MATH1081 notes

Nira (z5417727)

September 17th, 2022

Contents

1 Topic 1

1.1 Introduction

1. addition, multiplication, division and subtraction
2. Mainly dealing with finite sets

1.2 Sets and subsets

A set is a well defined collection of distinct objects

Example: $S = \{1, a, 3\}, A = \{\Pi, 1\}$.
1. $e \notin A$; it is not in A
2. For example, if A is a set of all integers; {all even integers} $= \{n \in \mathbb{R} | \text{n is even}\}$.
3. We can remove superfluos items (elements that occur more than one). $A = \{1, 2, 3, 3\}$ where 3 can be removed.

Example:
$A = \{1, 2, 3\}, B = \{2, 3, 1\}, C = \{1, 2, 3, 3\}, D = \{1, 3\}$.
Here, D is a proper subset of A, B, C; A, B, C are supersets of D.
$\subseteq$: Subset (proper subset),$\supseteq$: Superset.

1. To prove if a set is a proper subset; do the following:
For example, if $D \in A$, then check if $e \in D$
If $e \in D$, then $e \in A$. Thus, it would be a proper subset (here, e is just an element).

2. To prove that two sets are equal;
For example, if A = B, prove:
i) $A \subseteq B$; if an element is in A, then the element is in B.
ii) $B \subseteq A$; if an element is in B, then the element is in A.

1.3 Power Sets and Stability

Subsets of $A = \{1, 2, 3\}$:
1. Could throw everything out to get empty set Φ,
2. One element each: $\{1\}, \{2\}, \{3\}$,
3. Two elements: $\{1, 2\}, \{2, 3\}, \{1, 3\}$,
4. Set itself: A.
The set containing 1, 2, 3, 4 is called the powerset of A.

Given $A = \{1, 2, 3\}, B = \{1, 2, 3, 3\}, C = \{1, 3\}, D = \{1, 3\}$, where $A = B$, $C \subseteq A, B$ and $D \nsubseteq A, B, C$.
1. size of A = 3, B = 3, C = 2, D = 2.
[Exercise with A = 0, 1, 0, 1, B done in word].

1.4 Set Operations

Boolean Operators ("not" operation in programming):
1. Complement:
Let there be a set A in U (A: all of the people in the video, U: universal set of everyone in the world, A^c = complement of A).

$$\boxed{A^c = \{x \in U | x \notin A\}.}$$

2. Intersecting ("and" operation in programming):
If there is A, B, intersecting,

$$\boxed{A \cap B = \{x \in A | x \in B\}.}$$

3. Union ("or" operation in programming): If there is A, B, A or B is:

$$\boxed{A \cup B = \{x \in U | x \in A \text{ or } x \in B\}.}$$

4. Difference: If there is A, B, intersecting,

$$\boxed{A - B = \{x \in A | x \in B\}.}$$

[examples in word doc]

1.5 The Inclusion-Exclusion Principle

[example in Word]

$$\boxed{|A \cup B| = |A| + |B| - |A \cap B|.}$$

For three elements,

$$\boxed{|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.}$$

[example in word]

1.6 Sets Proofs

[proof question in word]
Hints for proofs:
1. To prove that $S \subseteq T$, we can assume that $x \in S$ and show that $x \in T$.
2. To prove that $S = T$, we can show that $S \subseteq T$ and $T \subseteq S$.

Scaffold:

Proof: Suppose that ..... (proof)we see that/ it follows ... (conclusion) (end with shaded box to indicat

Note that the "Suppose that" part of the proof is usually whatever the if statment mentions.

For example, if the question is "Prove that if $A \cap B = A$, then $A \cup B = B$, then the proof starts like this:

$\underline{Proof}$: Suppose that $A \cap B = A$.

