subseteq S \Rightarrow k \in S$" is also true.

Therefore, S has property (2.1) and **PCI** implies that $S = \mathbb{N}$. ▫

Theorem 2.45 (Fundamental Theorem of Arithmetic)**.** *Every natural number greater than* 1 *is prime or can be expressed uniquely as a product of primes.*

> **The meaning of the unique way of expressing a composite number as a product of primes:**
> Let m be a composite number. Then there is a unique way of writing m in the form
> $$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$
> where $p_1 < p_2 < \cdots < p_n$ are primes and $\alpha_1, \alpha_2, \cdots, \alpha_n$ are natural numbers.

Proof based on **WOP**. We first show that every natural number greater than 1 is either a prime or a products of primes, then show that the prime factor decomposition, when it is not prime, is unique.

1. Suppose that there is at least one natural number that is not a prime and cannot be written as a product of primes. The the set S of such numbers is non-empty, so **WOP** implies that S has a smallest element m. Since m is not a prime, $m = st$ for some natural numbers s and t that are greater than 1 and less than m. Both s and t are less than the smallest element of S, so they are not in S. Therefore, each of s and t is a prime or is the product of primes, which makes m a product of primes, a contradiction.

2. Suppose that there exist natural numbers that can be expressed in two or more different ways as the product of primes, and let n be the smallest such number (the existence of such a number is guaranteed by **WOP**). Then

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$$

for some $n, m \in \mathbb{N}$, where each p_i, q_j is prime and $p_i \neq p_j$ and $q_i \neq q_j$ if $i \neq j$. Then p_1 divides $q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$ which implies that $p_1 = q_j$ for some $j \in \{1, \cdots, m\}$. Then $\dfrac{n}{p_1} = \dfrac{n}{q_j}$ is a natural number smaller than n that has two different prime factorizations, a contradiction. ▫

Alternative Proof based on **PCI**. Let m be a natural number greater than 1. We note that 2 is a prime, so the statement is true when m is 2. Now assume that k is a prime or is a product of primes for all k such that $1 < k < m$. If m has no factors other than 1 and itself, then m is prime. Otherwise, $m = st$ for some natural numbers s and t that are greater than 1 and less than m. By the complete induction hypothesis, each of s and t either is prime or is a product of primes. Thus, $m = st$ is a product of primes, so the statement is true for m. Therefore, we conclude that every natural number greater than 1 is prime or is a product of primes by **PCI**. ▫

Theorem 2.46. *Let a and b be nonzero integers. Then there is a smallest positive linear combination of a and b.*

Proof. Let a and b be nonzero integers, and S be the set of all positive linear combinations of a and b; that is,

$$S = \{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\}.$$

Then $S \neq \varnothing$ since $a \cdot 1 + b \cdot 0 > 0$ or $a \cdot (-1) + b \cdot 0 > 0$. By **WOP**, S has a smallest element, which is the smallest positive linear combination of a and b. ▫

Theorem 2.47 (Division Algorithm)**.** *For all integers a and b, where $a \neq 0$, there exist a unique pair of integers (q, r) such that $b = aq + r$ and $0 \leqslant r < |a|$. In notation,*

$$\big(\forall\, (a, b) \in (\mathbb{Z} \backslash \{0\}) \times \mathbb{Z}\big)(\exists! (q, r) \in \mathbb{Z} \times \mathbb{Z})\big[(a = bq + r) \wedge (0 \leqslant r < |a|)\big].$$

Proof. We only prove the case that $a > 0$ (for if $a < 0$, we apply the Division Algorithm for b and $-a$ to conclude this case). Let $S = \{b - ak \mid k \in \mathbb{Z} \text{ and } b - ak \geqslant 0\}$.

1. If $0 \in S$, then a divides b; thus $q = \dfrac{b}{a}$ and $r = 0$.
2. If $0 \notin S$, then $b \neq 0$. It is clear that if $b > 0$, then $S \neq \varnothing$. If $b < 0$, then $-b > 0$; thus the Archimedean property (Theorem 2.39) implies that there exists $k \in \mathbb{N}$ such that $ak > -b$. Therefore, $b - a(-k) > 0$ which also implies that $S \neq \varnothing$. In either case, S is a non-empty subset of $\mathbb{N}$; thus **WOP** implies that S has a smallest element r. Then $b - aq = r$ for some $q \in \mathbb{Z}$; thus $b = aq + r$ and $r > 0$.

   Next, we show that $r < |a| = a$. Assume the contrary that $r \geqslant |a| = a$. Then $b - a(q + 1) = b - aq - a = r - a \geqslant 0$. Since we assume that $0 \notin S$, we must have $b - a(q + 1) > 0$. Therefore,

   $$0 < b - a(q + 1) = r - a < r = b - aq$$

   which shows that r is not the smallest element of S, a contradiction.

To complete the proof, we need to show that the pair (q, r) is unique. Suppose that there exist (q_1, r_1) and (q_2, r_2), where $0 \leqslant r_1, r_2 < |a|$, such that

$$b = aq_1 + r_1 = aq_2 + r_2 \,.$$

W.L.O.G., we can assume that $r_1 \geqslant r_2$; thus $a(q_2 - q_1) = r_1 - r_2 \geqslant 0$. Therefore, a divides $r_1 - r_2$ which is impossible if $0 < r_1 - r_2 < a$. Therefore, $r_1 = r_2$ and then $q_1 = q_2$. □

3 Relations and Partitions

3.1 Relations

Definition 3.1. Let A and B be sets. R is a ***relation*** from A to B if R is a subset of $A \times B$. A relation from A to A is called a ***relation*** on A. If $(a, b) \in R$, we say a is R-related (or simply related) to b and write aRb. If $(a, b) \notin R$, we write $a \not R b$.

Example 3.2. Let R be the relation "is older than" on the set of all people. If a is 32 yrs old, b is 25 yrs old, and c is 45 yrs old, then aRb, cRb, $a \not R c$.

Similarly, the "less than" relation on $\mathbb{R}$ is the set $\{(x, y) \,|\, x < y\}$.

Remark 3.3. Let A and B be sets. Every subset of $A \times B$ is a relation from A to B; thus every collection of ordered pairs is a relation. In particular, the empty set $\varnothing$ and the set $A \times B$ are relations from A to B ($R = \varnothing$ is the relation that "nothing" is related, while $R = A \times B$ is the relation that "everything" is related).

Definition 3.4. For any set A, the ***identity relation on*** A is the (diagonal) set

$$I_A = \{(a, a) \,|\, a \in A\}.$$

Definition 3.5. Let A and B be sets, and R be a relation from A to B. The ***domain*** of R is the set

$$\mathrm{Dom}(R) \equiv \{x \in A \,|\, \text{there exists } y \in B \text{ such that } xRy\} = \{x \in A \,|\, (\exists\, y \in B)(xRy)\},$$

and the ***range*** of R is the set

$$\mathrm{Rng}(R) \equiv \{y \in B \,|\, \text{there exists } x \in A \text{ such that } xRy\} = \{y \in B \,|\, (\exists\, x \in A)(xRy)\}.$$

In other words, the domain of a relation R from A to B is the collection of all first coordinate of ordered pairs in R, and the range of R is the collection of all second coordinates.

Definition 3.6. Let A and B be sets, and R be a relation from A to B. The ***inverse*** of R, denoted by R^{-1}, is the relation

$$R^{-1} = \{(y, x) \in B \times A \,|\, (x, y) \in R \text{ (or equivalently, } xRy)\}.$$

In other words, xRy if and only if $yR^{-1}x$ or equivalently, $(x, y) \in R$ if and only if $(y, x) \in R^{-1}$.

Example 3.7. Let $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, y < 4x^2 - 7\}$. To find the inverse of T, we note that

$$\begin{aligned}(x, y) \in T^{-1} &\Leftrightarrow (y, x) \in T \Leftrightarrow x < 4y^2 - 7 \Leftrightarrow x + 7 < 4y^2 \Leftrightarrow y^2 > \frac{x+7}{4} \\ &\Leftrightarrow (x, y) \in \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x + 7 < 0\} \cup \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, y^2 > \frac{x+7}{4} \geqslant 0\}.\end{aligned}$$

Theorem 3.8. *Let A and B be sets, and R be a relation from A to B.*

(a) $\mathrm{Dom}(R^{-1}) = \mathrm{Rng}(R)$. (b) $\mathrm{Rng}(R^{-1}) = \mathrm{Dom}(R)$.

Proof. The theorem is concluded since

$$b \in \mathrm{Dom}(R^{-1}) \Leftrightarrow (\exists\, a \in A)\big[(b,a) \in R^{-1}\big] \Leftrightarrow (\exists\, a \in A)\big[(a,b) \in R\big] \Leftrightarrow b \in \mathrm{Rng}(R)\,,$$
$$a \in \mathrm{Rng}(R^{-1}) \Leftrightarrow (\exists\, b \in B)\big[(b,a) \in R^{-1}\big] \Leftrightarrow (\exists\, b \in B)\big[(a,b) \in R\big] \Leftrightarrow a \in \mathrm{Dom}(R)\,. \qquad \square$$

Definition 3.9. Let A, B, C be sets, and R be a relation from A to B, S be a relation from B to C. The ***composite*** of R and S is a relation from A to C, denoted by $S \circ R$, given by

$$\begin{aligned} S \circ R &\equiv \big\{(a,c) \in A \times C \,\big|\, \text{there exists } b \in B \text{ such that } (a,b) \in R \text{ and } (b,c) \in S\big\} \\ &= \Big\{(a,c) \in A \times C \,\Big|\, (\exists\, b \in B)\big[(aRb) \wedge (bSc)\big]\Big\}\,. \end{aligned}$$

We note that $\mathrm{Dom}(S \circ R) \subseteq \mathrm{Dom}(R)$ and it may happen that $\mathrm{Dom}(S \circ R) \subsetneq \mathrm{Dom}(R)$.

Example 3.10. Let $A = \{1,2,3,4,5\}$, $B = \{p,q,r,s,t\}$ and $C = \{x,y,z,w\}$. Let R be the relation from A to B:

$$R = \big\{(1,p),(1,q),(2,q),(3,r),(4,s)\big\}$$

and S be the relation from B to C:

$$S = \big\{(p,x),(q,x),(q,y),(s,z),(t,z)\big\}\,.$$

Then $S \circ R = \big\{(1,x),(1,y),(2,x),(2,y),(4,z)\big\}$.

Example 3.11. Let $R = \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, y = x+1\big\}$ and $S = \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, y = x^2\big\}$. Then

$$\begin{aligned} R \circ S &= \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, y = x^2 + 1\big\}\,, \\ S \circ R &= \big\{(x,y) \in \mathbb{R} \times \mathbb{R} \,\big|\, y = (x+1)^2\big\}\,. \end{aligned}$$

Therefore, $S \circ R \neq R \circ S$.

Theorem 3.12. *Suppose that A, B, C, D are sets, R be a relation from A to B, S be a relation from B to C, and T be a relation from C to D.*

(a) $(R^{-1})^{-1} = R$.

(b) $T \circ (S \circ R) = (T \circ S) \circ R$ (*so composition is associative*).

(c) $I_B \circ R = R$ *and* $R \circ I_A = R$.

(d) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Proof. (a) the conclusion following from that

$$(a,b) \in (R^{-1})^{-1} \Leftrightarrow (b,a) \in R^{-1} \Leftrightarrow (a,b) \in R\,.$$

(b) Since $S \circ R$ is a relation from A to C, $T \circ (S \circ R)$ is a relation from $A \to D$. Similarly, $(T \circ S) \circ R$ is also a relation from A to D. Let $(a, d) \in A \times D$. Then using (1.1b),

$$\begin{aligned}(a,d) \in T \circ (S \circ R) &\Leftrightarrow (\exists\, c \in C)\big[(a,c) \in S \circ R \wedge (c,d) \in T\big] \\ &\Leftrightarrow (\exists\, c \in C)(\exists\, b \in B)\big[(a,b) \in R \wedge (b,c) \in S \wedge (c,d) \in T\big] \\ &\Leftrightarrow (\exists\, (b,c) \in B \times C)\big[(a,b) \in R \wedge (b,c) \in S \wedge (c,d) \in T\big] \\ &\Leftrightarrow (\exists\, b \in B)(\exists\, c \in C)\big[(a,b) \in R \wedge (b,c) \in S \wedge (c,d) \in T\big] \\ &\Leftrightarrow (\exists\, b \in B)\big[(a,b) \in R \wedge (b,d) \in T \circ S\big] \\ &\Leftrightarrow (a,d) \in (T \circ S) \circ R\,.\end{aligned}$$

Therefore, $T \circ (S \circ R) = (T \circ S) \circ R$.

(c) Let $(a, b) \in A \times B$ be given. Then

$$(a,b) \in I_B \circ R \Leftrightarrow (\exists\, c \in B)\big[(a,c) \in R \wedge (c,b) \in I_B\big]\,.$$

Note that $(c, b) \in I_B$ if and only if $c = b$; thus the fact that $b \in B$ implies that

$$(\exists\, c \in B)\big[(a,c) \in R \wedge (c,b) \in I_B\big] \Leftrightarrow (a,b) \in R\,.$$

Therefore, $(a, b) \in I_B \circ R \Leftrightarrow (a, b) \in R$. Similarly, $(a, b) \in R \circ I_A \Leftrightarrow (a, b) \in R$.

(d) Let $(a, c) \in A \times C$. Then

$$\begin{aligned}(c,a) \in (S \circ R)^{-1} &\Leftrightarrow (a,c) \in S \circ R \Leftrightarrow (\exists\, b \in B)\big[(a,b) \in R \wedge (b,c) \in S\big] \\ &\Leftrightarrow (\exists\, b \in B)\big[(c,b) \in S^{-1} \wedge (b,a) \in R^{-1}\big] \\ &\Leftrightarrow (c,a) \in R^{-1} \circ S^{-1}\,.\end{aligned}$$

□

3.2 Equivalence Relations

Definition 3.13. Let A be a set and R be a relation on A.

1. R is ***reflexive*** on A if $(\forall\, x \in A)(xRx)$ (or equivalently, $I_A \subseteq R$).
2. R is ***symmetric*** on A if $\big[\forall\, (x,y) \in A \times A\big](xRy \Leftrightarrow yRx)$ (or equivalently, $R = R^{-1}$).
3. R is ***transitive*** on A if $\big[\forall\, (x,y,z) \in A \times A \times A\big]\big[(xRy) \wedge (yRz)\big] \Rightarrow (xRz)\big]$.

A relation R on A which is reflexive, symmetric and transitive is called an ***equivalence relation*** on A.

Example 3.14. The relation "divides" on $\mathbb{N}$ is reflexive and transitive, but not symmetric. The relation "is greater than" on $\mathbb{N}$ is only transitive（遞移律）but not reflexive and transitive.

Example 3.15. Let A be a set. The relation "is a subset of" on the power set $\mathscr{P}(A)$ is reflexive, transitive but not symmetric.

Example 3.16. The relation $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x^2 = y^2\}$ is reflexive, symmetric and transitive on $\mathbb{R}$.

Example 3.17. The relation R on $\mathbb{Z}$ defined by $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \,|\, x + y \text{ is even}\}$ is reflexive, symmetric and transitive.

Remark 3.18. An equivalence relation is often denoted by $\sim$ (the same symbol as negation but $\sim$ as negation is always in front of a proposition while $\sim$ as an equivalence relation is always between two elements in a set).

Definition 3.19. Let A be a set and R be an equivalence relation on A. For $x \in A$, the ***equivalence class of*** x ***modulo*** R (or simply x ***mod*** R) is a subset of A given by

$$\bar{x} = \{y \in A \,|\, xRy\}.$$

Each element of $\bar{x}$ is called a ***representative*** of this class. The collection of all equivalence classes modulo R, called A ***modulo*** R, is denoted by A/R (and is the set $A/R = \{\bar{x} \,|\, x \in A\}$).

Example 3.20. The relation $H = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$ is an equivalence relation on the set $A = \{1, 2, 3\}$. Then

$$\bar{1} = \bar{2} = \{1, 2\} \quad \text{and} \quad \bar{3} = \{3\}.$$

Therefore, $A/H = \{\{1, 2\}, \{3\}\}$.

Theorem 3.21. *Let A be a non-empty set and R be an equivalence relation on A. For all $x, y \in A$, we have*

(a) *$x \in \bar{x}$ and $\bar{x} \subseteq A$.*

(b) *xRy if and only if $\bar{x} = \bar{y}$.*

(c) *$x \not R y$ if and only if $\bar{x} \cap \bar{y} = \varnothing$.*

Proof. It is clear that (a) holds. To see (b) and (c), it suffices to show that "$xRy \Rightarrow \bar{x} = \bar{y}$" and "$x \not R y \Rightarrow \bar{x} \cap \bar{y} = \varnothing$".

Assume that xRy. Then if $z \in \bar{x}$, we have xRz. The symmetry and transitivity of R then implies that yRz; thus $z \in \bar{y}$ which implies that $\bar{x} \subseteq \bar{y}$. Similarly, $\bar{y} \subseteq \bar{x}$; hence we conclude that "$xRy \Rightarrow \bar{x} = \bar{y}$".

Now assume that $\bar{x} \cap \bar{y} \neq \varnothing$. Then for for some $z \in A$ we have $z \in \bar{x} \cap \bar{y}$. Therefore, xRz and yRz. Since R is symmetric and transitive, then xRy which implies that "$x \not R y \Rightarrow \bar{x} \cap \bar{y} = \varnothing$". ▫

Definition 3.22. Let m be a fixed positive integer. For $x, y \in \mathbb{Z}$, we say x ***is congruent to*** y ***modulo*** m (以 m 為除數時 x 同餘 y) and write $x = y$ (***mod*** m) if m divides $(x - y)$. The number m is called the ***modulus*** of the congruence.

