

# MATH1081 notes

Nira (z5417727)

September 17th, 2022

## Contents

<b>1</b>	<b>Topic 1</b>	<b>2</b>
1.1	Introduction . . . . .	2
1.2	Sets and subsets . . . . .	3
1.3	Power Sets and Stability . . . . .	4
1.4	Set Operations . . . . .	5
1.5	The Inclusion-Exclusion Principle . . . . .	6
1.6	Sets Proofs . . . . .	7
1.7	Laws of Set Algebra . . . . .	8
1.8	Generalised Set Operations . . . . .	9
1.9	Russel's Paradox . . . . .	10
1.10	Cartesian Product . . . . .	11
1.11	Functions . . . . .	12
1.12	Image and Inverse Image . . . . .	13
1.13	Injective, Surjective, Bijective . . . . .	14
1.14	Composition of Functions . . . . .	15
1.15	Identity and Inverse Functions . . . . .	16
1.16	Inverse Function Proofs . . . . .	17
<b>2</b>	<b>Number Theory and Relations</b>	<b>18</b>
2.1	Numbers and Divisibility . . . . .	18
2.2	Primes . . . . .	19
2.3	Common Divisors and Multiples . . . . .	20
2.4	The Euclidean Algorithm . . . . .	22
2.5	Modular Arithmetic . . . . .	24

# **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;  $\{\text{all even integers}\} = \{n \in \mathbb{R} | n \text{ is even}\}$ .
3. We can remove superfluous 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  $\Phi$ ,
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  $D \not\subseteq A, B, C$ .

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  $A$ ).

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

2. Intersecting ("and" operation in programming):

If there is  $A, B$ , intersecting,

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

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

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

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

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

[examples in word doc]

## 1.5 The Inclusion-Exclusion Principle

[example in Word]

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

For three elements,

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

[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 indicate)
--

Note that the "Suppose that" part of the proof is usually whatever the if statement 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:

<u>Proof</u> : 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.  $A \cap (A \cup B) = A$  : 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  $A \cap B = B \cap A$ ). Similarly,  $U$  should be swapped with  $\emptyset$  and vice versa.

[examples in word]



## 1.8 Generalised Set Operations

Unions and Intersections; A saga:

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

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

Example:

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

[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.,  $S = \{A \mid A \text{ is a set and } A \notin A\}$ .

**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:

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

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

Sets with more than 2 elements:

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

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.

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

$X$ : number of students;  $Y$ : marks from 0 – 100.

Take function  $f : X \rightarrow Y$ ; where  $X$  is the domain and  $Y$  is the co domain.

Ie,  $f(x)$  =  $X$ 's mark ( $Y$ ).

Function  $f : X \rightarrow Y$  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):

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

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

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

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

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  $f : X \rightarrow Y$  is  $f(A) = \{y \in Y \mid y = f(x) \text{ for some } x \in A\} = \{f(x) \mid x \in A\}$ .

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

(image is just function values in the domain 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  $f : X \rightarrow Y$  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  $f : X \rightarrow Y$  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  $f$  ( $\text{range}(f) = Y$ ).

3. We say that a function  $f : X \rightarrow Y$  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  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$ , the composite of  $f$  and  $g$  is the function  $g \circ f : X \rightarrow Z$  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  $X = \{ \text{all MATH1081 students} \}$ ,  $Y = \{0, 1, \dots, 100\}$ ,  $Z = \{F, P, CR, D, HD\}$ .

Maps:  $f : X \rightarrow Y$ ;  $g : Y \rightarrow Z$ .

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

## 1.15 Identity and Inverse Functions

Identity Function:

$$i_x : x \rightarrow x; i_x(x) = x.$$

For any function  $f : X \rightarrow Y$ , we have  $f \circ i_x = f = i_y \circ f$ . A function  $g : Y \rightarrow X$  is an inverse of  $f : X \rightarrow Y$  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  $f \circ g = i_y$ .

1. A function can have at most one inverse.

If  $f : X \rightarrow Y$  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  $f : X \rightarrow Y$  has at most 1 inverse

Proof:

Let  $g_1, g_2 : Y \rightarrow X$  be inverse of  $f$ .

$$\text{Then } g_1 = g_1 \circ i_y$$

$$= g_1 \circ (f \circ g_2)$$

$$= (g_1 \circ f) \circ g_2$$

$$= i_x \circ g_2$$

$$= g_2 \text{ End of proof .}$$

[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.  $2 \mid N$  if and only if the decimal expansion of  $N$  ends in an even integer
2.  $5 \mid N$  if and only if the last decimal digit of  $N$  is 5 or 0.
3.  $3 \mid N$  if and only if the sum of the decimal digits of  $N$  is divisible by 3.
- 3':  $9 \mid N$  if and only if the sum of the decimal digits of  $N$  is divisible by 9.
4.  $11 \mid N$  if 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:

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

.

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  $\sqrt[n]{n}$ ,
3. If no prime less than or equal to  $\sqrt[n]{n}$  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  $p_1 < p_2 < \dots < p_k$  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

$$1. d \mid a \text{ and } d \mid b,$$

$$2. \text{ If } c \mid a \text{ and } c \mid b \text{ then } c \leq d.$$

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  $c \mid a$  and  $c \mid b$  then  $c \mid d$ .
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

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

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

We write  $l = \text{lcm}(a, b)$ .

Theorem:

For all positive integers  $a$  and  $b$ ;  $\gcd(a, b) \times \text{lcm}(a, b) = ab$ .

## 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  $q, r \in \mathbb{Z}$  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 previous 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  $a, b \in \mathbb{Z}$  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  $x, y \in \mathbb{Z}$  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  $m \mid (a - b)$ .

We write this as:

$$a \cong b(\text{mod } m).$$