For questions like "is this statement true", there are two ways to approach the question:
1. If the statement is true (if you think it is true), then prove it.
2. If the statement is false, then give a counter-example that proves it false.
[examples in word]

1.7 Laws of Set Algebra

Laws of Set Algebra

1. $A \cap B = B \cap A$: Commutative Law.
2. $A \cap (B \cap C) = (A \cap B) \cap C$: Associative Law.
3. $A \cap (B \cap C) = (A \cap B) \cup (A \cap C)$: Distributive Law.
4. $A \cap (A \cap B) = A$: Absorption Law.
5. $A \cap U = U \cap A = A$: Identity Law.
6. $A \cap A = A$: Idempotent Law.
7. $(A^c)^c = A$: Double Complement Law.
8. $A \cap \emptyset = \emptyset \cap A = \emptyset$: Domination Law.
9. $A \cap A^c = \emptyset$: Intersection with Complement Law.
10. $(A \cup B)^c = A^c \cap B^c$: De Moirve's Law.

The intersection can be swapped with the union to form another law (like, $A \cup B = B \cup A$ swapped as $A \cap B = B \cap A$.). Similarily, U should be swapped with $\emptyset$ and vice versa.
[examples in word]

1.8 Generalised Set Operations

Unions and Intersections; A saga:

1. $\cup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cap A_n$,
2. $\cap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$.

Example:

$$A_k = k, k+1;$$
$$= \cup_{i=1}^{3} A_k = A_1(\{1,2\}) \cup A_2(\{2,3\}) \cup A_3(\{3,4\}),$$
$$= \{1,2,3,4\}.$$

[example in word]

1.9 Russel's Paradox

A set may contain another set as one of its elements.
This raises the possibility that a set may contain itself as an element.

Problem: Try to let S be the set of all sets that are not elements of themselves, i.e., $\mathbf{S} = \{\mathbf{A} | \mathbf{A}$ is a set and $\mathbf{A} \notin \mathbf{A}\}$.
Is S an element of itself?
i) If $S \in S$, then the definition of S implies that $S \notin S$, a contradiction.
ii) If $S \notin S$, then the definition of S implies that $S \in S$, also a contradiction.
Hence neither $S \in S$ nor $S \notin S$. This is Russell's paradox.

1.10 Cartesian Product

[example in word]
The Cartesian product of two sets A and B, denoted by $A \times B$, is the set of all ordered pairs from A to B:

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

If $|A| = m$ and $|B| = n$, then we have $|A \times B| = mn$.

Sets with more than 2 elements:

Example: $A = \{a, b\}, B = \{1, 2, 3\}$.

$$\text{Cartesian Product } (A \times B) = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

(all of the ordered pairs – combinations)

[example in word]

When X and Y are small finite sets, we can use an arrow diagram to represent a subset S of $X \times Y$: we list the elements of X and the elements of Y , and then we draw an arrow from x to y for each pair $(x, y) \in S$.

1.11 Functions

Example: Take 2 sets X and Y, for which we have to find a function.

$$X = \{\text{all MATH 1081 students}\}, Y = \{0, 1, \ldots, 84, 85, \ldots, 100\}.$$

X: number of students; Y: marks from $0 - 100$.
Take function $f : X \to Y$; where X is the domain and Y is the co domain.
Ie, $f(x) =$ X's mark (Y).
Function $f : X \to Y$ satisfies $\{(x, f(x))|x \in X\} \subseteq X \times Y$ so that, for each $x \in X$;
1. $f(x)$ exists
2. $f(x)$ is unique

[example in word]

Note: be vary of the one-to-one function property lol

Floor function and ceiling functions:

1. Floor function (rounds down; smallest integer):

$$\lfloor x \rfloor = \max \{z \in Z | z \leq x\}.$$

2. Ceiling function (rounds up; largest integer):

$$\lceil x \rceil = \min \{z \in Z | z \geq x\}.$$

[example in word] Domain/codomain: $\lfloor x \rfloor / \lceil x \rceil : \mathbb{R} \to \mathbb{Z}$.

Range($\lceil x \rceil$) $= \mathbb{Z}$.

[example in word]

1.12 Image and Inverse Image

- The image of a set $A \subseteq X$ under a function $f : X \to Y$ is $f(A) = \{y \in Y \text{ — } y = f(x) \text{ for some } x \in A\} = \{f(x)|x \in A\}$.