Example 3.23. Using 4 as the modulus, we have

$$\begin{aligned} 3 &= 3 \pmod 4 \text{ because 4 divides } 3-3=0\,,\\ 9 &= 5 \pmod 4 \text{ because 4 divides } 9-5=4\,,\\ -27 &= 1 \pmod 4 \text{ because 4 divides } -27-1=-28\,,\\ 20 &= 8 \pmod 4 \text{ because 4 divides } 20-8=12\,,\\ 100 &= 0 \pmod 4 \text{ because 4 divides } 100-0=100\,. \end{aligned}$$

Theorem 3.24. *For every fixed positive integer m, the relation "congruence modulo m" is an equivalence relation on $\mathbb{Z}$.*

Proof. It is easy to see that $x = x \pmod m$ for all $x \in \mathbb{Z}$. Therefore, congruence modulo m is reflexive on $\mathbb{Z}$.

Now we show that the relation "congruence modulo m" is symmetric. Assume that $x = y \pmod m$. Then m divides $x - y$; that is, $x - y = mk$ for some $k \in \mathbb{Z}$. Therefore, $y - x = m(-k)$ which implies that m divides $y - x$; thus $y = x \pmod m$.

Finally, we show that the relation "congruence modulo m" is transitive. Assume that $x = y \pmod m$ and $y = z \pmod m$. Then $x - y = mk$ and $y - z = m\ell$ for some $k, \ell \in \mathbb{Z}$. Therefore, $x - z = m(k + \ell)$ which implies that m divides $x - y$; thus $x = z \pmod m$. ▫

Definition 3.25. The set of equivalence classes for the relation congruence modulo m is denoted by $\mathbb{Z}_m$.

Remark 3.26. The elements of $\mathbb{Z}_m$ are sometimes called the ***residue*** (or ***remainder***) classes modulo m.

Example 3.27. For congruence modulo 4, there are four equivalence classes:

$$\begin{aligned} \overline{0} &= \{\cdots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \cdots\} = \left\{4k \,\middle|\, k \in \mathbb{Z}\right\},\\ \overline{1} &= \{\cdots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \cdots\} = \left\{4k+1 \,\middle|\, k \in \mathbb{Z}\right\},\\ \overline{2} &= \{\cdots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \cdots\} = \left\{4k+2 \,\middle|\, k \in \mathbb{Z}\right\},\\ \overline{3} &= \{\cdots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \cdots\} = \left\{4k+3 \,\middle|\, k \in \mathbb{Z}\right\}. \end{aligned}$$

In general, we will prove that the equivalence relation "congruence modulo m" produces m equivalence classes

$$\overline{j} = \left\{mk + j \,\middle|\, k \in \mathbb{Z}\right\}, \qquad j = 0, 1, \cdots, m-1\,.$$

The collection of these equivalence classes, by definition $\mathbb{Z}/(\text{mod } m)$, is usually denoted by $\mathbb{Z}_m$.

Theorem 3.28. *Let m be a fixed positive integer. Then*

(a) *For integers x and y, $x = y \pmod m$ if and only if the remainder when x is divided by m equals the remainder when y divided by m.*

(b) *$\mathbb{Z}_m$ consists of m distinct equivalence classes: $\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, \cdots, \overline{m-1}\right\}$.*

Proof. (a) For a given $x \in \mathbb{Z}$, let $\big(q(x), r(x)\big)$ denote the unique pair in $\mathbb{Z} \times \mathbb{Z}$ obtained by the division algorithm satisfying

$$x = mq(x) + r(x) \quad \text{and} \quad 0 \leqslant r(x) < m\,.$$

Then

$$\begin{aligned} x = y \pmod m \Leftrightarrow m \text{ divides } x - y &\Leftrightarrow m \text{ divides } m\big(q(x) - q(y)\big) + r(x) - r(y) \\ &\Leftrightarrow m \text{ divides } r(x) - r(y) \Leftrightarrow r(x) - r(y) = 0\,, \end{aligned}$$

where the last equivalence following from the fact that $0 \leqslant r(x), r(y) < m$.

(b) By (a), x and y are in the same equivalence classes (produced by the equivalence relation "congruence modulo m") if and only if x and y has the same remainder when they are divided by m. Therefore, we find that

$$\bar{x} = \big\{mk + r(x) \,\big|\, k \in \mathbb{Z}\big\} = \overline{r(x)} \qquad \forall\, x \in \mathbb{Z}\,.$$

Since $r(x)$ has values from $\{0, 1, \cdots, m-1\}$, we find that $\mathbb{Z}_m = \big\{\bar{0}, \bar{1}, \cdots, \overline{m-1}\big\}$. The proof is completed if we show that $\bar{k} \cap \bar{j} = \varnothing$ if $k \neq j$ and $k, j \in \{0, 1, \cdots, m-1\}$. However, if $x \in \bar{k} \cap \bar{j}$, then

$$x = mq_1 + k = mq_2 + j$$

which is impossible since $k \neq j$ and $k, j \in \{0, 1, \cdots, m-1\}$. Therefore, there are exactly m equivalence classes. □

3.3 Partitions

Definition 3.29. Let A be a non-empty set. $\mathcal{P}$ is a ***partition*** of A if $\mathcal{P}$ is a collection of subsets of A such that

(i) if $X \in \mathcal{P}$, then $X \neq \varnothing$.

(ii) if $X \in \mathcal{P}$ and $Y \in \mathcal{P}$, then $X = Y$ or $X \cap Y = \varnothing$.

(iii) $\bigcup_{X \in \mathcal{P}} X = A$.

In other words, a partition of a set A is a pairwise disjoint collection of non-empty subsets of A whose union is A.

Example 3.30. The family $\mathscr{G} = \big\{[n, n+1) \,\big|\, n \in \mathbb{Z}\big\}$ is a partition of $\mathbb{R}$.

Example 3.31. Each of the following is a partition of $\mathbb{Z}$:

1. $\mathscr{P} = \{E, D\}$, where E is the collection of even integers and D is the collection of odd integers.
2. $\mathscr{X} = \{\mathbb{N}, \{0\}, \mathbb{Z}^-\}$, where $\mathbb{Z}^-$ is the collection of negative integers.
3. $\mathscr{H} = \{A_k \,|\, k \in \mathbb{Z}\}$, where $A_k = \{3k, 3k+1, 3k+2\}$.

Theorem 3.32. *If R is an equivalent relation on a non-empty set A, then A/R is a partition of A.*

Proof. First of all, each equivalence class $\bar{x} \in A/R$ must be non-empty since it contains x. Let $\bar{x}$ and $\bar{y}$ be two equivalence classes in A/R. If $\bar{x} \cap \bar{y} \neq \varnothing$, then there exists $z \in \bar{x} \cap \bar{y}$ which implies that xRz and yRz. By the symmetry and the transitivity of R we have xRy which implies, by (b) of Theorem 3.21, that $\bar{x} = \bar{y}$.

Finally, it is clear that $\bigcup_{\bar{x} \in A/R} \bar{x} \subseteq A$ since each $\bar{x} \subseteq A$. On the other hand, since each $y \in A$ belongs to the equivalence class $\bar{y}$, we must have $A \subseteq \bigcup_{\bar{x} \in A/R} \bar{x}$. Therefore, $A = \bigcup_{\bar{x} \in A/R} \bar{x}$. ▫

Theorem 3.33. *Let $\mathcal{P}$ be a partition of a non-empty set A. For $x, y \in A$, define xQy if and only if there exists $C \in \mathcal{P}$ such that $x, y \in C$. Then*

(a) *Q is an equivalence relation on A.*

(b) *$A/Q = \mathcal{P}$.*

Proof. It is clear that Q is reflexive and symmetric on A, so it suffices to show the transitivity of Q to complete (a). Suppose that xQy and yQz. By the definition of the relation Q there exists C_1 and C_2 in $\mathcal{P}$ such that $x, y \in C_1$ and $y, z \in C_2$; hence $C_1 \cap C_2 \neq \varnothing$. Then $C_1 = C_2$ by the fact that $\mathcal{P}$ is a partition and $C_1, C_2 \in \mathcal{P}$. Therefore, $x, z \in C_1$ which implies that xQz.

Next, we claim that if $C \in \mathcal{P}$, then $x \in C$ if and only if $\bar{x} = C$. It suffices to show the direction "$\Rightarrow$" since $x \in \bar{x}$. Suppose that $C \in \mathcal{P}$ and $x \in C$.

1. "$C \subseteq \bar{x}$": Let $y \in C$ be given. By the fact that $x \in C$ we must have yQx. Therefore, $y \in \bar{x}$ which shows $C \subseteq \bar{x}$.

2. "$\bar{x} \subseteq C$": Let $y \in \bar{x}$ be given. Then there exists $\widetilde{C} \in \mathcal{P}$ such that $x, y \in \widetilde{C}$. By the fact that $x \in C$, we find that $C \cap \widetilde{C} \neq \varnothing$. Since $\mathcal{P}$ is a partition of A and $C, \widetilde{C} \in \mathcal{P}$, we must have $C = \widetilde{C}$; thus $y \in C$. Therefore, $\bar{x} \subseteq C$.

Now we show that $A/Q = \mathcal{P}$. If $C \in \mathcal{P}$, then $C \neq \varnothing$; thus there exists $x \in C$ for some $x \in A$. Then the claim above shows that $C = \bar{x} \in A/Q$. Therefore, $\mathcal{P} \subseteq A/Q$. On the other hand, if $\bar{x} \in A/Q$, by the fact that $\mathcal{P}$ is a partition of A, there exists $C \in \mathcal{P}$ such that $x \in C$. Then the claim above shows that $\bar{x} = C$. Therefore, $A/Q \subseteq \mathcal{P}$. ▫

Remark 3.34. The relation Q defined in Theorem 3.33 is called ***the equivalence relation associated with the partition*** $\mathcal{P}$.

Example 3.35. Let $A = \{1, 2, 3, 4\}$, and let $\mathcal{P} = \big\{\{1\}, \{2, 3\}, \{4\}\big\}$ be a partition of A with three sets. The equivalence relation Q associated with $\mathcal{P}$ is $\big\{(1, 1), (2, 2), (3, 3), (4, 4), (2, 3), (3, 2)\big\}$. The three equivalence classes for Q are $\overline{1} = \{1\}$, $\overline{2} = \overline{3} = \{2, 3\}$ and $\overline{4} = \{4\}$. The collection of all equivalence classes A/Q is precisely $\mathcal{P}$.

Example 3.36. The collect $\mathcal{P} = \{A_0, A_1, A_2, A_3\}$, where

$$A_0 = \{4k \,|\, k \in \mathbb{Z}\}\,, \quad A_1 = \{4k+1 \,|\, k \in \mathbb{Z}\}\,, \quad A_2 = \{4k+2 \,|\, k \in \mathbb{Z}\}\,, \quad A_3 = \{4k+3 \,|\, k \in \mathbb{Z}\}\,,$$

is a partition of $\mathbb{Z}$ because of the division algorithm. The equivalence relation associated with the partition $\mathcal{P}$ is the relation of congruence modulo 4, and each A_i is the residue class of i modulo 4 for $i = 0, 1, 2, 3$.

3.4 Modular Arithmetic

Theorem 3.37. *Let m be a positive integer and a, b, c and d be integers. If $a = c \pmod m$ and $b = d \pmod m$, then $a + b = c + d \pmod m$ and $a \cdot b = c \cdot d \pmod m$.*

Proof. Since $a = c \pmod m$ and $b = d \pmod m$, we have $a - c = mk_1$ and $b - d = mk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Then

$$a + b = c + mk_1 + d + mk_2 = c + d + m(k_1 + k_2)$$

and

$$a \cdot b = (c + mk_1) \cdot (d + mk_2) = c \cdot d + m(c \cdot k_2 + d \cdot k_1 + k_1 \cdot k_2)\,.$$

Therefore, $a + b = c + d \pmod m$ and $a \cdot b = c \cdot d \pmod m$. □

By Theorem 3.37, we are able to define the addition and the multiplication on $\mathbb{Z}_m$.

Definition 3.38. For each natural number m,

1. the ***sum of the classes*** $\bar{x}$ and $\bar{y}$ in $\mathbb{Z}_m$, denoted by $\bar{x} + \bar{y}$, is defined to be the class containing the integer $x + y$;
2. the ***product of the classes*** $\bar{x}$ and $\bar{y}$ in $\mathbb{Z}_m$, denoted by $\bar{x} \cdot \bar{y}$, is defined to be the class containing the integer $x \cdot y$.

In symbols, $\bar{x} + \bar{y} = \overline{x + y}$ and $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$.

Example 3.39. In $\mathbb{Z}_6$, $\bar{5} + \bar{3} = \bar{2}$ and $\bar{4} \cdot \bar{5} = \bar{2}$.

Example 3.40. In $\mathbb{Z}_8$, $(\bar{5} + \bar{7}) \cdot (\bar{6} + \bar{5}) = \bar{12} \cdot \bar{11} = \bar{4} \cdot \bar{3} = \bar{12} = \bar{4}$.

Example 3.41. Find $\overline{3^{63}}$ in $\mathbb{Z}_7$. Since

$$\bar{3}^{\bar{1}} = \bar{3}\,, \qquad \bar{3}^{\bar{2}} = \bar{2}\,, \qquad \bar{3}^{\bar{3}} = \bar{6}\,, \qquad \bar{3}^{\bar{4}} = \bar{4}\,, \qquad \bar{3}^{\bar{5}} = \bar{5}\,, \qquad \bar{3}^{\bar{6}} = \bar{1}\,,$$

we have $\bar{3}^{\overline{63}} = \overline{3^{60} \cdot 3^3} = \bar{6}$.

Example 3.42. For every integer k, 6 divides $k^3 + 5k$. In fact, by the division algorithm, for each $k \in \mathbb{Z}$ there exists a unique pair (q, r) such that $k = 6q + r$ for some $0 \leqslant r < 5$. Therefore, in $\mathbb{Z}_6$ we have

$$\overline{k^3 + 5k} = \overline{(6q + r)^3} + \overline{5(6q + r)} = \overline{r^3} + \overline{5 \cdot r} = \overline{r^3} + \overline{(-1) \cdot r} = \overline{r^3 - r}\,.$$

It is clear that then $\overline{k^3 + 5k} = \bar{0}$ since $\overline{0^3 - 0} = \overline{1^3 - 1} = \overline{2^3 - 2} = \overline{3^3 - 3} = \overline{4^3 - 4} = \overline{5^3 - 5}$.

Theorem 3.43. *Let m be a positive composite integer. Then there exists non-zero equivalence classes $\overline{x}$ and $\overline{y}$ in $\mathbb{Z}_m$ such that $\overline{x} \cdot \overline{y} = \overline{0}$.*

Proof. Since m is a positive composite integer, $m = x \cdot y$ for some $x, y \in \mathbb{N}$, $1 < x, y < m$. Since $1 < x, y < m$, $\overline{x}, \overline{y} \neq \overline{0}$. Therefore, in $\mathbb{Z}_m$ $\overline{0} = \overline{m} = \overline{x} \cdot \overline{y}$ which concludes the theorem. ▫

Theorem 3.44. *Let p be a prime. If $\overline{x} \cdot \overline{y} = \overline{0}$ in $\mathbb{Z}_p$, then either $\overline{x} = \overline{0}$ or $\overline{y} = \overline{0}$.*

Proof. Let $\overline{x}, \overline{y} \in \mathbb{Z}_p$ and $\overline{x} \cdot \overline{y} = \overline{0}$. Then $x \cdot y = 0 \pmod{p}$. Therefore, p divides $x \cdot y$. Since p is prime, $p|x$ or $p|y$ which implies that $\overline{x} = \overline{0}$ or $\overline{y} = \overline{0}$. ▫

Theorem 3.45 (Cancellation Law for $\mathbb{Z}_p$)**.** *Let p be a prime. If $xy = xz \pmod{p}$ and $x \neq 0 \pmod{p}$, then $y = z \pmod{p}$.*

Proof. If $xy = xz \pmod{p}$, then $x(y - z) = 0 \pmod{p}$. By the previous theorem $\overline{x} = \overline{0}$ or $\overline{y - z} = \overline{0}$. Since $x \neq 0 \pmod{p}$, we must have $\overline{y} = \overline{z}$; thus $y = z \pmod{p}$. ▫

4 Functions

4.1 Functions as Relations

Definition 4.1. Let A and B be sets. A ***function*** $f : A \to B$ consists of two sets A and B together with a "rule" that assigns to each $x \in A$ a special element of B denoted by $f(x)$. One writes $x \mapsto f(x)$ to denote that x is mapped to the element $f(x)$. A is called the ***domain*** (定義域) of f, and B is called the ***target*** or ***co-domain*** of f. The ***range*** (値域) of f or the ***image*** of f, is the subset of B defined by $f(A) = \{f(x) \,|\, x \in A\}$.

Each function is associated with a collection of ordered pairs $\{(x, f(x)) \,|\, x \in A\} \subseteq A \times B$. Since a collection of ordered pairs is a relation, we can say that a function is a relation from one set to another. However, not every relation can serve as a function. The relation $R = \{(1, 5), (2, 7), (1, 8)\}$ cannot describe a function since two numbers 5 and 9 are assigned to 1. Therefore, a function must be a relation with additional special properties and we have the following

Definition 4.2 (Alternative Definition of Functions)**.** A ***function*** (or ***mapping***) from A to B is a relation f from A to B such that

(i) the domain of f is A; that is, $(\forall x \in A)(\exists y \in B)((x, y) \in f\,)$, and

(ii) if $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.

We write $f : A \to B$, and this is read "f is a function from A to B" or "f maps A to B". The set B is called the ***co-domain*** of f. In the case where $B = A$, we say f is a function on A.

When $(x, y) \in f$, we write $y = f(x)$ instead of xfy. We say that y is the ***image*** of f at x (or value of f at x) and that x is a ***pre-image*** of y.

Remark 4.3. A function has only one domain and one range but many possible co-domains.

Remark 4.4. A function on $\mathbb{R}$ is usually called a real-valued function or simply real function. The domain of a real function is usually understood to be the largest possible subset of $\mathbb{R}$ on which the function takes values.

Definition 4.5. A function x with domain $\mathbb{N}$ is called an ***infinite sequence***, or simply a ***sequence***. The image of the natural number n is usually written as x_n instead of $x(n)$ and is called the ***n-th term of the sequence***.

Definition 4.6. Let A, B be sets, and $A \subseteq B$.

1. The the ***identity function/map*** on A is the function $I_A : A \to A$ given by $I_A(x) = x$ for all $x \in A$.

2. The ***inclusion function/map*** from A to B is the function $\iota : A \to B$ given by $\iota(x) = x$ for all $x \in A$.

3. The ***characteristic/indicator function*** of A (defined on B) is the map $\mathbf{1}_A : B \to \mathbb{R}$ given by
$$\mathbf{1}_A(x) = \begin{cases} 1 & \text{if } x \in A\,, \\ 0 & \text{if } x \in B \backslash A\,. \end{cases}$$

4. The ***greatest integer function*** on $\mathbb{R}$ is the function $[\cdot] : \mathbb{R} \to \mathbb{Z}$ given by
$$[x] = \text{the largest integer which is not greater than } x\,.$$
The function $[\cdot]$ is also called the ***floor function*** or the ***Gauss function***.

5. Let R be an equivalence relation on A. The ***canonical map*** for the equivalence relation R is the map from A to A/R which maps $x \in A$ to $\bar{x}$, the equivalence class of x modulo R.

Theorem 4.7. *Two functions f and g are equal if and only if*

(i) $\mathrm{Dom}(f) = \mathrm{Dom}(g)$, *and*

(ii) *for all $x \in \mathrm{Dom}(f)$, $f(x) = g(x)$.*

Example 4.8. The identity map of A and the inclusion map from A to B are identical functions.

Example 4.9. $f(x) = \dfrac{x}{x}$ and $g(x) = 1$ are different functions since they have different domains.

Remark 4.10. When a rule of correspondence assigns more than one values to an object in the domain, we say "the function is not well-defined", meaning that it is not really a function. A proof that a function is well-defined is nothing more than a proof that the relation defined by a given rule is single valued.

Example 4.11. Let $\bar{x}$ denote the equivalence class of x modulo the congruence relation modulo 4 and $\widetilde{y}$ denote the equivalence class of y modulo the congruence relation modulo 10. Define $f(\bar{x}) = \widetilde{2 \cdot x}$. Then this "function" is not really a function since $\bar{0} = \bar{4}$ but $\widetilde{2 \cdot 0} = \widetilde{0}$ while $\widetilde{2 \cdot 4} = \widetilde{8} \neq \widetilde{0}$. In other words, the way f assigns value to $\bar{x}$ is not well-defined.

Example 4.12. Let $\bar{x}$ denote the equivalence class of x modulo the congruence relation modulo 8 and $\widetilde{y}$ denote the equivalence class of y modulo the congruence relation modulo 4. The function $f : \mathbb{Z}_8 \to \mathbb{Z}_4$ given by $f(\bar{x}) = \widetilde{x+2}$ is well-defined. To see this, suppose that $\bar{x} = \bar{z}$ in $\mathbb{Z}_8$. Then 8 divides $x - z$ which implies that 4 divides $x - z$; thus 4 divides $(x + 2) - (z + 2)$. Therefore, $x + 2 = z + 2 \pmod 4$ or equivalently, $\widetilde{x+2} = \widetilde{z+2}$. So f is well-defined.

4.2 Constructions of Functions

Definition 4.13. Let $f : A \to B$ and $g : B \to C$ be functions. The ***inverse*** of f is the relation from B to A:
$$f^{-1} = \big\{(y, x) \in B \times A \,\big|\, y = f(x)\big\} = \big\{(y, x) \in B \times A \,\big|\, (x, y) \in f\big\}\,.$$

When f^{-1} describes a function, f^{-1} is called the ***inverse function/map*** of f.

The ***composite*** of f and g is the relation from A to C:

$$g \circ f = \big\{(x,z) \in A \times C \,\big|\, \text{there exists (a unique) } y \in B \text{ such that } (x,y) \in f \text{ and } (y,z) \in g\big\}.$$

Remark 4.14. Using the notation in Definition 4.2, if $(x,z) \in g \circ f$, then $z = (g \circ f)(x)$. On the other hand, if $(x,z) \in g \circ f$, there exists (a unique) $y \in B$ such that $(x,y) \in f$ and $(y,z) \in g$. Then $y = f(x)$ and $z = g(y)$. Therefore, we also have $z = g(f(x))$; thus $(g \circ f)(x) = g(f(x))$.

Theorem 4.15. *Let A, B and C be sets, and $f : A \to B$ and $g : B \to C$ be functions. Then $g \circ f$ is a function from A to C, and* $\mathrm{Dom}(g \circ f) = A$.

Proof. By the definition of composition of relations, $g \circ f$ is a relation from A to C.

1. First, we show that $\mathrm{Dom}(g \circ f) = A$. Clearly $\mathrm{Dom}(g \circ f) \subseteq A$, so it suffices to show that $A \subseteq \mathrm{Dom}(g \circ f)$. Let $x \in A$. Since $f : A \to B$ is a function, there exists $y \in B$ such that $(x,y) \in f$. Since $g : B \to C$ is a function, there exists $z \in C$ such that $(y,z) \in g$. This shows that for every $x \in A$, there exists $z \in C$ such that $(x,z) \in g \circ f$; thus $\mathrm{Dom}(g \circ f) = A$.

2. Next, we show that if $(x,z_1) \in g \circ f$ and $(x,z_2) \in g \circ f$, then $z_1 = z_2$. Suppose that $(x,z_1) \in g \circ f$ and $(x,z_2) \in g \circ f$. Then there exists $y_1, y_2 \in B$ such that $(x,y_1) \in f$ and $(y_1,z_1) \in g$, while $(x,y_2) \in f$ and $(y_2,z_2) \in g$. Since f is a function, $y_1 = y_2$; thus that g is a function implies that $z_1 = z_2$. □

Theorem 4.16. *Let A, B, C, D be sets, and $f : A \to B$, $g : B \to C$, $h : C \to D$ be functions. Then $h \circ (g \circ f) = (h \circ g) \circ f$.*

Proof. We note that both functions $h \circ (g \circ f)$ and $(h \circ g) \circ f$ have A as their domains, so by Theorem 4.7 it suffices to shows that for all $x \in A$, $\big(h \circ (g \circ f)\big)(x) = \big((h \circ g) \circ f\big)(x)$. Nevertheless,

$$\big(h \circ (g \circ f)\big)(x) = h\big((g \circ f)(x)\big) = h\big(g(f(x))\big) = (h \circ g)(f(x)) = \big((h \circ g) \circ f\big)(x).$$ □

Similarly, Theorem 4.7 can be applied to prove the following two theorems.

Theorem 4.17. *Let $f : A \to B$ be a function. Then $f \circ I_A = f$ and $I_B \circ f = f$.*

Theorem 4.18. *Let $f : A \to B$ be a function, and $C = \mathrm{Rng}(f)$. If $f^{-1} : C \to A$ is a function, then $f^{-1} \circ f = I_A$ and $f \circ f^{-1} = I_C$.*

Definition 4.19. Let $f : A \to B$ be a function, and $D \subseteq A$. The ***restriction*** of f to D, denoted by $f|_D$, is the function

$$f|_D = \big\{(x,y) \,\big|\, y = f(x) \text{ and } x \in D\big\}.$$

If g and h are functions and g is a restriction of h, the h is called an ***extension*** of g.

Since functions now are treated as sets (of ordered pairs), we can talk about the unions and intersections of functions.

Example 4.20. Let F and G be functions

$$F = \big\{(1,2),(2,6),(3,-9),(5,7)\big\},$$
$$G = \big\{(1,8),(2,6),(4,8),(5,7),(8,3)\big\}.$$

Then $F \cap G = \big\{(2,6),(5,7)\big\}$ is a function with domain $\{2,5\}$ which is a proper subset of $\mathrm{Dom}(F) \cap \mathrm{Dom}(G) = \{1,2,5\}$.

On the other hand, $\big\{(1,2),(1,8)\big\} \subseteq F \cup G$; thus $F \cup G$ cannot be a function.

It turns out that if f and g are functions, then $f \cap g$ is always a function and $f \cap g$ can be defined as the restriction of either f and g. To be more precise, we have the following

Theorem 4.21. *Suppose that f and g are functions. Then $f \cap g$ is a function with domain $A = \big\{x \,\big|\, f(x) = g(x)\big\}$, and*

$$f \cap g = f|_A = g|_A\,.$$

Proof. Let $(x,y) \in f \cap g$. Then $y = f(x) = g(x)$; thus

$$\mathrm{Dom}(f \cap g) = \big\{x \,\big|\, f(x) = g(x)\big\}\,.$$

Write $f = \big\{(x,f(x)) \,\big|\, x \in \mathrm{Dom}(f)\big\}$ and $g = \big\{(x,g(x)) \,\big|\, x \in \mathrm{Dom}(g)\big\}$, and let $A = \big\{x \,\big|\, f(x) = g(x)\big\}$. If $(x,y_1),(x,y_2) \in f \cap g$, $(x,y_1),(x,y_2) \in f$ which, by the fact that f is a function, implies that $y_1 = y_2$. Therefore, $f \cap g$ is a function. Moreover,

$$f \cap g = \big\{(x,y) \,\big|\, \exists\, x \in A, y = f(x)\big\}$$

which implies that $f \cap g = f|_A$. □

For $f \cup g$ being a function, it is (sufficient and) necessary that if $x \in \mathrm{Dom}(f) \cap \mathrm{Dom}(g)$, then $f(x) = g(x)$. Moreover, if $f \cup g$ is a function, then $f = (f \cup g)|_{\mathrm{Dom}(f)}$ and $g = (f \cup g)|_{\mathrm{Dom}(g)}$. In particular, we have the following

Theorem 4.22. *Let f and g be functions with $\mathrm{Dom}(f) = A$ and $\mathrm{Dom}(g) = B$. If $A \cap B = \varnothing$, then $f \cup g$ is a function with domain $A \cup B$. Moreover,*

$$(f \cup g)(x) = \begin{cases} f(x) & \text{if } x \in A\,, \\ g(x) & \text{if } x \in B\,. \end{cases} \tag{4.1}$$

Proof. Clearly $\mathrm{Dom}(f \cup g) = A \cup B$. Suppose that $(x,y_1),(x,y_2) \in f \cup g$. If $(x,y_1) \in f$, then $x \in \mathrm{Dom}(f)$; thus by the fact that $A \cap B = \varnothing$, we must have $(x,y_2) \in f$. Since f is a function, $y_1 = f(x) = y_2$. Similarly, if $(x,y_1) \in g$, then $(x,y_2) \in g$ which also implies that $y_1 = g(x) = y_2$. Therefore, $f \cup g$ is a function and (4.1) is valid. □

Definition 4.23. Let f be a real-valued function defined on an interval $I \subseteq \mathbb{R}$.

1. The function f is said to be $\begin{matrix} \textbf{\textit{increasing}} \\ \textbf{\textit{decreasing}} \end{matrix}$ on I if $x \leqslant y$ implies that $\begin{matrix} f(x) \leqslant f(y) \\ f(x) \geqslant f(y) \end{matrix}$ for all $x, y \in I$.
2. The function f is said to be $\begin{matrix} \textbf{\textit{strictly increasing}} \\ \textbf{\textit{strictly decreasing}} \end{matrix}$ on I if $x < y$ implies that $\begin{matrix} f(x) < f(y) \\ f(x) > f(y) \end{matrix}$ for all $x, y \in I$.

4.3 Functions that are Onto; One-to-One Functions

Definition 4.24. Let $f : A \to B$ be a function.

1. The function f is said to be ***surjective*** or ***onto*** B if $\mathrm{Rng}(f) = B$. When f is surjective, f is called a surjection, and we write $f : A \xrightarrow{\text{onto}} B$.

2. The function f is said to be ***injective*** or ***one-to-one*** if it holds that "$f(x) = f(y) \Rightarrow x = y$". When f is injective, f is called a injection, and we write $f : A \xrightarrow{1-1} B$.

3. The function f is called a ***bijection*** if it is both injective and surjective. When f is a bijection, we write $f : A \xrightarrow[onto]{1-1} B$.

Remark 4.25. 1. It is always true that $\mathrm{Rng}(f) \subseteq B$; thus $f : A \to B$ is onto if and only if $B \subseteq \mathrm{Rng}(f)$. In other words, $f : A \to B$ is onto if and only if every $b \in B$ has a pre-image. Therefore, to prove that $f : A \to B$ is onto B, it is sufficient to show that for every $b \in B$ there exists $a \in A$ such that $f(a) = b$.

2. The direct proof of that $f : A \to B$ is injective is to verify the property that "$f(x) = f(y) \Rightarrow x = y$". A proof of the injectivity of f by contraposition assumes that $x \neq y$ and one needs to show that $f(x) \neq f(y)$.

Theorem 4.26. (a) *If $f : A \to B$ is onto B and $g : B \to C$ is onto C, then $g \circ f$ is onto C.*

(b) *If $f : A \to B$ is one-to-one and $g : B \to C$ is one-to-one, then $g \circ f$ is one-to-one.*

Proof. 1. Let $c \in C$. By the surjectivity of g, there exists $b \in B$ such that $g(b) = c$. The surjectivity of f then implies the existence of $a \in A$ such that $f(a) = b$. Therefore, $(g \circ f)(a) = g(f(a)) = g(b) = c$ which concludes (a).

2. Assume that $(g \circ f)(x) = (g \circ f)(y)$. Then $g(f(x)) = g(f(y))$; thus by the injectivity of g, $f(x) = f(y)$. Therefore, the injectivity of f implies that $x = y$ which concludes (b). □

By Theorem 4.26, we can easily conclude the following

Theorem 4.27. *If $f : A \to B$, $g : B \to C$ are bijections, then $g \circ f : A \to C$ is a bijection.*

Theorem 4.28. *Let $f : A \to B$ and $g : B \to C$ be functions.*

(a) *If $g \circ f$ is onto C, then g is onto C.*

(b) *If $g \circ f$ is one-to-one, then f is one-to-one.*

Proof. (a) Let $c \in C$. Since $g \circ f$ is onto C, there exists $a \in A$ such that $(g \circ f)(a) = c$. Let $b = f(a)$. Then $g(b) = g(f(a)) = (g \circ f)(a) = c$.

(b) Suppose that $f(x) = f(y)$. Then $(g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y)$, and the injectivity of $g \circ f$ implies that $x = y$. □

Remark 4.29. In part (a) of Theorem 4.28, we cannot conclude that f is also onto B since there might be a proper subset $\widetilde{B} \subsetneq B$ such that $f : A \to \widetilde{B}$, $g : \widetilde{B} \to C$ and $g \circ f$ is onto C. For example, Let $A = B = \mathbb{R}$, $C = \mathbb{R}^+ \cup \{0\}$, and $f(x) = g(x) = x^2$. Then clearly f is not onto B but $g \circ f$ is onto C.

In part (b) of Theorem 4.28, we cannot conclue that g is one-to-one since it might happen that g is one-to-one on $\mathrm{Rng}(f) \subsetneq B$ but g is not one-to-one on B. For example, let $A = C = \mathbb{R}^+ \cup \{0\}$, $B = \mathbb{R}$, and $f(x) = x^2$, $g(x) = \log(1 + |x|)$. Then clearly g is not one-to-one, but $g \circ f$ is one-to-one.

Theorem 4.30. *If $f : A \to B$ is one-to-one, then every restriction of f is one-to-one.*

Theorem 4.31. *Let $f : A \to C$ and $g : B \to D$ be functions. Suppose that A and B are disjoint sets.*

(a) *If f is onto C and g is onto D, then $f \cup g : A \cup B \to C \cup D$ is onto $C \cup D$.*

(b) *If f is one-to-one, g is one-to-one, and C and D are disjoint, then $f \cup g : A \cup B \to C \cup D$ is one-to-one.*

Proof. We note that Theorem 4.22 implies that $f \cup g : A \cup B \to C \cup D$ is a function.

(a) Let $y \in C \cup D$. Then $y \in C$ or $y \in D$. W.L.O.G., we can assume that $y \in C$. Since $f : A \to C$ is onto C, there exists $x \in A$ such that $(x, y) \in f$. By Theorem 4.22, $(f \cup g)(x) = f(x) = y$. Therefore, $f \cup g$ is onto $C \cup D$.

(b) Suppose that $(x_1, y), (x_2, y) \in f \cup g \subseteq (A \times C) \cup (B \times D)$. Then $(x_1, y) \in f$ or $(x_1, y) \in g$. W.L.O.G., we can assume that $(x_1, y) \in f$. Since $f \subseteq A \times C$ and $g \subseteq B \times D$, by the fact that $C \cap D = \varnothing$ we must have $(x_2, y) \in f$ for otherwise $y \in C \cap D$, a contradiction.

Now, since $(x_1, y), (x_2, y) \in f$, the injectivity of f then implies that $x_1 = x_2$. ▫

4.4 Inverse Functions

We recall that the inverse of a function $f : A \to B$ is the relation

$$y f^{-1} x \Leftrightarrow x f y \Leftrightarrow (x, y) \in f \Leftrightarrow y = f(x)\,.$$

This relation is a function, called the inverse function of f, if the relation itself is a function with certain domain.