- The inverse image of a set $B \subseteq Y$ under a function $f : X \to Y is f^{-1}(B) = \{x \in X|f(x) \in B\}$.

(image is just function values in the doman and inverse image is function values in range).

note: this is just function and inverse functions.

[example in word]

1.13 Injective, Surjective, Bijective

Formal Definitions:

Recall that if f is a function from X to Y , then for every $x \in X$, there is exactly one $y \in Y$ such that $f(x) = y$.

1. We say that a function $f : X \to Y$ is injective or one-to-one if, for every $y \in Y$, there is at most one $x \in X$ such that $f(x) = y$.
Example: for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$.

2. We say that a function $f : X \to Y$ is surjective or onto if, for every $y \in Y$, there is at least one $x \in X$ such that $f(x) = y$. the range of f is the same as the codomain of f (range(f) = Y).

3. We say that a function $f : X \to Y$ is bijective if f is both injective and surjective (one-to-one and onto).

for every $y \in Y$, there is exactly one $x \in X$ such that $f(x) = y$.
[example in word]

1.14 Composition of Functions

For functions $f : X \to Y$ and $g : Y \to Z$, the composite of f and g is the function $g \circ f : X \to Z$ defined by $(g \circ f)(x) = g(f(x))$ for all $x \in X$.

The composite function $g \circ f$ exists whenever the range of f is a subset of the domain of g.

In general, $g \circ f$ and $f \circ g$ are not the same composite functions. Associativity of composition (assuming they exist): $h \circ (g \circ f) = (h \circ g) \circ f$.

Example: Take sets $X = \{$ **all MATH1081 students** $\}, Y = \{0, 1, \ldots, 100\}, Z = \{F, P, CR, D, HD\}$.

Maps: $f = X \to Y; g = Y \to Z$.

A) $g \circ f : X \to Z$.
$(f \circ g)(y) = f(g(y))$.
[examples in word]

1.15 Identity and Inverse Functions

Identity Function:

$\boxed{i_x : x \to x; i_x(x) = x.}$

For any function $f : X \to Y$, we have $f \circ i_x = f = i_y \circ f$. A function $g : Y \to X$ is an inverse of $f : X \to Y$ if $g(f(x)) = x$ for all $x \in X$ and $f(g(y)) = y$ for all $y \in Y$,
or equivalently, $g \circ f = i_x$ and $f \circ g = i_y$.

$\boxed{\text{1. A function can have at most one inverse.}}$

If $f : X \to Y$ has an inverse, then we say that f is invertible, and we denote the inverse off by f^{-1}. Thus,$f^{-1} \circ f = i_x$ and $f \circ f^{-1} = i_y$.

If g is the inverse of f, then f is the inverse of g. Thus, $(f^{-1})^{-1} = f$.

[example in word]

1.16 Inverse Function Proofs

Theorem and Proof:

1. A function $f : X \to Y$ has at most 1 inverse

Proof:

$$\begin{aligned} &\text{Let } g_1, g_2 : Y \to X \text{ be inverse of } f. \\ &\text{Then } : g_1 = g_i \circ i_y \\ &= g_i \circ (f \circ g_2) \\ &= (g_i \circ f) \circ g_2 \\ &= i_x \circ g_2 \\ &= g_2 \text{ End of proof .} \end{aligned}$$

[example in word]

2 Number Theory and Relations

2.1 Numbers and Divisibility

[topic 2 done in word (SteelsSlides1): maybe put in definitions here ?? that depends]

Number Set Notation:

1. The positive integers: $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$,
2. The natural numbers: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$,
3. The integers: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$,
4. The rational numbers: $\mathbb{Q} = \{m/n : m \in \mathbb{Z}, n \in \mathbb{Z}^+\}$,
5. The real numbers, $\mathbb{R}$ and the complex numbers $\mathbb{C}$.