Definition 4.32. A function $f : A \to B$ is said to be an ***one-to-one correspondence*** if f is a bijection.

Theorem 4.33. *Let $f : A \to B$ be a function.*

(a) *f^{-1} is a function from $\mathrm{Rng}(f)$ to A if and only if f is one-to-one.*

(b) *If f^{-1} is a function, then f^{-1} is one-to-one.*

Proof. (a) "⇒" If $(x_1, y), (x_2, y) \in f$, then $(y, x_1), (y, x_2) \in f^{-1}$. Since f^{-1} is a function, we must have $x_1 = x_2$. Therefore, f is one-to-one.

"⇐" If $(y, x_1), (y, x_2) \in f^{-1}$, then $(x_1, y), (x_2, y) \in f$, and the injectivity of f implies that $x_1 = x_2$. Therefore, Theorem 3.8 implies that f^{-1} is a function with domain $\text{Rng}(f)$.

(b) Suppose that f^{-1} is a function, and $(y_1, x), (y_2, x) \in f^{-1}$. Then $(x, y_1), (x, y_2) \in f$ which, by the fact that f is a function, implies that $y_1 = y_2$. Therefore, f^{-1} is one-to-one. □

Corollary 4.34. *The inverse of a one-to-one correspondence is a one-to-one correspondence.*

Theorem 4.35. *Let $f : A \to B$, $g : B \to A$ be functions. Then*

(a) *$g = f^{-1}$ if and only if $g \circ f = I_A$ and $f \circ g = I_B$ (if and only if $f = g^{-1}$).*

(b) *If f is surjective, and $g \circ f = I_A$, then $g = f^{-1}$.*

(c) *If f is injective, and $f \circ g = I_B$, then $g = f^{-1}$.*

Proof. We first prove the following two claims:

(1) If $g \circ f = I_A$, then $f^{-1} \subseteq g$. (2) If $f \circ g = I_B$, then $g \subseteq f^{-1}$.

To see (1), let $(y, x) \in f^{-1}$ be given. Then $(x, y) \in f$ or $y = f(x)$. Since $(g \circ f) = I_A$, we must have

$$g(y) = g(f(x)) = (g \circ f)(x) = I_A(x) = x$$

or equivalently, $(y, x) \in g$. Therefore, $f^{-1} \subseteq g$.

To see (2), let $(y, x) \in g$ be given. Then $x = g(y)$; thus the fact that $(f \circ g) = I_B$ implies that

$$f(x) = f(g(y)) = (f \circ g)(y) = I_B(y) = y$$

or equivalently, $(x, y) \in f$. Therefore, $(y, x) \in f^{-1}$; thus $g \subseteq f^{-1}$.

(a) "⇒" This direction is a direct consequence of Theorem 4.18.

"⇐" This direction is a direct consequence of the claims above.

(b) Suppose that $f : A \to B$ is surjective and $g \circ f = I_A$. Then claim (1) implies that $f^{-1} \subseteq g$; thus it suffices to show that $g \subseteq f^{-1}$. Let $(y, x) \in g$. Then by the surjectivity of f there exists $x_1 \in A$ such that $y = f(x_1)$ or equivalently, $(y, x_1) \in f^{-1}$. On the other hand,

$$x = g(y) = g(f(x_1)) = (g \circ f)(x_1) = I_A(x_1) = x_1 \,.$$

Therefore, $g \subseteq f^{-1}$.

(c) Now suppose that $f : A \to B$ is injective and $f \circ g = I_B$. Then claim (2) implies that $g \subseteq f^{-1}$; thus it suffices to show that $f^{-1} \subseteq g$. Let $(y, x) \in f^{-1}$ or equivalently, $(x, y) \in f$ or $y = f(x)$. By the fact that $f \circ g = I_B$, we have $f(g(y)) = y$; thus the injectivity of f implies that $g(y) = x$ or $(y, x) \in g$. Therefore, $f^{-1} \subseteq g$ which completes the proof. □

Corollary 4.36. *If $f : A \to B$ is a one-to-one correspondence, and $g : B \to A$ be a function. Then $g = f^{-1}$ if and only if $g \circ f = I_A$ or $f \circ g = I_B$.*

Example 4.37. Let $A = \mathbb{R}$ and $B = \{x \,|\, x \geqslant 0\}$. Define $f : A \to B$ by $f(x) = x^2$ and $g : B \to A$ by $g(y) = \sqrt{y}$. Then $f \circ g = I_B$ but g is not inverse function of f since $(g \circ f)(x) = |x|$ for all $x \in A$.

Definition 4.38. Let A be a non-empty set. A ***permutation*** of A is a one-to-one correspondence from A onto A.

Theorem 4.39. *Let A be a non-empty set. Then*

(a) *the identity map I_A is a permutation of A.*

(b) *the composite of permutations of A is a permutation of A.*

(c) *the inverse of a permutation of A is a permutation of A.*

(d) *if f is a permutation of A, then $f \circ I_A = I_A \circ f = f$.*

(e) *if f is a permutation of A, then $f \circ f^{-1} = f^{-1} \circ f = I_A$.*

(f) *if f and g are permutations of A, then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

4.5 Set Images

Definition 4.40. Let $f : A \to B$ be a function, and $X \subseteq A$, $Y \subseteq B$. The ***image*** of X (under f) or ***image set*** of X, denoted by $f(X)$, is the set

$$f(X) = \left\{y \in B \,\middle|\, y = f(x) \text{ for some } x \in X\right\} = \left\{f(x) \,\middle|\, x \in X\right\},$$

and the ***pre-image*** of Y (under f) or the ***inverse image*** of Y, denoted by $f^{-1}(Y)$, is the set

$$f^{-1}(Y) = \left\{x \in A \,\middle|\, f(x) \in Y\right\}.$$

Remark 4.41. Here are some facts about images of sets that follow from the definitions:

(a) If $a \in D$, then $f(a) \in f(D)$.

(b) If $a \in f^{-1}(E)$, then $f(a) \in E$.

(c) If $f(a) \in E$, then $a \in f^{-1}(E)$.

(d) If $f(a) \in f(D)$ and f is one-to-one, then $a \in D$.

Theorem 4.42. *Let $f : A \to B$ be a function. Suppose that C, D are subsets of A, and E, F are subsets of B. Then*

(a) *$f(C \cap D) \subseteq f(C) \cap f(D)$. In particular, if $C \subseteq D$, then $f(C) \subseteq f(D)$.*

(b) $f(C \cup D) = f(C) \cup f(D)$.

(c) $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$. *In particular, if* $E \subseteq F$, *then* $f^{-1}(E) \subseteq f^{-1}(F)$.

(d) $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$.

(e) $C \subseteq f^{-1}(f(C))$.

(f) $f(f^{-1}(E)) \subseteq E$.

Proof. (a) Let $y \in f(C \cap D)$. Then there exists $x \in C \cap D$ such that $y = f(x)$. Therefore, $y \in f(C)$ and $y \in f(D)$; thus $y \in f(C) \cap f(D)$.

(b) Let $y \in B$ be given. Then

$$\begin{aligned} y \in f(C \cup D) &\Leftrightarrow (\exists\, x \in C \cup D)\big(y = f(x)\big) \Leftrightarrow (\exists\, x \in C)\big(y = f(x)\big) \vee (\exists\, x \in D)\big(y = f(x)\big) \\ &\Leftrightarrow \big(y \in f(C)\big) \vee \big(y \in f(D)\big) \Leftrightarrow y \in f(C) \cup f(D)\,. \end{aligned}$$

(c) Let $x \in A$ be given. Then

$$\begin{aligned} x \in f^{-1}(E \cap F) &\Leftrightarrow f(x) \in E \cap F \Leftrightarrow \big(f(x) \in E\,\big) \wedge \big(f(x) \in F\,\big) \\ &\Leftrightarrow \big(x \in f^{-1}(E)\big) \wedge \big(x \in f^{-1}(F)\big) \Leftrightarrow x \in f^{-1}(E) \cap f^{-1}(F)\,. \end{aligned}$$

(d) Let $x \in A$ be given. Then

$$\begin{aligned} x \in f^{-1}(E \cup F) &\Leftrightarrow f(x) \in E \cup F \Leftrightarrow \big(f(x) \in E\,\big) \vee \big(f(x) \in F\,\big) \\ &\Leftrightarrow \big(x \in f^{-1}(E)\big) \vee \big(x \in f^{-1}(F)\big) \Leftrightarrow x \in f^{-1}(E) \cup f^{-1}(F)\,. \end{aligned}$$

(e) Let $x \in C$. Then $f(x) \in f(C)$; thus $x \in f(f^{-1}(C))$. Therefore, $C \subseteq f^{-1}(f(C))$.

(f) Suppose that $y \in f(f^{-1}(E))$. Then there exists $x \in f^{-1}(E)$ such that $f(x) = y$. Since $x \in f^{-1}(E)$, there exists $z \in E$ such that $f(x) = z$. Then $y = z$ which implies that $y \in E$. Therefore, $f(f^{-1}(E)) \subseteq E$. ▫

Remark 4.43. 1. In part (a) of Theorem 4.42, it is possible that $f(C \cap D) \subsetneq f(C) \cap f(D)$. For example, $f(x) = x^2$, $C = (-\infty, 0)$ and $D = (0, \infty)$. Then $C \cap D = \varnothing$ which implies that $f(C \cap D) = \varnothing$; however, $f(C) = f(D) = (0, \infty)$.

2. In part (e) of Theorem 4.42, it is possible that $C \subsetneq f^{-1}(f(C))$. For example, if $f(x) = x^2$ and $C = [0, 1]$, then $f^{-1}(f(C)) = f^{-1}([0, 1]) = [-1, 1] \supsetneq [0, 1]$.

3. In part (f) of Theorem 4.42, it is possible that $f(f^{-1}(E)) \subsetneq E$. For example, if $f(x) = x^2$ and $E = [-1, 1]$, then $f(f^{-1}(E)) = f([0, 1]) = [0, 1] \subsetneq [-1, 1]$.

5 Cardinality

5.1 Equivalent Sets; Finite Sets

Definition 5.1. Two sets A and B are ***equivalent*** if there exists a one-to-one function from A onto B. The sets are also said to be ***in one-to-one correspondence***, and we write $A \approx B$.

If A and B are not equivalent, we write $A \not\approx B$.

Example 5.2. The set of even integers is equivalent to the set of odd integers.

Example 5.3. For $a, b, c, d \in \mathbb{R}$, with $a < b$ and $c < d$, the open intervals (a, b) and (c, d) are equivalent. Therefore, any two open intervals are equivalent, even when the intervals have different length.

Example 5.4. Let $\mathscr{F}$ be the set of all binary sequences; that is, the set of all functions from $\mathbb{N} \to \{0, 1\}$. Then $\mathscr{F} \approx \mathscr{P}(\mathbb{N})$, the power set of $\mathbb{N}$. To see this, we define $\phi : \mathscr{F} \to \mathscr{P}(\mathbb{N})$ by $\phi(x) \equiv \left\{k \in \mathbb{N} \,\middle|\, x_k = 1\right\}$ for all $x \in \mathscr{F}$. Then ϕ is well-defined and $\phi : \mathscr{F} \xrightarrow[onto]{1-1} \mathscr{P}(\mathbb{N})$.

Theorem 5.5. *Equivalence of sets is an equivalence relation on the class of all sets.*

Proof. 1. Reflexivity: for all sets A, the identity map I_A is a one-to-one correspondence on A.

2. Symmetry: Suppose that $A \approx B$; that is, there exists a one-to-one correspondence ϕ from A to B. Then Theorem 4.33 ϕ^{-1} is a one-to-one correspondence from B to A; thus $B \approx A$.

3. Transitivity: Suppose that $A \approx B$ and $B \approx C$. Then there exist one-to-one correspondences $\phi : A \xrightarrow[onto]{1-1} B$ and $\psi : B \xrightarrow[onto]{1-1} C$. By Theorem 4.27, we conclude that $\psi \circ \phi : A \to C$ is an one-to-one correspondence; thus $A \approx C$. ▫

Lemma 5.6. *Suppose that A, B, C and D are sets with $A \approx C$ and $B \approx D$.*

(a) *If A and B are disjoint and C and D are disjoint, then $A \cup B \approx C \cup D$.*

(b) *$A \times B \approx C \times D$.*

Proof. Suppose that $\phi : A \xrightarrow[onto]{1-1} C$ and $\psi : B \xrightarrow[onto]{1-1} D$.

(a) Then Theorem 4.31 implies that $\phi \cup \psi : A \cup B \to C \cup D$ is a one-to-one correspondence.

(b) Let $f : A \times B \to C \times D$ be given by $f(a, b) = \big(\phi(a), \psi(b)\big)$. Then f is a one-to-one correspondence from $A \times B$ to $C \times D$. ▫

Definition 5.7. For each natural number k, let $\mathbb{N}_k = \{1, 2, \cdots, k\}$. A set S is ***finite*** if $S = \varnothing$ or $S \approx \mathbb{N}_k$ for some $k \in \mathbb{N}$. A set S is ***infinite*** if S is not a finite set.

Definition 5.8. Let S be a finite set. If $S = \varnothing$, then S has ***cardinal number*** 0 (or ***cardinality*** 0), and we write $\#S = 0$. If $S \approx \mathbb{N}_k$ for some natural number k, then S has ***cardinal number*** k (or ***cardinality*** k), and we write $\#S = k$.

Remark 5.9. 1. In the definition above, we have to make sure that $\mathbb{N}_k \not\approx \mathbb{N}_j$ if $k \neq j$ (otherwise the cardinality is not well-defined). Suppose that $\phi : \mathbb{N}_k \to \mathbb{N}_j$ is a one-to-one correspondence. By Theorem 5.5 we can assume that $k \leqslant j$. If $k < j$, then $\phi(\mathbb{N}_k) = \big\{\phi(1), \phi(2), \cdots, \phi(k)\big\} \neq \mathbb{N}_j$ since the number of elements in $\phi(\mathbb{N}_k)$ and $\mathbb{N}_j$ are different. In other words, if $k < j$, $\phi : \mathbb{N}_k \to \mathbb{N}_j$ cannot be surjective. This implies that $\mathbb{N}_k \approx \mathbb{N}_j$ if and only if $k = j$.

2. The cardinality of a set S can also be denoted by $n(S)$, $\bar{\bar{S}}$, $\mathrm{card}(S)$ as well.

Theorem 5.10. *If A is finite and $B \approx A$, then B is finite.*

Lemma 5.11. *If S is a finite set with cardinality k and x is any object not in S, then $S \cup \{x\}$ is finite and has cardinality $k + 1$.*

Lemma 5.12. *For every $k \in \mathbb{N}$, every subset of $\mathbb{N}_k$ is finite.*

Proof. We prove by induction. Let $S = \big\{k \in \mathbb{N} \,\big|\, \text{the statement "every subset of } \mathbb{N}_k \text{ is finite" holds}\big\}$.

1. There are only two subsets of $\mathbb{N}_1$, namely $\varnothing$ and $\mathbb{N}_1$. Since $\varnothing$ and $\mathbb{N}_1$ are both finite, we have $1 \in S$.

2. Suppose that $k \in S$. Then every subset of $\mathbb{N}_k$ is finite. Since $\mathbb{N}_{k+1} = \mathbb{N}_k \cup \{k+1\}$, every subset of $\mathbb{N}_{k+1}$ is either a subset of $\mathbb{N}_k$, or the union of a subset of $\mathbb{N}_k$ and $\{k+1\}$. By the fact that $k \in S$, we conclude from Lemma 5.11 that every subset of $\mathbb{N}_{k+1}$ is finite.

Therefore, **PMI** implies that $S = \mathbb{N}$. □

Theorem 5.13. *Every subset of a finite set is finite.*

Theorem 5.14. (a) *If A and B are disjoint finite sets, then $A \cup B$ is finite, and $\#(A \cup B) = \#A + \#B$.*

(b) *If A and B are finite sets, then $A \cup B$ is finite, and $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.*

(c) *If $A_1, A_2, \cdots, A_n$ are finite sets, then $\bigcup_{k=1}^{n} A_k$ is finite.*

Proof. (a) W.L.O.G., we assume that $A \approx \mathbb{N}_k$ and $B \approx \mathbb{N}_\ell$ for some $k, \ell \in \mathbb{N}$. Let $H = \{k+1, k+2, \cdots, k+\ell\}$. Then $\mathbb{N}_\ell \approx H$ since $\phi(x) = k + x$ is a one-to-one correspondence from $\mathbb{N}_\ell \to \{k+1, k+2, \cdots, k+\ell\}$. By part (a) of Lemma 5.6, we conclude that $A \cup B \approx \mathbb{N}_k \cup H = \mathbb{N}_{k+\ell}$; thus $\#(A \cup B) = \#A + \#B$.

(b) Note that $A \cup B$ is the disjoint union of A and $B \backslash A$, where $B \backslash A$ is a subset of a finite set B which makes $B \backslash A$ a finite set. Therefore, $A \cup B$ is finite.