Tests (Divisibility):

1. 2 — N if and only if the decimal expansion of N ends in an even integer
2. 5 — N if and only if the last decimal digit of N is 5 or 0.
3. 3 — N if and only if the sum of the decimal digits of N is divisible by 3.
3': 9 — N if and only if the sum of the decimal digits of N is divisible by 9.
4. 11 — Nif the alternating sum of the decimal digits of N is divisible by 11. (example: $1232 = 1 - 2 + 3 - 2 = 0$)

[proof in word]

2.2 Primes

[in word]

Primes Definition: Formal: Another way of saying this is if p is prime:

$$x \text{ — } p \text{ implies } x \in \{-1, 1, -p, p\}$$

.

Theorems:

1. If p is prime and $p|ab$, then $p|a$ or $p|b$,
2. If n is composite, then it has a prime factor less than or equal to $\sqrt[2]{n}$,
3. If no prime less than or equal to $\sqrt[2]{n}$ divides n then n is a prime,
4. Every integer $n \geq 2$ can be written uniquely as a product of a finite number of primes in increasing order i.e. $n = p_1^{m_1} * p_2^{m_2} \dots p_k^{m_k}$ for primes $p_1 < p_2 < \cdots < p_k$ and exponents $m_1, m_2, \dots, m_k \in \mathbb{Z}^+$.

Open Results about Primes:

1. A prime of the form $2^n + 1$ is called a Fermat prime.
2. A prime of the form $2^n - 1$ is called a Mersenne prime.
3. Two primes that differ by 2, are called twin primes. For example, 3 and 5 are twin primes; so are 29 and 31.
4. The Goldbach Conjecture is that they are: it has been proved true for all numbers with fewer than about 17 digits.

2.3 Common Divisors and Multiples

[mostly on word]
All $a, b \in \mathbb{Z}$ have (at least) one common divisor, namely 1, and so we can define the following:
For $a, b \in \mathbb{Z}$, not both zero, the positive integer d such that

$$1.d \text{ — } aandd \text{ — } b,$$

$$2.If c \text{ — } aandc \text{ — } bthenc \leq d.$$

is called the greatest common divisor of a and b. We write $d = gcd(a, b)$.

Begin by writing a and b as a product of primes.

Properties of GCD:

1. gcd (a, b) is not affected by the signs of a or b
2. Condition (2) in the definition of gcd can be replaced by $(2')$ if c — a and c — b then c — d.
3. For $a \in \mathbb{Z}^+$, gcd $(a, 0) = a$.

Least Common Multiple

All $a, b \in \mathbb{Z}$ have (at least) one common multiple, namely ab, and so we can define the following: For $a, b \in \mathbb{Z}$, not both zero, the positive integer l such that

$$1)a \text{ — } l \text{ and } b \text{ — } l$$

2)If a — c and b — c then $l \leq c$ is called the least common multiple of a and b.

We write $l =$ lcm (a, b).

Theorem:

For all positive integers a and b; gcd$(a, b)x$ lcm $(a, b) = ab$.

Quotient and Remainder

[mostly in word]

The Quotient-Remainder Theorem (aka The Division Algorithm)

If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, then there exist unique $q, r \in Z$ such that (q: quotient; r: remainder):

$$a = bq + r \text{ and } 0 \leq r < b.$$

Note: q can be found using floor function; $q = \lfloor a/b \rfloor$.; then $r = a - qb$.

2.4 The Euclidean Algorithm

[mostly in word]

If $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

The Euclidian Algorithm: General Case [steps]

1) Let a and b be integers with $a > b \geq 0$.
2) If $b = 0$, then $\gcd(a, b) = a$.
3) If $b > 0$, use the Quotient-Remainder theorem to write $a = bq + r$ where $0 \leq r < b$. Then by our prevous result, $\gcd(a, b) = \gcd(b, r)$.
4) Repeat steps 2 and 3 to find $\gcd(b, r)$.