To see $\#(A \cup B) = \#A + \#B - \#(A \cap B)$, using (a) it suffices to show that $\#(B \backslash A) = \#B - \#(A \cap B)$. Nevertheless, note that $B = (B \backslash A) \cup (A \cap B)$ in which the union is in fact a disjoint union; thus (a) implies that

$$\#B = \#(B \backslash A) + \#(A \cap B) \quad \text{or equivalently,} \quad \#(B \backslash A) = \#B - \#(A \cap B)\,.$$

(c) Let $A_1, A_2, \cdots$ be finite sets, and $S = \left\{ n \in \mathbb{N} \,\middle|\, \bigcup_{k=1}^{n} A_k \text{ is finite} \right\}$. Then $1 \in S$ by assumption. Suppose that $n \in S$. Then $n+1 \in S$ because of (b). **PMI** then implies that $S = \mathbb{N}$. □

Lemma 5.15. *Let $k \geqslant 2$ be a natural number. For $x \in \mathbb{N}_k$, $\mathbb{N}_k \backslash \{x\} \approx \mathbb{N}_{k-1}$.*

Theorem 5.16 (Pigeonhole Principle)**.** *Let $n, r \in \mathbb{N}$ and $f : \mathbb{N}_n \to \mathbb{N}_r$ be a function. If $n > r$, then f is not injective.*

Corollary 5.17. *If $\#A = n$, $\#B = r$ and $r < n$, then there is no one-to-one function from A to B.*

Corollary 5.18. *If A is finite, then A is not equivalent to any of its proper subsets.*

5.2 Infinite Sets

Recall that a set A is infinite if A is not finite. By Corollary 5.18, if a set is equivalent to one of its proper subset, then that set cannot be finite. Therefore, $\mathbb{N}$ is not finite since there is a one-to-one correspondence from $\mathbb{N}$ to the set of even numbers.

The set of natural numbers $\mathbb{N}$ is a set with infinite cardinality. The standard symbol for the cardinality of $\mathbb{N}$ is $\aleph$. There are two kinds of infinite sets, denumerable sets and uncountable sets. We start from the denumerable sets which is defined in the following

Definition 5.19. A set S is said to be ***denumerable*** if $S \approx \mathbb{N}$. For a denumerable set S, we say S has cardinal number $\aleph_0$ (or cardinality $\aleph_0$) and write $\#S = \aleph_0$.

Example 5.20. The set of even numbers and the set of odd numbers are denumerable.

Example 5.21. The set $\{p, q, r\} \cup \{n \in \mathbb{N} \,|\, n \neq 5\}$ is denumerable.

Theorem 5.22. *The set $\mathbb{Z}$ is denumerable.*

Proof. Consider the function $f : \mathbb{N} \to \mathbb{Z}$ given by $f(x) = \begin{cases} \dfrac{x}{2} & \text{if } x \text{ is even}, \\ \dfrac{1-x}{2} & \text{if } x \text{ is odd}. \end{cases}$ □

Theorem 5.23. (a) *The set $\mathbb{N} \times \mathbb{N}$ is denumerable.*

(b) *If A and B are denumerable sets, then $A \times B$ is denumerable.*

Proof. (a) Consider the function $F : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $F(m, n) = 2^{m-1}(2n-1)$. Then $F : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is bijective.

(b) If A and B are denumerable sets, then $A \approx \mathbb{N}$ and $B \approx \mathbb{N}$. By (b) of Lemma 5.6, we find that $A \times B \approx \mathbb{N} \times \mathbb{N}$; thus $A \times B \approx \mathbb{N}$ since $\approx$ is an equivalence relation. □

Uncountable sets are understood when the concept of countability is known.

Definition 5.24. A set S is said to be ***countable*** if S is finite or denumerable. We say S is ***uncountable*** if S is not countable.

Theorem 5.25. *The open interval* $(0,1)$ *is uncountable.*

Proof. Assume the contrary that there exists $f : \mathbb{N} \to (0,1)$ which is one-to-one and onto. Write $f(k)$ in decimal expansion (十進位展開); that is,

$$\begin{aligned} f(1) &= 0.d_{11}d_{21}d_{31}\cdots \\ f(2) &= 0.d_{12}d_{22}d_{32}\cdots \\ \vdots &\qquad\quad \vdots \\ f(k) &= 0.d_{1k}d_{2k}d_{3k}\cdots \\ \vdots &\qquad\quad \vdots \end{aligned}$$

Here we note that repeated 9's are chosen by preference over terminating decimals; that is, for example, we write $\frac{1}{4} = 0.249999\cdots$ instead of $\frac{1}{4} = 0.250000\cdots$.

Let $x \in (0,1)$ be such that $x = 0.d_1d_2\cdots$, where

$$d_k = \begin{cases} 5 & \text{if } \ d_{kk} \neq 5\,, \\ 3 & \text{if } \ d_{kk} = 5\,. \end{cases}$$

(建構一個 x 使其小數點下第 k 位數與 $f(k)$ 的小數點下第 k 位數不相等). Then $x \neq f(k)$ for all $k \in \mathbb{N}$, a contradiction; thus $(0,1)$ is uncountable. ▫

Definition 5.26. A set S has cardinal number $\mathbf{c}$ (or cardinality $\mathbf{c}$) if S is equivalent to $(0,1)$. We write $\#S = \mathbf{c}$, which stands for ***continuum***.

Theorem 5.27. (a) *Even open interval* (a,b) *is uncountable and has cardinality* $\mathbf{c}$.

(b) *The set* $\mathbb{R}$ *of all real numbers is uncountable and has cardinality* $\mathbf{c}$.

Proof. (a) The function $f(x) = a + (b-a)x$ maps from $(0,1)$ to (a,b) and is a one-to-one correspondence.

(b) Using (a), $(0,1) \approx \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$. Moreover, the function $f(x) = \tan x$ maps from $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ to $\mathbb{R}$ and is a one-to-one correspondence; thus $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \approx \mathbb{R}$. Since $\approx$ is an equivalence relation, $(0,1) \approx \mathbb{R}$. ▫

Example 5.28. The circle with the north pole removed is equivalent to the real line.

Example 5.29. The set $A = (0,2) \cup [5,6)$ has cardinality $\mathbf{c}$ since the function $f : (0,1) \to A$ given by

$$f(x) = \begin{cases} 4x & \text{if } 0 < x < \frac{1}{2}\,, \\ 2x + 4 & \text{if } \frac{1}{2} \leqslant x < 1 \end{cases}$$

is a one-to-one correspondence from $(0,1)$ to A.

5.3 Countable Sets

In this section we focus on the countability of sets.

Proposition 5.30. *Let S be a non-empty set. The following three statements are equivalent:*

(a) *S is countable;*

(b) *there exists a surjection $f : \mathbb{N} \to S$;*

(c) *there exists an injection $f : S \to \mathbb{N}$.*

Proof. "(a) $\Rightarrow$ (b)" First suppose that $S = \{x_1, \cdots, x_n\}$ is finite. Define $f : \mathbb{N} \to S$ by

$$f(k) = \begin{cases} x_k & \text{if } k < n\,, \\ x_n & \text{if } k \geqslant n\,. \end{cases}$$

Then $f : \mathbb{N} \to S$ is a surjection. Now suppose that S is denumerable. Then by definition of countability, there exists $f : \mathbb{N} \xrightarrow[onto]{1-1} S$.

"(a) $\Leftarrow$ (b)" W.L.O.G. we assume that S is an infinite set. Let $k_1 = 1$. Since $\#(S) = \infty$, $S_1 \equiv S \backslash \{f(k_1)\} \neq \varnothing$; thus $N_1 \equiv f^{-1}(S_1)$ is a non-empty subset of $\mathbb{N}$. By the well-ordered principle (**WOP**) of $\mathbb{N}$, N_1 has a smallest element denoted by k_2. Since $\#(S) = \infty$, $S_2 = S \backslash \{f(k_1), f(k_2)\} \neq \varnothing$; thus $N_2 \equiv f^{-1}(S_2)$ is a non-empty subset of $\mathbb{N}$ and possesses a smallest element denoted by k_3. We continue this process and obtain a set $\{k_1, k_2, \cdots\} \subseteq \mathbb{N}$, where $k_1 < k_2 < \cdots$, and k_j is the smallest element of $N_{j-1} \equiv f^{-1}(S \backslash \{f(k_1), f(k_2), \cdots, f(k_{j-1})\})$.

Claim: $f : \{k_1, k_2, \cdots\} \to S$ is one-to-one and onto.

Proof of claim: The injectivity of f is easy to see since $f(k_j) \notin \big\{f(k_1), f(k_2), \cdots, f(k_{j-1})\big\}$ for all $j \geqslant 2$. For surjectivity, assume that there is $s \in S$ such that $s \notin f(\{k_1, k_2, \cdots\})$. Since $f : \mathbb{N} \to \mathbb{S}$ is onto, $f^{-1}(\{s\})$ is a non-empty subset of $\mathbb{N}$; thus possesses a smallest element k. Since $s \notin f(\{k_1, k_2, \cdots\})$, there exists $\ell \in \mathbb{N}$ such that $k_\ell < k < k_{\ell+1}$. As a consequence, we find $k \in N_\ell$ such that $k < k_{\ell+1}$ which contradicts to the fact that $k_{\ell+1}$ is the smallest element of N_ℓ.

Define $g : \mathbb{N} \to \{k_1, k_2, \cdots\}$ by $g(j) = k_j$. Then $g : \mathbb{N} \to \{k_1, k_2, \cdots\}$ is one-to-one and onto; thus $h = g \circ f : \mathbb{N} \xrightarrow[onto]{1-1} S$.

"(a) $\Rightarrow$ (c)" If $S = \{x_1, \cdots, x_n\}$ is finite, we simply let $f : S \to \mathbb{N}$ be $f(x_n) = n$. Then f is clearly an injection. If S is denumerable, by definition there exists $g : \mathbb{N} \xrightarrow[onto]{1-1} S$ which implies that $f = g^{-1} : S \to \mathbb{N}$ is an injection.

"(a) $\Leftarrow$ (c)" Let $f : S \to \mathbb{N}$ be an injection. If f is also surjective, then $f : S \xrightarrow[onto]{1-1} \mathbb{N}$ which implies that S is denumerable. Now suppose that $f(S) \subsetneq \mathbb{N}$. Since S is non-empty, there exists $s \in S$. Let $g : \mathbb{N} \to S$ be defined by

$$g(n) = \begin{cases} f^{-1}(n) & \text{if } n \in f(S)\,, \\ s & \text{if } n \notin f(S)\,. \end{cases}$$

Then clearly $g : \mathbb{N} \to S$ is surjective; thus the equivalence between (a) and (b) implies that S is countable. ▫

Example 5.31. We have seen that the set $\mathbb{N}\times\mathbb{N}$ is countable. Now consider the map $f:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ defined by $f((m,n))=2^m3^n$. This map is not a bijection; however, it is an injection; thus Proposition 5.30 implies that $\mathbb{N}\times\mathbb{N}$ is countable.

Example 5.32. The set $\mathbb{Q}^+$ of positive rational numbers is denumerable. Since $\mathbb{Q}^+$ is infinite, it suffice to check the countability of $\mathbb{Q}^+$. Consider the map $f:\mathbb{N}^2\to\mathbb{Q}^+$ defined by $f(m,n)=\dfrac{m}{n}$. Then f is onto $\mathbb{Q}^+$; thus Proposition 5.30 implies that $\mathbb{Q}^+$ is countable.

Theorem 5.33. *Any non-empty subset of a countable set is countable.*

Proof. Let S be a countable set, and A be a non-empty subset of S. Since S is countable, by Proposition 5.30 there exists a surjection $f:\mathbb{N}\to S$. On the other hand, since A is a non-empty subset of S, there exists $a\in A$. Define

$$g(x)=\begin{cases} x & \text{if } x\in A\,,\\ a & \text{if } x\notin A\,.\end{cases}$$

Then $h=g\circ f:\mathbb{N}\to A$ is a surjection, and Proposition 5.30 shows that A is countable. □

Corollary 5.34. *A set A is countable if and only if A is equivalent to some subset of $\mathbb{N}$.*

Theorem 5.35. *The union of denumerable denumerable sets is denumerable*（無窮可數個無窮可數集的聯集是無窮可數的）*. In other words, if $\mathscr{F}$ is a denumerable collection of denumerable sets, then $\bigcup_{A\in\mathscr{F}} A$ is denumerable.*

Proof. Let $\mathscr{F}=\{A_i \mid i\in\mathbb{N}, A_i \text{ is denumerable}\}$ be an indexed family of denumerable sets, and define $A=\bigcup_{i=1}^{\infty}A_i$. Since A_i is denumerable, $A_i=\{x_{i1},x_{i2},x_{i3},\cdots\}$. Then $A=\{x_{ij}\mid i,j\in\mathbb{N}\}$. Let $f:\mathbb{N}\times\mathbb{N}\to A$ be defined by $f((i,j))=x_{ij}$. Then $f:\mathbb{N}\times\mathbb{N}\to A$ is a surjection. Moreover, Theorem 5.23 implies that there exists a bijection $g:\mathbb{N}\to\mathbb{N}\times\mathbb{N}$; thus $h=f\circ g:\mathbb{N}\to A$ is a surjection which, by Proposition 5.30, implies that A is countable. Since $A_1\subseteq A$, A is infinite; thus A is denumerable. □

Corollary 5.36. *The union of countable countable sets is countable*（可數個可數集的聯集是可數的）.

Proof. By adding empty sets into the family or adding $\mathbb{N}$ into a finite set if necessary, we find that the union of countable countable sets is a subset of the union of denumerable denumerable sets. By Theorem 5.33, we find that the union of countable countable sets is countable. □

Corollary 5.37. $\mathbb{Q}$ *is countable.*

Proof. Let $\mathbb{Q}^+$ and $\mathbb{Q}^-$ denote the collection of positive and negative rational numbers, respectively. By Example 5.32, the set $\mathbb{Q}^+$ is countable. Since $\mathbb{Q}^+\approx\mathbb{Q}^-$ (between them there exists a one-to-one correspondence $f(x)=-x$), $\mathbb{Q}^-$ is also countable. Therefore, Theorem 5.35 implies that $\mathbb{Q}=\mathbb{Q}^+\cup\mathbb{Q}^-\cup\{0\}$ is countable. □

Corollary 5.38. (a) *If $\mathscr{F}$ is a finite pairwise disjoint family of denumerable sets, then $\bigcup_{A\in\mathscr{F}} A$ is countable.*

(b) *If A and B are countable sets, then $A \cup B$ is countable.*

(c) *If $\mathscr{F}$ is a finite collection of countable sets, then $\bigcup_{A\in\mathscr{F}} A$ is countable.*

(d) *If $\mathscr{F}$ is a denumerable family of countable sets, then $\bigcup_{A\in\mathscr{F}} A$ is countable.*

7 Concepts of Analysis

7.1 Convergent Sequences

Recall that a sequence is a function with domain $\mathbb{N}$. For $n \in \mathbb{N}$, the image of n is called the n-th term of the sequence and is written as x_n. In the following discussion, sequences always take value in $\mathbb{R}$. In other words, we only consider real sequences.

Definition 7.1. Let $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{R}$ be a sequence. $\{x_n\}_{n=1}^{\infty}$ is said to be ***convergent*** if there exists $L \in \mathbb{R}$ such that for every $\varepsilon > 0$,

$$\#\big\{n \in \mathbb{N} \,\big|\, x_n \notin (L-\varepsilon, L+\varepsilon)\big\} < \infty\,.$$

Such an L is called a ***limit*** of the sequence. In notation,

$$\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{R} \text{ is convergent} \quad \Leftrightarrow \quad (\exists\, L \in \mathbb{R})(\forall\, \varepsilon > 0)\big(\#\{n \in \mathbb{N} \,|\, x_n \notin (L-\varepsilon, L+\varepsilon)\} < \infty\big).$$

If L is a limit of $\{x_n\}_{n=1}^{\infty}$, we say $\{x_n\}_{n=1}^{\infty}$ converges to L and write $x_n \to L$ as $n \to \infty$. If $\{x_n\}_{n=1}^{\infty}$ is not convergent, we say that $\{x_n\}_{n=1}^{\infty}$ diverges or is divergent.

Example 7.2. Let $x_n = \dfrac{(-1)^n}{n+1}$. We show that $\{x_n\}_{n=1}^{\infty}$ converges to 0. By definition, we need to show for every $\varepsilon > 0$ the set $A_\varepsilon = \big\{n \in \mathbb{N} \,\big|\, x_n \notin (-\varepsilon, \varepsilon)\big\}$ is finite. Note that $A_\varepsilon = \big\{n \in \mathbb{N} \,\big|\, |x_n| \geqslant \varepsilon\big\}$; thus

$$A_\varepsilon = \big\{n \in \mathbb{N} \,\big|\, \frac{1}{n+1} \geqslant \varepsilon\big\} = \big\{n \in \mathbb{N} \,\big|\, n \leqslant \frac{1}{\varepsilon} - 1\big\}\,.$$

Therefore, $\#A_\epsilon = \big[\frac{1}{\varepsilon}\big] - 1 < \infty$ which implies that $\{x_n\}_{n=1}^{\infty}$ converges to 0.

Example 7.3. The sequence $\{y_n\}_{n=1}^{\infty}$ given by $y_n = \dfrac{3 + (-1)^n}{2}$ diverges. To see this, we have to show that any real number L cannot be the limit of $\{y_n\}_{n=1}^{\infty}$.

Let $L \in \mathbb{R}$ be given and $\varepsilon = \dfrac{1}{2}$. Then $(L-\varepsilon, L+\varepsilon)$ at most contains one integer. Since y_n only takes value 1 or 2 and $\#\big\{n \in \mathbb{N} \,\big|\, y_n = 1\big\} = \#\big\{n \in \mathbb{N} \,\big|\, y_n = 2\big\} = \infty$, we find that

$$\#\big\{n \in \mathbb{N} \,\big|\, y_n \notin (L-\varepsilon, L+\varepsilon)\big\} = \infty$$

which implies $\{y_n\}_{n=1}^{\infty}$ cannot converges to L.