Example: Find $\gcd(708, 540)$

$$708 = 540 \cdot 1 + 168,$$

$$540 = 168 \cdot 3 + 36,$$

$$168 = 36 \cdot 4 + 24,$$

$$36 = 24 \cdot 1 + 12,$$

$$24 = 12 \cdot 2 + 0.$$

So,

$$\gcd\ (708, 540) = 12.$$

Note: gcd is the last non-zero remainder.

Bezout's Identity

For $a, b \in Z$ not both zero, there exist integers x and y (not unique) such that:

$\gcd\ (a, b) = ax + by.$

Theorem: Integers a and b are relatively prime if and only if there exists $x, y \in Z$ such that $ax + by = 1$.

Extended Euclidean Theorem: The Extended Euclidean Algorithm is a more efficient way of finding the numbers in Bézout's Identity: In looking for $\gcd(a, b)$, assume $a > b > 0$.
1. We make up a table with five columns labelled i, q_i, r_i, x_i, y_i, where i labels the rows.
2. We set row 1 to be $1, 0, a, 1, 0$ and row 2 to be $2, 0, b, 0, 1$. Thus $q_1 = q_2 = 0; r_1 = a, r_2 = b; x_1 = y_2 = 1; x_2 = y_1 = 0$.
3. Then for i from 3 onwards, q_i is the quotient on dividing r_{i-2} by r_{i-1} (a divided by b in the first case).

4. Then subtract q_i times the rest of row $i-1$ from row $i-2$.
5. Repeat until we get $r_{n+1} = 0$ for some n, then stop. Then the gcd is r_n and $r_n = ax_n + by_n$, that is the last row before r_i was zero gives the gcd, the x and the y.
In fact a similar identity holds at each step: $r_i = ax_i + by_i$.

2.5 Modular Arithmetic

[mostly in word]

Let $m \geq 2$ be an integer. We say that a and b are congruent modulo m if $m|(a-b)$.
We write this as:

$$a \cong b(modm).$$

The reason we have taken our modulus m to be greater than 2 is that
1) As $m|(a-b)$ iff $-m|(a-b)$, there is nothing to be gained from using negative moduli.
2) All numbers are congruent modulo 1, so that is not interesting.
3) divisibility by 0 is not defined.

Theorem
For integers $a, b$and $m, a \cong b(modm)$ if and only if there is an integer k such that $a = b + km$.

Arithmetic with Congrences
Suppose $a \cong b(modm)$ and $c \cong d(modm)$.
Then

$$(1a)(a+c) \cong (b+d)(modm).$$

$$(1b)(a-c) \cong (b-d)(modm).$$

$$(2)ac \cong bd(modm).$$

$$(3)an \cong bn(modm)foralln \in N.$$

$$(4)Ifk — mthena \cong b(modk).$$

$\boxed{note : neverdividecongruences}$

Applications of Congruence Arithmetic:
1. Pseudo-random Numbers
2. Equations with no solutions

3 Logic and Proofs

3.1 Introduction to Logic and Proofs

Mathematical proof: consists of logical deduction on the basis of agreed premises. Apart from human error the results are certain.

Techniques for Proof:

• Always explain what you are doing, and your reasons for drawing your conclusions.
• Simplify!
• Keep the aim in mind.
• Plan a solution.
• Work on one side of an equation or inequation to relate it to the other.

To study proofs: you always have to practice!! No matter what. There are techniques, but most of the time you will have to practice proofs.
What we study is methods of proof and logic.

3.2 Example of Proofs

[in word?? mostly?? i think so yeah]

Example: $\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000000}$.
Techniques:
1. Common denominator (simple answer);
2. Reciprocals; 1/2a < 1/a kinda way (bigger denominator smaller fractions)
3. Simplify

Proof. We have

$$\frac{1}{1000} - \frac{1}{1001} = \frac{1001 - 1000}{1000 \text{ x } 1001} = \frac{1}{1001000}$$

But $1001000 > 1000000$, and both are positive numbers, so

$$\frac{1}{1001000} < \frac{1}{1000000}$$

Therefore

$$\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000000}.$$

It is handy to use calculators, but this is generally bad practice as there is no understanding.

Equality proofs should ideally not be proved by calculators!

3.3 Further Examples fo Proofs

Another example:
Example: $\sqrt[8]{8!} < \sqrt[9]{9!}$.
[rough working]

$$\Rightarrow 8! < \sqrt[9]{9!^8},$$
$$\Rightarrow (8!)^9 < (9!)^8,$$
$$\Rightarrow (1 \times 2 \times \cdots \times 8)^9 < (1 \times 2 \times \cdots \times 9)^8,$$
$$\Rightarrow (1 \times 2 \times \cdots \times 8)^9 < (1 \times 2 \times \cdots \times 8)^8 \times 9^8,$$
$$\Rightarrow 1 \times 2 \times \cdots \times 8 < 9^8.$$

which is obviously less than 9 times 9 times etc, therefore making the statement true.

However, you can't start like this. Ie, you have to start with the fact that is true, then ending up with the question.
You have to check if it can be reversed (ie reversing steps in a proof: is that possible?).
(in this case, you can reverse it: proof in word.)

Things to learn from this proof:

• Go back to definitions (expand the definition)
• Simplify!
• A proof is often discovered by working backwards; but it must often be written forwards.
• Explain logical and technical steps in words (with punctuation!)

3.4 Generalisation and 'All' Statements

• For examples such as $\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000^2}$, we can replace n with 1000 to give:

$$\frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2},$$

where $\forall n \in \mathbb{Z}^+; \frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2}$.

This is called a **universal statement** (an 'All' statement). The replacement of n with 1000 as such is called **generalisation**.
[proof for the n statement in word]

Things to learn:

• A common proof pattern for $\forall x \in A,$ property B holds is:

$$\text{Let } x \in A. \ldots \text{Therefore } x \text{ has a property } B.$$

• Cannot be proved by listing examples

All Statement Written in:
•$\forall x \in A,$ property B holds;
• For Each $x \in A, x \in B$;
• every A is a B;
• if x is an $A,$ then x is a B;
• No A is not a B;
•$\forall x \in A, x \in B$;
• B is true if A is true;
• A is true only if B is true;
• property A is sufficient(information) for property B to hold;
• property B is necessary for property A to hold;

[example in word]

3.5 Exhaustion of Cases

[proofs in word]

Things to learn from these sort of proofs:
• Explain what you are doing
• Outline proof like how you would outline 'all' statement Proofs
• Often useful where there is natural division of the problem into smaller cases (like where you can use induction or splitting into cases as such);
Examples include absolute value proofs, (modular) congruences or divisibility.
• Clearly state the seperate cases, and be sure all cases really are covered.
• Patterns for "if A then B" is:

Suppose that A is true ... Therefore B is true.

• Expand the definition
• Keep aim in mind!!! Find general steps, substitute, reduce where necessary.

3.6 Writing Proofs

[proofs in word] • Usually involves two stage:
1. Discover reasons why statement is true
2. present these reasons as a coherent, carefully written argument.

Theorem 1. *Let n be an integer. If n is even, then n^2 is even.*
• *use a basic idea to prove it (for example, $n = 2k$, so $n^2 = 4k^2$).*

Things to learn from proof
• Written in complete sentences, with correct spelling and grammar!
• Sentence should begin with a word, not a variable/number.
• In text, writing equations consequtively with no words between them can make it unclear.

Bad Practice: Let $n = 2k, k \in \mathbb{Z}$.

Good practice: Let $n = 2k,$ where $k \in \mathbb{Z}$.

Structure of a Proof
• Begin with a clear statement.
• Write the word "Proof"; then begin argument.
• Any notation used; introduce variables properly.
• Logic of the proof should be clear.
• Include a conclusion that indicates end. Can include "QED" but not necessary.

Helping the reader
• Give reasons for all conclusions.
• Helpful to explain technical and algebraic steps.
• Need to make comments about variables being integers, etc.
• Try to the get the level of the argument right.

3.7 Converse; If and Only if

The **converse** of "if A then B" is "if B then A", and so forth.

Converse of a statement may or may not be true.