Example 7.4. Recall that a permutation of a non-empty set A is a one-to-one correspondence from A onto A. Let $\pi : \mathbb{N} \to \mathbb{N}$ be a permutation of $\mathbb{N}$, and $\{x_n\}_{n=1}^{\infty}$ be a convergent sequence. Then $\big\{x_{\pi(n)}\big\}_{n=1}^{\infty}$ is also convergent since if L is the limit of $\{x_n\}_{n=1}^{\infty}$ and $\varepsilon > 0$,

$$\#\big\{n \in \mathbb{N} \,\big|\, x_{\pi(n)} \notin (x-\varepsilon, x+\varepsilon)\big\} = \#\big\{n \in \mathbb{N} \,\big|\, x_n \notin (x-\varepsilon, x+\varepsilon)\big\} < \infty\,.$$

Proposition 7.5. *Let $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{R}$ be a sequence and L be a real number. Then $\{x_n\}_{n=1}^{\infty}$ converges to L if and only if for every $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $|x_n - L| < \varepsilon$ whenever $n \geqslant N$. In notation,*

$$\{x_n\}_{n=1}^{\infty} \text{ converges to } L \quad \Leftrightarrow \quad (\forall\, \varepsilon > 0)(\exists\, N \in \mathbb{N})(n \geqslant N \Rightarrow |x_n - L| < \varepsilon)\,.$$

Proof. "$\Rightarrow$" Let $\varepsilon > 0$ be given, and $A_\epsilon = \big\{n \in \mathbb{N} \,\big|\, x_n \notin (L-\varepsilon, L+\varepsilon)\big\}$. Since $\{x_n\}_{n=1}^{\infty}$ converges to L, $k \equiv \#A_\epsilon < \infty$. Suppose that $n_1 < n_2 < \cdots < n_k$ belongs to A_ϵ. Let $N = n_k + 1$. Then $N \in \mathbb{N}$ and if $n \geqslant N$, $n \notin A_\epsilon$ which implies that if $n \geqslant N$, $x_n \in (L-\varepsilon, L+\varepsilon)$ or equivalently,

$$|x_n - L| < \varepsilon \quad \text{whenever} \quad n \geqslant N\,.$$

"$\Leftarrow$" Let $\varepsilon > 0$ be given. Then for some $N \in \mathbb{N}$, if $n \geqslant N$, we have $|x_n - L| < \varepsilon$ or equivalently, if $n \geqslant N$, $x_n \in (L-\varepsilon, L+\varepsilon)$. This implies that

$$\#\big\{n \in \mathbb{N} \,\big|\, x_n \notin (L-\varepsilon, L+\varepsilon)\big\} < N < \infty\,. \qquad \square$$

Remark 7.6. A sequence $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{R}$ diverges if (and only if)

$$(\forall\, L \in \mathbb{R})(\exists\, \varepsilon > 0)\big(\#\{n \in \mathbb{N} \,|\, x_n \notin (L-\varepsilon, L+\varepsilon)\} = \infty\big)$$

which is equivalent to that

$$(\forall\, L \in \mathbb{R})(\exists\, \varepsilon > 0)(\forall\, N \in \mathbb{N})(\exists\, n \geqslant N)(|x_n - L| \geqslant \varepsilon)\,.$$

Example 7.7. Now we use the ε-N argument as the definition of the convergence of sequences to re-establish the convergence of sequences in Example 7.2, 7.3 and 7.4.

Example 7.2 - revisit: Let $\varepsilon > 0$ be given, and $x_n = \dfrac{(-1)^n}{n+1}$. Let $N = \big[\frac{1}{\varepsilon}\big] + 1$. Since $\big[\frac{1}{\varepsilon}\big] > \dfrac{1}{\varepsilon} - 1$, if $n \geqslant N$ we must have $n > \dfrac{1}{\varepsilon} - 1$; thus if $n \geqslant N$, $\dfrac{1}{n+1} < \varepsilon$. Therefore,

$$|x_n - 0| < \varepsilon \quad \text{whenever} \quad n \geqslant N$$

which implies that $\{x_n\}_{n=1}^{\infty}$ converges to 0.

Example 7.3 - revisit: Let $L \in \mathbb{R}$ be given. Choose $\varepsilon = \dfrac{1}{2}$. For $N \in \mathbb{N}$, define

$$n = \begin{cases} N+1 & \text{if } |y_N - L| < \varepsilon\,, \\ N+2 & \text{if } |y_N - L| \geqslant \varepsilon\,. \end{cases}$$

Then $n \geqslant N$. Moreover, if $|y_N - L| < \varepsilon$, then $|y_n - L| \geqslant |y_n - y_N| - |y_N - L| > 1 - \varepsilon = \varepsilon$, while if $|y_N - L| \geqslant \varepsilon$ then clearly $|y_n - L| \geqslant \varepsilon$. Therefore,

$$(\forall\, L \in \mathbb{R})(\exists\, \varepsilon > 0)(\forall\, N \in \mathbb{N})(\exists\, n \geqslant N)(|y_n - L| \geqslant \varepsilon)\,.$$

Example 7.4 - revisit: Now suppose that $\{x_n\}_{n=1}^{\infty}$ is a convergent sequence with limit L, and $\varepsilon > 0$ be given. Then by the convergence of $\{x_n\}_{n=1}^{\infty}$ to L, there exists $N_1 \in \mathbb{N}$ such that if $n \geqslant N_1$, we have $|x_n - L| < \varepsilon$. Define $N = \max\big\{\pi^{-1}(1), \pi^{-1}(2), \cdots, \pi^{-1}(N_1)\big\}$. Then if $n \geqslant N$, $\pi(n) \geqslant N_1$ which implies that

$$\big|x_{\pi(n)} - L\big| < \varepsilon \quad \text{whenever} \quad n \geqslant N\,.$$

Therefore, $\{x_{\pi(n)}\}_{n=1}^{\infty}$ converges to L.

From the example above, we notice that proving the convergence using the ε-N argument seems more complicated; however, it is an necessary evil so we encourage the readers to major it.

Theorem 7.8. *If $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{R}$ is a sequence such that $x_n \to x$ and $x_n \to y$ as $n \to \infty$, then $x = y$. (The uniqueness of the limit).*

Proof. Assume the contrary that $x \neq y$. W.L.O.G. we may assume that $x < y$, and let $\varepsilon = \dfrac{y-x}{2} > 0$. Then

$$\#\big\{n \in \mathbb{N} \,\big|\, x_n \notin (x-\varepsilon, x+\varepsilon)\big\} < \infty \tag{7.1}$$

and

$$\#\big\{n \in \mathbb{N} \,\big|\, x_n \notin (y-\varepsilon, y+\varepsilon)\big\} < \infty\,.$$

Note that the latter implies that $\#\big\{n \in \mathbb{N} \,\big|\, x_n \in (y-\varepsilon, y+\varepsilon)\big\} = \infty$ which contradicts to (7.1) since

$$(x-\varepsilon, x+\varepsilon) \cap (y-\varepsilon, y+\varepsilon) = \varnothing\,.$$ ▫

Alternative proof using ε-N definition. Assume the contrary that $x \neq y$. W.L.O.G. we may assume that $x < y$, and let $\varepsilon = \dfrac{y-x}{2} > 0$ $(x + \varepsilon = y - \varepsilon)$. Since $x_n \to x$ and $x_n \to y$ as $n \to \infty$,

$$(\exists\, N_1 \in \mathbb{N})(n \geqslant N_1 \Rightarrow |x_n - x| < \varepsilon)$$

and

$$(\exists\, N_2 \in \mathbb{N})(n \geqslant N_2 \Rightarrow |x_n - y| < \varepsilon)\,.$$

Then if $n \geqslant N \equiv \max\{N_1, N_2\}$, we have both $|x_n - x| < \varepsilon$ and $|x_n - y| < \varepsilon$ for all $n \geqslant N$. As a consequence, $x_n < x + \varepsilon$ and $x_n > y - \varepsilon$ for all $n \geqslant N$, a contradiction. So $x = y$. ▫

Notation: Since the limit of a convergent sequence $\{x_n\}_{n=1}^{\infty}$ is unique, we use $\lim\limits_{n\to\infty} x_n$ to denote the limit of $\{x_n\}_{n=1}^{\infty}$ when $\{x_n\}_{n=1}^{\infty}$ is convergent.

Example 7.9. Prove that the sequence $\{x_n\}_{n=1}^{\infty}$ given by $x_n = \dfrac{3n^2}{n^2+1}$ converges.

Theorem 7.10. *Suppose that $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ and $\{c_n\}_{n=1}^{\infty}$ are sequences of real numbers such that $a_n \leqslant b_n \leqslant c_n$ for all $n \in \mathbb{N}$. If $\lim\limits_{n\to\infty} a_n = \lim\limits_{n\to\infty} c_n = L$, then $\lim\limits_{n\to\infty} b_n = L$.*

Proof. Let $\varepsilon > 0$ be given. Since $\lim\limits_{n\to\infty} a_n = L$ and $\lim\limits_{n\to\infty} b_n = L$, by definition

$$(\exists\, N_1 \in \mathbb{N})(n \geqslant N_1 \Rightarrow |x_n - x\,| < \varepsilon)\,,$$

and

$$(\exists\, N_2 \in \mathbb{N})(n \geqslant N_2 \Rightarrow |x_n - y\,| < \varepsilon)\,.$$

Let $N = \max\{N_1, N_2\}$. Then $N \in \mathbb{N}$ and if $n \geqslant N$, $L - \varepsilon < a_n \leqslant c_n \leqslant b_n < L + \varepsilon$; thus $\lim\limits_{n\to\infty} c_n = L$. ▫

Example 7.11. Let $\{x_n\}_{n=1}^{\infty}$ be a sequence given by $x_n = \dfrac{\sin n}{n}$. Then $\lim\limits_{n\to\infty} \dfrac{\sin n}{n} = 0$.

Definition 7.12. Let $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{R}$ be a sequence.

1. $\{x_n\}_{n=1}^{\infty}$ is said to be ***bounded*** (有界的) if there exists $M > 0$ such that $|x_n| \leqslant M$ for all $n \in \mathbb{N}$.

2. $\{x_n\}_{n=1}^{\infty}$ is said to be ***bounded from above*** (有上界) if there exists $M \in \mathbb{R}$, called an ***upper bound*** of the sequence, such that $x_n \leqslant M$ for all $n \in \mathbb{N}$.

3. $\{x_n\}_{n=1}^{\infty}$ is said to be ***bounded from below*** (有下界) if there exists $m \in \mathbb{R}$, called a ***lower bound*** of the sequence, such that $m \leqslant x_n$ for all $n \in \mathbb{N}$.

Proposition 7.13. *A convergent sequence is bounded* (數列收斂必有界).

Proof. Let $\{x_n\}_{n=1}^{\infty}$ be a convergent sequence with limit x. Then there exists $N > 0$ such that

$$x_n \in (x-1, x+1) \qquad \forall\, n \geqslant N.$$

Let $M = \max\big\{|x_1|, |x_2|, \cdots, |x_{N-1}|, |x|+1\big\}$. Then $|x_n| \leqslant M$ for all $n \in \mathbb{N}$. ▫

Theorem 7.14. *Suppose that $x_n \to x$ and $y_n \to y$ as $n \to \infty$, λ is a constant. Then*

1. *$x_n \pm y_n \to x \pm y$ as $n \to \infty$.*

2. *$x_n \cdot y_n \to x \cdot y$ as $n \to \infty$.*

3. *If $y_n, y \neq 0$, then $\dfrac{x_n}{y_n} \to \dfrac{x}{y}$ as $n \to \infty$.*

Proof. 1. Let $\varepsilon > 0$ be given. Since $x_n \to x$ and $y_n \to y$ as $n \to \infty$, there exist $N_1, N_2 \in \mathbb{N}$ such that $|x_n - x| < \dfrac{\varepsilon}{2}$ for all $n \geqslant N_1$ and $|y_n - x| < \dfrac{\varepsilon}{2}$ whenever $n \geqslant N_2$. Define $N = \max\{N_1, N_2\}$. Then $N \in \mathbb{N}$ and if $n \geqslant N$,

$$|(x_n \pm y_n) - (x \pm y)| \leqslant |x_n - x\,| + |y_n - y\,| < \varepsilon\,;$$

thus $x_n \pm y_n \to x \pm y$ as $n \to \infty$.

2. Since $x_n \to x$ and $y_n \to y$ as $n \to \infty$, by Proposition 7.13 there exists $M > 0$ such that $|x_n| \leqslant M$ and $|y_n| \leqslant M$. Let $\varepsilon > 0$ be given. Then

$$(\exists\, N_1 \in \mathbb{N})\big(n \geqslant N_1 \Rightarrow |x_n - x\,| < \tfrac{\varepsilon}{2M}\big)\,,$$

and

$$(\exists\, N_2 \in \mathbb{N})\big(n \geqslant N_2 \Rightarrow |y_n - y\,| < \tfrac{\varepsilon}{2M}\big)\,.$$

Define $N = \max\{N_1, N_2\}$. Then $N \in \mathbb{N}$, and if $n \geqslant N$,

$$\begin{aligned} |x_n \cdot y_n - x \cdot y| &= |x_n \cdot y_n - x_n \cdot y + x_n \cdot y - x \cdot y| \leqslant |x_n \cdot (y_n - y)| + |y \cdot (x_n - x)| \\ &\leqslant M \cdot |y_n - y| + M \cdot |x_n - x| < M \cdot \frac{\varepsilon}{2M} + M \cdot \frac{\varepsilon}{2M} = \varepsilon. \end{aligned}$$

3. It suffices to show that $\lim_{n\to\infty}\frac{1}{y_n}=\frac{1}{y}$ if $y_n, y\neq 0$ (because of 2). Since $\lim_{n\to\infty} y_n = y$, there exists $N_1\in\mathbb{N}$ such that $|y_n-y|<\frac{|y|}{2}$ whenever $n\geqslant N_1$. Therefore, $|y|-|y_n|<\frac{|y|}{2}$ for all $n\geqslant N_1$ which further implies that $|y_n|>\frac{|y|}{2}$ for all $n\geqslant N_1$.

   Let $\varepsilon>0$ be given. Since $\lim_{n\to\infty} y_n = y$, there exists $N_2\in\mathbb{N}$ such that $|y_n-y|<\frac{|y|^2}{2}\varepsilon$ whenever $n\geqslant N_2$. Define $N=\max\{N_1,N_2\}$. Then $N\in\mathbb{N}$ and if $n\geqslant N$,

$$\left|\frac{1}{y_n}-\frac{1}{y}\right|=\frac{|y_n-y|}{|y_n||y|}<\frac{|y|^2}{2}\varepsilon\cdot\frac{1}{|y|}\frac{2}{|y|}=\varepsilon\,.$$ □

Definition 7.15. A sequence $\{y_j\}_{j=1}^{\infty}$ is called a ***subsequence*** of a sequence $\{x_n\}_{n=1}^{\infty}$ if there exists a strictly increasing function $f:\mathbb{N}\to\mathbb{N}$ such that $y_j=x_{f(j)}$. In this case, we often write $f(j)=n_j$ and $y_j=x_{n_j}$.

In other words, a subsequence of a sequence is derived by deleting some elements without changing the order of remaining elements.

Example 7.16. Let $\{x_n\}_{n=1}^{\infty}\subseteq\mathbb{R}$ be a sequence. Then $\{x_{2n}\}_{n=1}^{\infty}$ and $\{x_{2n-1}\}_{n=1}^{\infty}$ are subsequences of $\{x_n\}_{n=1}^{\infty}$. Moreover, $\{x_{2n}\}_{n=1}^{\infty}$ is obtained by deleting all the odd terms of $\{x_n\}_{n=1}^{\infty}$ (without changing the order), and $\{x_{2n-1}\}_{n=1}^{\infty}$ is obtained by deleting all the even terms of $\{x_n\}_{n=1}^{\infty}$ (without changing the order).

Theorem 7.17. *A sequence $\{x_n\}_{n=1}^{\infty}\subseteq\mathbb{R}$ converges if and only if every subsequence of $\{x_n\}_{n=1}^{\infty}$ converges (to the same limit).*

Proof. Since $\{x_n\}_{n=1}^{\infty}$ isself is a subsequence of $\{x_n\}_{n=1}^{\infty}$, it suffices to show the implication from LHS to RHS.