Converse fallacy refers to try and prove the converse of the statement because it is not true.

[examples in word]

Things to Learn from the proof

• Disproving an "all" statement just means finding a counterexample; ie find one example where A is true but B is false.

If and only if When a statement "if A then B" and converse "if B then A" are both true, then we can combine it to write "A iff B" ($A \leftrightarrow B$).

Statement can be rephrased as the following:
• "if A then B", conversely "every A is B and every B is A".
• A is a necessary and sufficient condition for B;
•$A \iff B$.

[examples in word]

Note: "Iff" statements really consists of two statements; therefore proof is of two parts.

Common proof patter for iff statements:
"Firstly, let x be an A" ..."Therefore, x is a B." "Conversely, let x be a B. ... Therefore, x is an A.

Theorem 2. *Let $n \in \mathbb{Z}$. Then, $6|n$ iff both $2|n$ and $3|n$.*

(1. suppose $6|n$, then find $2|n$ and $3|n$; then prove converse [converse; $\gcd(2,3) = 1$ therefore $2 \times 3|n$].)

Things to learn from proof:
• Expand definitions!!
• Keep goal in mind.
• Make logical subdivision clear by writing "Firstly" and "Conversely"
• Each part follows the normal format for an "if ... then" proof.
• "Similarily" saves work for the reader, not the writer.

3.8 "Some" Statements

Asserts that there exists something which satisfies a certain condition.

"There exists something such that ..." means that there is one object or more with the given property.

For example: "there exists $x \in \mathbb{R}$ such that $x^2 = 2$"

Examples of "some" statements

- Some integers are positive.
- There exists a function $f : \mathbb{R} \to \mathbb{R}$ which is both odd and even.
- Some students enjoy doing Maple tests.
- $S \neq \emptyset$.
- $6|n$.
- a is odd.

A "some" statement can be written as:

- some A is a B;
- some As are Bs;
- there exists an A which is (also) a B;
- for some $x \in A$ we have $x \in B$;
- property B holds for some $x \in A$;
- $\exists\ x \in A : x \in B$;

[example in word]

Things to learn from proofs:

- Discover the proof by working backwards; but write proof in right order.
- Real work is "behind the scenes"; requires much more knowledge of algebra and calculus.
- Proof with f gives a "some" statement which has an "all" statement within.

3.9 "Some" statements confused

Sometimes it is possible to prove a "some" statement without producing any particular object.

Example: Let $f(x) = x^5 + 2x - 2$. Then $f(x) = 0$ for some $x \in [0, 1]$.
Check end points. The graphs are continuous curves.

Proof. Let $f(x) = x^5 + 2x - 2$. Then, $f(0) = -2$, which is negative, while $f(1) = 1$; which is positive. So, the graph of f, being a continuous curve, must cross x-axis somewhere between 0 and 1; and at this crossing point we have $f(x) = 0$.
(existence proof) therefore, it completes the proof.

[other example in word]

Things to learn from proofs:

• Needed background knowledge
• Tedious to find actual x and y values to prove, so find generic solutions that make proofs easier.
• "Clearly" does not mean you don't have to check the following statement. (ie you have to check if the most obvious statement in the question is also true.)

Existence and uniqueness. A statement of the form "there exists a unique $x \in S$ such that ..."
asserts that there is one and only one object having the given property.

Proof for such statements:
• show $\exists$ an object with given property;
• show there cannot be two diff objects with property. Common proof patter is as follows:

"Suppose that x_1 and x_2 have the same property."
...
"Therefore, $x_1 = x_2$."

[examples in word: $a = bq + r$.]

Things to learn from proof:
• Clearly distinguish the "existence" and "uniqueness" parts of the proof.

3.10 Multiple Quantifiers

• The words "all" and "some" -¿ quantifiers. A statement can have more than one quantifier.