Suppose that $\lim_{n\to\infty} x_n = L$. We claim that every subsequence $\{x_{n_j}\}_{j=1}^{\infty}$ of $\{x_n\}_{n=1}^{\infty}$ also converges to L. Let $\varepsilon>0$ be given. Since $\lim_{n\to\infty} x_n = L$, there exists $N\in\mathbb{N}$ such that $|x_n-L|<\varepsilon$ whenever $n\geqslant N$. Note that if $j\geqslant N$, we must have $n_j\geqslant N$; thus if $j\geqslant N$, we must have $\left|x_{n_j}-L\right|<\varepsilon$. □

7.2 Limits and Continuity of Real-Valued Functions

Definition 7.18. Let $I\subseteq\mathbb{R}$ be an interval, $a\in I$, and f be a real-valued function defined on $I-\{a\}$. We say that ***the limit of f at a*** exists if for every sequence $\{a_n\}_{n=1}^{\infty}\subseteq I$ satisfying

1. $a_n\neq a$ for all $n\in\mathbb{N}$, 2. $\lim_{n\to\infty} a_n = a$,

the sequence $\{b_n\}_{n=1}^{\infty}$ given by $b_n=f(a_n)$ converges. （一函數在 a 的極限存在如果「所有在 I 中取值不是 a 但收斂到 a 的數列其函數值所形成的數列都收斂」） Using the logic notation, the limit of f at a exists if

$$\left(\forall\,\{a_n\}_{n=1}^{\infty}\subseteq I\backslash\{a\}\right)\left(\lim_{n\to\infty} a_n=a\Rightarrow\lim_{n\to\infty} f(a_n)\text{ exists}\right).$$

Proposition 7.19. *Let $I \subseteq \mathbb{R}$ be an interval, $a \in I$, and f be a real-valued function defined on $I\backslash\{a\}$. If the limit of f at a exists, then there exists a unique $L \in \mathbb{R}$ such that $\lim\limits_{n\to\infty} f(a_n) = L$ for every sequence $\{a_n\}_{n=1}^{\infty} \subseteq I\backslash\{a\}$ converging to a.*

Proof. Suppose that contrary that there exist two sequences $\{a_n\}_{n=1}^{\infty}, \{b_n\}_{n=1}^{\infty} \subseteq I\backslash\{a\}$ and two numbers L_1, L_2 such that $a_n \to a, b_n \to a$ as $n \to \infty$ and

$$\lim_{n\to\infty} f(a_n) = L_1 \quad \text{and} \quad \lim_{n\to\infty} f(b_n) = L_2\,.$$

Define a sequence $\{c_n\}_{n=1}^{\infty}$ by $c_n = \begin{cases} a_{\frac{n+1}{2}} & \text{if } n \text{ is odd}\,, \\ b_{\frac{n}{2}} & \text{if } n \text{ is even}\,; \end{cases}$ that is, $\{c_n\}_{n=1}^{\infty} = \{a_1, b_1, a_2, b_2, a_3, b_3, \cdots\}$. Then $c_n \to a$ as $n \to \infty$; thus by the definition of the limit of functions, there exists L such that

$$\lim_{n\to\infty} f(c_n) = L\,.$$

Since $\{f(a_n)\}_{n=1}^{\infty}$ and $\{f(b_n)\}_{n=1}^{\infty}$ are both subsequences of $\{f(c_n)\}_{n=1}^{\infty}$, Theorem 7.17 implies that $L = L_1 = L_2$, a contradiction. □

Notation: If the limit of f at a exists, by Proposition 7.19,

$$(\exists! L \in \mathbb{R})\big(\forall\, \{a_n\}_{n=1}^{\infty} \subseteq I\backslash\{a\}\big)\big(\lim_{n\to\infty} a_n = a \Rightarrow \lim_{n\to\infty} f(a_n) = L\big)\,.$$

This unique real number L is called the limit of f at a, and is denoted by $\lim\limits_{x\to a} f(x)$.

Example 7.20. Consider the function $f : [0,1] \to \mathbb{R}$ defined by $f(x) = \begin{cases} \sin\dfrac{1}{x} & \text{if } x \neq 0\,, \\ 0 & \text{if } x = 0\,. \end{cases}$ Then f is not continuous at 0 since letting $x_n = \dfrac{1}{2n\pi}$ and $y_n = \dfrac{1}{2n\pi + \pi/2}$, we have $x_n \to 0$ and $y_n \to 0$ as $n \to \infty$ but $f(x_n) = 0$ while $f(y_n) = 1$ for all $n \in \mathbb{N}$.

Theorem 7.21. *Suppose that $I \subseteq \mathbb{R}$ is an interval, $a \in I$, and f, g are two functions defined on I, except possibly at a, such that $f(x) = g(x)$ for all $x \in I\backslash\{a\}$. If $\lim\limits_{x\to a} f(x)$ exists, then $\lim\limits_{x\to a} g(x)$ exists, and $\lim\limits_{x\to a} f(x) = \lim\limits_{x\to a} g(x)$.*

Proof. Since $\lim\limits_{x\to a} f(x)$ exists, every sequence $\{x_n\}_{n=1}^{\infty} \subseteq I\backslash\{a\}$ converging to Let $\{x_n\}_{n=1}^{\infty} \subseteq I\backslash\{a\}$ be a sequence converging to a. Since $\lim\limits_{x\to a} f(x)$ exists, $\lim\limits_{n\to\infty} f(x_n) = L$ for some $L \in \mathbb{R}$. By the fact that $f(x) = g(x)$ for $x \in I\backslash\{a\}$, $\lim\limits_{n\to\infty} g(x_n) = L$. □

Proposition 7.22. *Let $I \subseteq \mathbb{R}$ be an interval, $a \in I$, and f be a real-valued function defined on $I\backslash\{a\}$. Then $\lim\limits_{x\to a} f(x) = L$ if and only if*

$$(\forall\, \varepsilon > 0)(\exists\, \delta > 0)\big[(0 < |x - a| < \delta) \wedge (x \in I) \Rightarrow |f(x) - L| < \varepsilon\big]\,.$$

Proof. "⇒" Assume the contrary that there exists $\varepsilon > 0$ such that for all $\delta > 0$, there exists $x_\delta \in I\backslash\{a\}$ with

$$0 < |x_\delta - a| < \delta \quad \text{and} \quad \big|f(x_\delta) - b\big| \geqslant \varepsilon\,.$$

In particular, letting $\delta = \dfrac{1}{n}$, we can find $\{x_n\}_{k=1}^{\infty} \subseteq I\backslash\{a\}$ such that

$$0 < |x_n - a| < \frac{1}{n} \quad \text{and} \quad \big|f(x_n) - L\big| \geqslant \varepsilon\,.$$

Then $x_n \to a$ as $n \to \infty$ but $f(x_n) \nrightarrow L$ as $n \to \infty$, a contradiction.

"$\Leftarrow$" Let $\{x_n\}_{k=1}^{\infty} \subseteq I\backslash\{a\}$ be such that $x_n \to a$ as $n \to \infty$, and $\varepsilon > 0$ be given. By assumption,

$$\exists\, \delta > 0 \ni \big|f(x) - L\big| < \varepsilon \text{ whenever } 0 < |x - a| < \delta \text{ and } x \in I\,.$$

Since $x_n \to a$ as $n \to \infty$, there exists $N > 0$ such that $|x_n - a| < \delta$ whenever $n \geqslant N$. Therefore,

$$\big|f(x_n) - L\big| < \varepsilon \quad \forall\, n \geqslant N$$

which shows that $\lim\limits_{n\to\infty} f(x_n) = L$. □

Definition 7.23. Let $I \subseteq \mathbb{R}$ be an interval, and $a \in I$. A function $f : I \to \mathbb{R}$ is said to be continuous at a if $\lim\limits_{x\to a} f(x) = f(a)$. In other words, $f : I \to \mathbb{R}$ is continuous at a if

$$(\forall\, \varepsilon > 0)(\exists\, \delta > 0)\big[(|x - a| < \delta) \wedge (x \in I) \Rightarrow \big|f(x) - f(a)\big| < \varepsilon\big]\,.$$

A function $f : I \to \mathbb{R}$ is said to be continuous on I if f is continuous at every point of I.

Remark 7.24. Almost identical proof of showing Proposition 7.22 implies that "f is continuous at a if and only if for every sequence $\{x_n\}_{n=1}^{\infty} \subseteq I$ converging to a, one has $\lim\limits_{n\to\infty} f(x_n) = f(a)$." (一函數 f 在 a 連續如果「所有在 I 中收斂到 a 的數列其函數值所形成的數列都收斂到 $f(a)$」)

Lemma 7.25. *Let $I, J \subseteq \mathbb{R}$ be intervals, and $f : I \to \mathbb{R}$, $g : J \to \mathbb{R}$ be functions. If $f(I) \subseteq J$, $\lim\limits_{x\to a} f(x) = b \in J$, and g is continuous at b, then $\lim\limits_{x\to a}(g \circ f)(x) = g(b)$.*

Proof. Let $\{x_n\}_{n=1}^{\infty} \subseteq I\backslash\{a\}$ such that $x_n \to a$ as $n \to \infty$. Since $\lim\limits_{x\to a} f(x) = b$, we have

$$\lim_{n\to\infty} f(x_n) = b\,.$$

In other words, $\big\{f(x_n)\big\}_{n=1}^{\infty}$ is a convergent sequence with limit b. By the continuity of g at b and Remark 7.24, $\lim\limits_{n\to\infty} g(f(x_n)) = g(b)$. Therefore, for every sequence $\{x_n\}_{n=1}^{\infty} \subseteq I\backslash\{a\}$ such that $x_n \to a$ as $n \to \infty$, one has $\lim\limits_{n\to\infty}(g \circ f)(x_n) = g(b)$. This implies that $\lim\limits_{x\to a}(g \circ f)(x) = g(b)$. □

Alternative proof. Let $\varepsilon > 0$ be given. Since g is continuous at b, there exists $\sigma > 0$ such that

$$\big|g(y) - g(b)\big| < \varepsilon \quad \text{whenever} \quad |y - b| < \sigma \text{ and } y \in J\,.$$

For such $\sigma > 0$, there exists $\delta > 0$ such that

$$\big|f(x) - b\big| < \sigma \quad \text{whenever} \quad 0 < |x - a| < \delta \text{ and } x \in I\,.$$

Therefore, if $0 < |x - a| < \delta$ and $x \in I$,

$$\big|(g \circ f)(x) - g(b)\big| = \big|g(f(x)) - g(b)\big| < \varepsilon$$

since we also have $|f(x) - b| < \sigma$ and $f(x) \in J$. □

Remark 7.26. Suppose that $\lim_{x\to a} f(x) = b$. It is possible that if $\lim_{x\to b} g(x) = c$ but $\lim_{x\to a}(g\circ f)(x) \neq c$. For example, let $f(x) = b$ be a constant function, and $g(x)$ be defined by

$$g(x) = \begin{cases} 0 & \text{if } x \neq b\,, \\ 1 & \text{if } x = b\,. \end{cases}$$

Then $(g\circ f)(x) = 1$, and $\lim_{x\to a}(g\circ f)(x) = 1 \neq 0 = \lim_{x\to b} g(x)$.

Theorem 7.27. *Let $I, J \subseteq \mathbb{R}$ be intervals, and $f : I \to \mathbb{R}$, $g : J \to \mathbb{R}$ be functions. If $f(I) \subseteq J$, f is continuous at $a \in I$, $f(a) \in J$ and g is continuous at $f(a)$, then $g \circ f$ is continuous at a.*

7.3 The Completeness Property

Definition 7.28. A set $\mathcal{F}$ is said to be a ***field*** (體) if there are two operations $+$ and $\cdot$ such that

1. $x + y \in \mathcal{F}$, $x \cdot y \in \mathcal{F}$ if $x, y \in \mathcal{F}$. (封閉性)
2. $x + y = y + x$ for all $x, y \in \mathcal{F}$. (commutativity, 加法的交換性)
3. $(x + y) + z = x + (y + z)$ for all $x, y, z \in \mathcal{F}$. (associativity, 加法的結合性)
4. There exists $0 \in \mathcal{F}$, called 加法單位元素, such that $x + 0 = x$ for all $x \in \mathcal{F}$. (the existence of zero)
5. For every $x \in \mathcal{F}$, there exists $y \in \mathcal{F}$ (usually y is denoted by $-x$ and is called x 的加法反元素) such that $x + y = 0$. One writes $x - y \equiv x + (-y)$.
6. $x \cdot y = y \cdot x$ for all $x, y \in \mathcal{F}$. (乘法的交換性)
7. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in \mathcal{F}$. (乘法的結合性)
8. There exists $1 \in \mathcal{F}$, called 乘法單位元素, such that $x \cdot 1 = x$ for all $x \in \mathcal{F}$. (the existence of unity)
9. For every $x \in \mathcal{F}$, $x \neq 0$, there exists $y \in \mathcal{F}$ (usually y is denoted by x^{-1} and is called x 的乘法反元素) such that $x \cdot y = 1$. One writes $x \cdot y \equiv x \cdot x^{-1} = 1$.
10. $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in \mathcal{F}$. (distributive law, 分配律)
11. $0 \neq 1$.

Definition 7.29. A ***partial order*** over a set P is a binary relation $\preccurlyeq$ which is reflexive, anti-symmetric and transitive, in the sense that

1. $x \preccurlyeq x$ for all $x \in P$ (reflexivity).
2. $x \preccurlyeq y$ and $y \preccurlyeq x \Rightarrow x = y$ (anti-symmetry).
3. $x \preccurlyeq y$ and $y \preccurlyeq z \Rightarrow x \preccurlyeq z$ (transitivity).

A set with a partial order is called a ***partially ordered set***.

Definition 7.30. Let $(P, \preccurlyeq)$ be a partially ordered set. Two elements $x, y \in P$ are said to be ***comparable*** if either $x \preccurlyeq y$ or $y \preccurlyeq x$.

Definition 7.31. A partial order under which every pair of elements is comparable is called a ***total order*** or ***linear order***.

Definition 7.32. An ***ordered field*** is a totally ordered field $(\mathcal{F}, +, \cdot, \preccurlyeq)$ satisfying that

1. If $x \preccurlyeq y$, then $x + z \preccurlyeq y + z$ for all $z \in \mathcal{F}$ (compatibility of $\preccurlyeq$ and $+$).
2. If $0 \preccurlyeq x$ and $0 \preccurlyeq y$, then $0 \preccurlyeq x \cdot y$ (compatibility of $\preccurlyeq$ and $\cdot$).

Example 7.33. $(\mathbb{Q}, +, \cdot, \leqslant)$ and $(\mathbb{R}, +, \cdot, \leqslant)$ are ordered fields.

Definition 7.34. Let $(\mathcal{F}, +, \cdot, \preccurlyeq)$ be an ordered field.

1. The relation $\succcurlyeq$ is defined by "$x \succcurlyeq y \Leftrightarrow y \preccurlyeq x$".
2. The relation $\prec$ is defined by "$x \prec y \Leftrightarrow x \preccurlyeq y \wedge x \neq y$".
3. The relation $\succ$ is defined by "$x \succ y \Leftrightarrow y \prec x$".

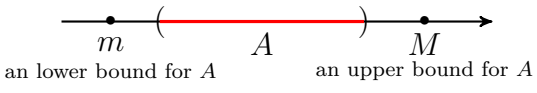
Theorem 7.35. *If $a < b$ in an ordered field $\mathcal{F}$, then there exists $c \in \mathcal{F}$ such that $a < c < b$.*

Definition 7.36. Let $(\mathcal{F}, +, \cdot, \preccurlyeq)$ be an ordered field, and $\varnothing \neq A \subseteq \mathcal{F}$. A number $M \in \mathcal{F}$ is called an ***upper bound*** (上界) for A if $x \preccurlyeq M$ for all $x \in A$, and a number $m \in \mathcal{F}$ is called a ***lower bound*** (下界) for A if $x \succcurlyeq m$ for all $x \in A$. If there is an upper bound for A, then A is said to be ***bounded from above***, while if there is a lower bound for A, then A is said to be ***bounded from below***. A number $b \in \mathcal{F}$ is called a ***least upper bound*** (最小上界) if

1. b is an upper bound for A, and
2. if M is an upper bound for A, then $M \succcurlyeq b$.

A number a is called a ***greatest lower bound*** (最大下界) if

1. a is a lower bound for A, and
2. if m is a lower bound for A, then $m \preccurlyeq a$.



If A is not bounded above, the least upper bound of A is set to be ∞, while if A is not bounded below, the greatest lower bound of A is set to be $-\infty$. The least upper bound of A is also called the ***supremum*** of A and is usually denoted by $\mathrm{lub}A$ or $\sup A$, and "the" greatest lower bound of A is also called the ***infimum*** of A, and is usually denoted by $\mathrm{glb}A$ or $\inf A$. If $A = \varnothing$, then $\sup A = -\infty$, $\inf A = \infty$.

Remark 7.37. Let $(\mathcal{F}, +, \cdot, \leqslant)$ be an ordered field.

1. If $b_1, b_2 \in \mathcal{F}$ are least upper bounds for a set $A \subseteq \mathcal{F}$, then $b_1 = b_2$. Therefore, $\sup A$ is a well-defined concept. Similarly, $\inf A$ is a well-defined concept.

2. Since the sentence "$x \in \varnothing \Rightarrow x \leqslant M$" is true for all $M \in \mathcal{F}$, we conclude that $\sup \varnothing = -\infty$. Similarly, $\inf \varnothing = \infty$.

Example 7.38. In the ordered field $\mathbb{R}$,

1. $\sup(0, 3) = 3$ and $\inf(0, 3) = 0$.

2. $\sup \mathbb{N}$ does not exist, but $\inf(\mathbb{N}) = 1$.

3. Let $A = \{2^{-k} \,|\, k \in \mathbb{N}\}$. Then $\inf A = 0$ and $\sup A = \dfrac{1}{2}$.

4. Let $B = \{x \in \mathbb{Q} \,|\, x^2 < 2\}$. Then $\inf B = -\sqrt{2}$ and $\sup B = \sqrt{2}$.

How about considering the supremum and infimum for the sets above in the ordered field $\mathbb{Q}$?

Theorem 7.39. *Let $(\mathcal{F}, +, \cdot, \leqslant)$ be an ordered field, and A be a subset of $\mathcal{F}$. Then $s = \sup A$ if and only if*

(i) $(\forall\, \varepsilon > 0)(\forall\, x \in A)(x < s + \varepsilon)$. (ii) $(\forall\, \varepsilon > 0)(\exists\, x \in A)(x > s - \varepsilon)$.

Proof. "$\Rightarrow$" (i) is part of the definition of being a least upper bound.

(ii) If M is an upper bound of A, then we must have $M \geqslant s$; thus $s - \varepsilon$ is not an upper bound of A. Therefore, $\exists\, x \in A \ni x > s - \varepsilon$.

"$\Leftarrow$" First, we show that s is an upper bound for A. If not, there exists $x \in A$ such that $s < x$. Let $\varepsilon = x - s > 0$. Then we do not have (i) since $x \in A$ but $x \nless s + \varepsilon$.