Examples:
• For every $x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ such that $y > x$.
• $\exists y \in \mathbb{Z}$ such that for every $x \in \mathbb{Z}, y > x$. (not the same as the first statement.)
• $2^29 - 1$ is composite. (rewrite: $2^29 - 1 = ab$ where $a > 1, b > 1$ for some integers a, b.)
• For any prime there is a larger prime.
• $(6, -1, 5)$ is a linear combination of $(1, 1, 2)$ and $(1, 2, 3)$.
• There is a function $f : \mathbb{R} \to \mathbb{R}$ which is equal to its own derivative.
• Every positive real number has a real square root.
• For all $A, B, C \subseteq U, A \cup (B \cup C) = (A \cup B) \cup C$.
• The function $f : X \to Y$ is onto.

Theorem 3. *Any composite positive integer has a factor greater than* 1 *and less than or equal to its square root.*

Note: Making the quantifiers explicit, the statement is:

"for every composite integer n $\exists$ c, a factor of n such that $c > 1$ and $c \leq \sqrt{n}$".

Let n be composite.

$$n = ab, a > 1, b > 1.$$

Case $I : a \leq \sqrt{(n)}$

$$c = a, \text{ has required properties.}$$

Case $II : a > \sqrt{n}$

$$c = b; b = \frac{n}{a} < \frac{n}{\sqrt{n}} = \sqrt{n}.$$

Therefore, $c|n, 1 < c \leq \sqrt{n}$.

Things to learn from proof:
• Rewrite the given statement if necessary to make the quantifiers clear.
• Patter of "all" proof: within this, patter of "existence" proof.
• Another example of "proof by exhaustion" of cases.
• Expand the defintion!!

3.11 Multiple quantifiers continued (limits)

Theorem 4. $\lim_{x\to\infty} \frac{4x^2+7x+19}{2x^2+3} = 2$.

Note: According to definition of a limit, we must show that for every $\epsilon > 0, \exists$ a real number M such that

$$\text{if } x > M \text{ then } | \frac{4x^2+7x+19}{2x^2+3} - 2 | < \epsilon.$$

Proof: Let $x > 0$.
Choose $M = \max(1, \frac{10}{\epsilon})$.
Let $x > M$. Then

$$x > 1 \text{ and } x > \frac{10}{\epsilon}.$$

so

$$\begin{aligned} | \frac{4x^2+7x+19}{2x^2+3} - 2 | &= | \frac{7x+13}{2x^2+3} |, \\ &= \frac{7x+13}{2x^2+3}, \\ &< \frac{7x+13}{2x^2} \text{ (because } x > 1), \\ &= \frac{10}{x}, \\ &= \frac{10}{\frac{10}{\epsilon}} \text{ (since } x = \frac{10}{\epsilon}), \\ &= \epsilon. \end{aligned}$$

Therefore, $\lim_{x\to\infty} \frac{4x^2+7x+19}{2x^2+3} = 2$.

Things to learn from proof:
• Expand definition!!
• Logical structure of statement to be proved is: "for all ... there exists ... such that if ... then ...", and proof follows structure properly.
• Working backwards is very important!!

3.12 Change of order of quantifiers

Two adjacent quantifiers of the same kind can be interchanged. Example:

$$\exists\ \alpha \in \mathbb{R}, \exists\ \beta \in \mathbb{R}, (6, -1, 5) = \alpha(1, 1, 2) + \beta(1, 2, 3).$$

means the same as:

$$\exists\ \beta \in \mathbb{R}, \exists\ \alpha \in \mathbb{R}, (6, -1, 5) = \alpha(1, 1, 2) + \beta(1, 2, 3).$$

as both statements exert two variables being real numbers; satifies equation.

Another example:

$$\forall A \subseteq U, \forall B \subseteq U, A \cap B = B \cap A.$$

and

$$\forall B \subseteq U, \forall A \subseteq U, A \cap B = B \cap A.$$

are the same as it is both subsets of U.

"All" and a "some" quantifier may not be interchanged.

[example in word]

Things to learn from proof:
- Clearly distinguish between what is given and what you have to prove
- "imaginative" step of the proof: come up with 'numbers' to suit the equation.
- Working backwards is important
- Going back to the definition is a profitable idea.