Next we show that if M is an upper bound of A, then $M \geqslant s$. Assume the contrary. Then $\exists\, M$ such that M is an upper bound of A but $M < s$. Let $\varepsilon = s - M$, then there is no $x \in S \ni x > s - \varepsilon$. $\rightarrow\leftarrow$ □

Definition 7.40 (Completeness)**.** Let $(\mathcal{F}, +, \cdot, \leqslant)$ be an ordered field. $\mathcal{F}$ is said to be ***complete*** (完備) if every non-empty subset of $\mathcal{F}$ that has an upper bound in $\mathcal{F}$ has a supremum that is an element of $\mathcal{F}$. (非空有上界的集合必有最小上界)

Theorem 7.41. *The field $(\mathbb{R}, +, \cdot, \leqslant)$ is a complete ordered field.*

Theorem 7.42 (Archimedean Principle for $\mathbb{R}$)**.** *For every real number x, there is a natural number n such that $n > x$.*

Proof. Let $x \in \mathbb{R}$. If $x < 1$, then the choice $n = 1$ validates $n > x$. Suppose $x \geqslant 1$. Define $A = \{n \in \mathbb{N} \,|\, n \leqslant x\}$. Then $1 \in A$ and x is an upper bound for A. By the completeness of $\mathbb{R}$, $s \equiv \sup A \in \mathbb{R}$ exists. Since s is the least upper bound for A, $s - 1$ is not an upper bound for A; thus there exists $m \in A$ such that $m > s - 1$ or $s < m + 1$. Then $m + 1 \notin A$ which implies that $m + 1 \nleqslant x$. The choice $n = m + 1$ satisfies $n > x$. □

Example 7.43. The set $B = \{x \in \mathbb{Q} \,|\, x^2 < 2\}$ is bounded above in the field $\mathbb{Q}$ but has no supremum in $\mathbb{Q}$. To see this, first we note that B is bounded above since 2 is an upper bound of B. Suppose that $s = \sup B \in \mathbb{Q}$ exists.

1. If $s < \sqrt{2}$, then $s - \sqrt{2} > 0$. The Archimedean property of $\mathbb{R}$ implies that there exists $K \in \mathbb{N}$ such that $K > \dfrac{1}{s - \sqrt{2}} > 0$. Then $\sqrt{2} < s - \dfrac{1}{K}$ which implies that $s - \dfrac{1}{K}$ is an upper bound of B. Therefore, s is not the least upper bound, a contradiction.

2. If $s > \sqrt{2}$, then $\sqrt{2} - s > 0$. The Archimedean property of $\mathbb{R}$ implies that there exists $M \in \mathbb{N}$ such that $M > \dfrac{1}{\sqrt{2} - s} > 0$. Then $s + \dfrac{1}{M} < \sqrt{2}$ which shows that $s + \dfrac{1}{M} \in B$. Therefore, s cannot be an upper bound of B since $s \nleqslant s + \dfrac{1}{M}$.

Therefore, $\sup B = \sqrt{2} \notin \mathbb{Q}$.

7.4 The Heine-Borel Theorem

Definition 7.44. Let a and δ be real numbers with $\delta > 0$. The ***δ-neighborhood*** of a is the set $\mathcal{N}(a, \delta) = \big\{x \in \mathbb{R} \,\big|\, |x - a| < \delta\big\}$.

Therefore, a sequence $\{x_n\}_{n=1}^{\infty}$ converges to a if for every $\varepsilon > 0$, there are only finite number of $n \in \mathbb{N}$ such that x_n lies outside the ε-neighborhood of a. We also note that if $0 < \delta_1 < \delta_2$, then $\mathcal{N}(a, \delta_1) \subseteq \mathcal{N}(a, \delta_2)$.

Definition 7.45. For a set $A \subseteq \mathbb{R}$, a point x is said to be an ***interior point*** of A if there exists $\delta > 0$ such that $\mathcal{N}(a, \delta) \subseteq A$.

Definition 7.46. A set $A \subseteq \mathbb{R}$ is said to be ***open*** if every point of A is an interior point of A. In other words, $A \subseteq \mathbb{R}$ is open if for every $x \in A$, there exists $\delta > 0$ such that $\mathcal{N}(a, \delta) \subseteq A$.

Example 7.47. The empty set $\varnothing$ and the universe $\mathbb{R}$ are open.

Theorem 7.48. *Every interval $(a, b) \subseteq \mathbb{R}$, where $-\infty \leqslant a < b \leqslant \infty$, is an open set.*

Proof. Let $x \in (a, b)$. W.L.O.G., we can assume that at least one a and b is finite. Define $\delta = \min\{x - a, b - x\}$. Then $0 < \delta < \infty$. Moreover, if $y \in \mathcal{N}(x, \delta)$, we must have $|y - x| < \delta$; thus if $y \in \mathcal{N}(x, \delta)$,

$$y - a = y - x + x - a > -\delta + x - a \geqslant 0 \quad \text{and} \quad b - y = b - x + x - y > b - x - \delta \geqslant 0$$

which implies that $\mathcal{N}(x, \delta) \subseteq (a, b)$. ▫

Theorem 7.49. *Let $\mathscr{F}$ be a non-empty collection of open subsets of $\mathbb{R}$. Then*

(a) $\bigcup\limits_{A \in \mathscr{F}} A$ *is an open set.*

(b) *If $\mathscr{F}$ has finitely many open sets, then $\bigcap\limits_{A \in \mathscr{F}} A$ is an open set.*

Proof. (a) Let $x \in \bigcup_{A\in\mathscr{F}} A$. Then $x \in A$ for some $A \in \mathscr{F}$. Since A is open, x is an interior point of A; thus there exists $\delta > 0$ such that $\mathcal{N}(x,\delta) \subseteq A$. Then $\mathcal{N}(x,\delta) \subseteq \bigcup_{A\in\mathscr{F}} A$ and we establish that $\bigcup_{A\in\mathscr{F}} A$ is open.

(b) Suppose that $\mathscr{F} = \{A_1, A_2, \cdots, A_k\}$ and A_j's are open for $1 \leqslant j \leqslant k$. Let $x \in \bigcap_{A\in\mathscr{F}} A$. Then $x \in A_j$ for all $1 \leqslant j \leqslant k$. Since each A_j is open, there exists $\delta_j > 0$ such that $\mathcal{N}(x,\delta_j) \subseteq A_j$. Define $\delta = \min\{\delta_1, \cdots, \delta_k\}$. Then $\delta > 0$ and $\mathcal{N}(x,\delta) \subseteq \mathcal{N}(x,\delta_j) \subseteq A_j$ for all $1 \leqslant j \leqslant k$. As a consequence, $\mathcal{N}(x,\delta) \subseteq \bigcap_{j=1}^{k} A_j = \bigcap_{A\in\mathscr{F}} A$. ▫

Definition 7.50. A set A is said to be ***closed*** if its complement $A^{\complement} = \mathbb{R}\backslash A$ is open.

Theorem 7.51. *A subset $A \subseteq \mathbb{R}$ is closed if and only if every convergent sequence $\{x_n\}_{n=1}^{\infty} \subseteq A$ converges to a limit in A.*

Proof. ($\Rightarrow$) Let $\{x_n\}_{n=1}^{\infty} \subseteq A$ be a convergent sequence with limit x. If $x \notin A$, then $x \in A^{\complement}$. By the closedness of A, there exists $\delta > 0$ such that $\mathcal{N}(x,\delta) \subseteq A^{\complement}$. Since $\{x_n\}_{n=1}^{\infty} \subseteq A$, $x_n \notin \mathcal{N}(x,\delta)$ which contradicts to the fact that $\{x_n\}_{n=1}^{\infty}$ converges to x. Therefore, $x \in A$.

($\Leftarrow$) Suppose the contrary that there exists $x \in A^{\complement}$ such that for all $\delta > 0$, $\mathcal{N}(x,\delta) \nsubseteq A^{\complement}$; thus for all $\delta > 0$, $\mathcal{N}(x,\delta) \cap A \neq \varnothing$. Therefore, there exists a sequence $\{x_n\}_{n=1}^{\infty}$ such that $x_n \in \mathcal{N}\big(x, \frac{1}{n}\big) \cap A$. Then $x_n \to x$ as $n \to \infty$ since

$$|x_n - x| < \frac{1}{n}\,;$$

thus by assumption, $x \in A$, a contradiction. ▫

Corollary 7.52. *Let $A \subseteq \mathbb{R}$ be closed and $x \in \mathbb{R}$. If $A \cap \mathcal{N}(x,\delta) \neq \varnothing$ for all $\delta > 0$, then $x \in A$.*

Theorem 7.53. *If $\varnothing \neq A \subseteq \mathbb{R}$ is closed and bounded, then* $\sup A \in A$ *and* $\inf A \in A$.

Proof. We only prove the case that $\sup A \in A$ since the proof of the counterpart is similar.

Let $x = \sup A$. Then $x \in \mathbb{R}$, and for all $n \in \mathbb{N}$, by Theorem 7.39 there exists $x_n \in A$ such that

$$x - \frac{1}{n} < x_n \leqslant x\,;$$

thus we construct a sequence $\{x_n\}_{n=1}^{\infty} \subseteq A$ and $x_n \to x$ (by the Sandwich theorem). Therefore, Theorem 7.51 implies that $x \in A$. ▫

Definition 7.54. Let $A \subseteq \mathbb{R}$. A collection $\mathscr{F}$ of open subsets of $\mathbb{R}$ is an ***open cover*** for A if $A \subseteq \bigcup_{U\in\mathscr{F}} U$. If $\mathscr{B} \subseteq \mathscr{F}$ is a sub-collection of $\mathscr{F}$ and $\mathscr{B}$ is also an open cover for A, $\mathscr{B}$ is called an ***subcover*** of $\mathscr{F}$ (for A). $\mathscr{B}$ is called a ***finite subcover*** if there is only finitely many elements in $\mathscr{B}$.

Example 7.55. For $n \in \mathbb{N}$, let U_n denote the open set $\big(n - \frac{1}{n}, n + \frac{1}{n}\big)$, and $\mathscr{F}$ be the indexed family $\mathscr{F} \equiv \{U_n \,|\, n \in \mathbb{N}\}$. Then $\mathscr{F}$ is an open cover of $\mathbb{N}$ with no subcovers other than $\mathscr{F}$ itself.

Example 7.56. Since $\bigcup_{n=1}^{\infty}(-\infty, n) = \mathbb{R}$, the family $\mathscr{F} \equiv \big\{(-\infty, n) \,\big|\, n \in \mathbb{N}\big\}$ is an open cover for $\mathbb{R}$. There are many subcover of $\mathscr{F}$ for $\mathbb{R}$, such as

$$\big\{(-\infty, 2n) \,\big|\, n \in \mathbb{N}\big\} \quad \text{or} \quad \big\{(-\infty, 2n+1) \,\big|\, n \in \mathbb{N}\big\}.$$

Definition 7.57. A subset $K \subseteq \mathbb{R}$ is said to be ***compact*** if for every open cover $\mathscr{F}$ for K, there is a finite subcover of $\mathscr{F}$ for K. In logic notation,

$$K \text{ is compact } \Leftrightarrow (\forall\, \mathscr{F} \text{ open cover of } K)(\exists\, \mathscr{B} \subseteq \mathscr{F})\big(\#\mathscr{B} < \infty \wedge \mathscr{B} \text{ is an open cover of } K\big).$$

Example 7.58. The set $A = \{1\} \cup \left\{ \dfrac{n+1}{n} \,\middle|\, n \in \mathbb{N} \right\}$ is compact.

Let $\mathscr{F} = \big\{ U_\alpha \,\big|\, \alpha \in I \big\}$ be an open cover of A. Then $1 \in U_{\alpha_0}$ for some $\alpha_0 \in I$. Since $\mathcal{U}_{\alpha_0}$ is open, there exists $\delta > 0$ such that $\mathcal{N}(1, \delta) \subseteq \mathcal{U}_{\alpha_0}$. Since $\lim\limits_{n\to\infty} \dfrac{n+1}{n} = 1$, there exists $N > 0$ such that $\dfrac{n+1}{n} \in \mathcal{N}(1, \delta)$ for all $n \geqslant N$. Therefore,

$$\{1\} \cup \left\{ \frac{n+1}{n} \,\middle|\, n \geqslant N \right\} \subseteq U_{\alpha_0}.$$

Let U_{α_j}, where $1 \leqslant j \leqslant N-1$, be open sets in $\mathscr{F}$ such that $\dfrac{j+1}{j} \in U_{\alpha_j}$. We note that such α_j exists since $\mathscr{F}$ is an open cover for A. Then

$$A \subseteq \bigcup_{j=0}^{N-1} U_{\alpha_j}.$$

Lemma 7.59. *A compact set must be closed.*

Proof. Let K be a compact set. Suppose the contrary that there exists a convergent sequence $\{x_n\}_{n=1}^{\infty} \subseteq K$ with limit $x \notin K$. For each $y \in K$, the $\dfrac{|x-y|}{2}$-neighborhood of y is open and non-empty; thus

$$\mathscr{F} = \left\{ \mathcal{N}\big(y, \tfrac{|x-y|}{2}\big) \,\middle|\, y \in K \right\}$$

is an open cover of K. Since K is compact, there is a finite subcover

$$\mathscr{B} = \left\{ \mathcal{N}\big(y_k, \tfrac{|x-y_k|}{2}\big) \,\middle|\, 1 \leqslant k \leqslant M, y_1, \cdots, y_M \in K \right\}$$

of $\mathscr{F}$ for K. Let $\delta = \min\big\{ \frac{|x-y_1|}{2}, \frac{|x-y_2|}{2}, \cdots, \frac{|x-y_M|}{2} \big\}$. Then $|x - y_k| \geqslant 2\delta$ for $1 \leqslant k \leqslant M$ and $\delta > 0$. Since $x_n \to x$ as $n \to \infty$, there exists $N > 0$ such that $|x_n - x| < \delta$ whenever $n > N$. Then for $1 \leqslant k \leqslant M$ and $n > N$,

$$|y_k - x_n| \geqslant |y_k - x| - |x - x_n| > |y_k - x| - \frac{|y_k - x|}{2} = \frac{|y_k - x|}{2}.$$

Therefore, if $n > N$, $x_n \notin \mathcal{N}\big(y_k, \frac{|y_k - x|}{2}\big)$ which implies that $x_n \notin \bigcup\limits_{U \in \mathscr{B}} U$, a contradiction (since $x_n \in K$). ▫

Lemma 7.60. *A compact set must be bounded.*

Proof. Let $K \subseteq \mathbb{R}$ be a compact set. Define $\mathscr{F} \equiv \big\{(-n, n) \,\big|\, n \in \mathbb{N}\big\}$. Then clearly $\mathscr{F}$ is an open cover of K since $\mathscr{F}$ also covers $\mathbb{R}$. Since K is compact, there is a finite subcover

$$\mathscr{B} = \big\{(-n_k, n_k) \,\big|\, 1 \leqslant k \leqslant M, n_1, \cdots, n_M \in \mathbb{N}\big\}$$

of $\mathscr{F}$ for K. Let $N = \max\{n_1, \cdots, n_k\}$. Then

$$K \subseteq \bigcup_{k=1}^{M} (-n_k, n_k) \subseteq (-N, N)$$

which implies that $|x| \leqslant N + 1$ for all $x \in K$. Therefore, K is bounded. ▫

Theorem 7.61 (Heine-Borel Theorem)**.** *A subset $K \subseteq \mathbb{R}$ is compact if and only if K is closed and bounded.*

Proof. By Lemma 7.59 and 7.60, it suffices to shows that if K is closed and bounded, then K is compact. Let $\mathscr{F} = \big\{U_\alpha \,\big|\, \alpha \in I\big\}$ be an open cover for K. For each $x \in R$, define $K_x = \big\{a \in K \,\big|\, a < x\big\}$. Define

$$D = \big\{x \in \mathbb{R} \,\big|\, K_x \text{ is included in a union of finitely many open sets from } \mathscr{F}\big\}.$$

We claim that D is non-empty and D has no upper bound.

1. Since K is bounded, $\inf K \in \mathbb{R}$ exists. Let $z < \inf K$. Then K_z is empty which implies that $z \in D$.

2. Suppose the contrary that D is bounded from above. Then $x_0 = \sup D$ exists in $\mathbb{R}$. If there is $\varepsilon > 0$ such that $K \cap \mathcal{N}(x_0, \varepsilon) = \varnothing$, then $x_0 + \varepsilon \in D$ which contradicts to that $x_0 = \sup D$. Therefore, $K \cap \mathcal{N}(x_0, \varepsilon) \neq \varnothing$ for all $\varepsilon > 0$. By the closedness of K, $x_0 \in K$.

   Since $\mathscr{F}$ is an open cover, $x_0 \in U_{\alpha_0}$ for some $U_{\alpha_0} \in \mathscr{F}$. Since U_{α_0} is open, there exists $\delta > 0$ such that $\mathcal{N}(x_0, \delta) \subseteq U_{\alpha_0}$. Since $x_0 = \sup D$, there exists $x_1 \in (x_0 - \delta, x_0] \cap D$. Since $x_1 \in D$ there exist $U_{\alpha_1}, U_{\alpha_2}, \cdots, U_{\alpha_n} \in \mathscr{F}$ such that $K_{x_1} \subseteq \bigcup_{j=1}^{n} U_{\alpha_j}$. Let $x_2 = x_0 + \dfrac{\delta}{2}$. Then $x_2 \in U_{\alpha_0}$; thus $K_{x_2} \subseteq \bigcup_{j=0}^{n} U_{\alpha_j}$ which implies that $x_2 \in D$ which contradicts to that $x_0 = \sup D$.

Now, since K is bounded, $\sup K \in \mathbb{R}$. Since D has no upper bound, there exists $d \in D$ such that $d > \sup K$. Therefore, $K_d = K$ which implies that K is included in a union of finitely many open sets from $\mathscr{F}$; thus K is compact. ▫