

# MTHE 217 - Lecture Notes

## ALGEBRAIC STRUCTURES WITH APPLICATIONS

Prof. Felix Parraud • Fall 2025 • Queen's University

### Contents

<b>1</b>	<b>Propositional Logic</b>	<b>3</b>
1.1	Connectives . . . . .	3
<b>2</b>	<b>Valid Arguments</b>	<b>5</b>
2.1	Statement Definitions . . . . .	5
2.2	Logical Relationships . . . . .	5
2.3	Important Tricks and Definitions . . . . .	5
<b>3</b>	<b>Proof Examples</b>	<b>7</b>
3.1	Proof with multiple premises . . . . .	7
3.2	Methods of proof . . . . .	8
3.3	Logic Gates . . . . .	8
<b>4</b>	<b>Set Theory</b>	<b>9</b>
4.1	Quantifiers and definitions . . . . .	9
4.2	Sets . . . . .	9
<b>5</b>	<b>Operations on Sets</b>	<b>10</b>
5.1	Definitions . . . . .	10
5.2	Finite and Disjoint Sets . . . . .	10
5.3	Inclusion-Exclusion Theorem . . . . .	11
<b>6</b>	<b>Equivalence Relations and Functions</b>	<b>12</b>
6.1	Cartesian Product . . . . .	12
6.2	Binary Relation . . . . .	12
6.3	Orderings . . . . .	12
6.4	Equivalence Relations . . . . .	12
<b>7</b>	<b>Equivalence class and congruence classes</b>	<b>14</b>
7.1	Congruence is an equivalence relation proof . . . . .	14
7.2	Equivalence class and congruence class . . . . .	14
7.3	Partition . . . . .	15
<b>8</b>	<b>Functions</b>	<b>16</b>
8.1	Definition . . . . .	16
8.2	Images . . . . .	16

<b>9</b>	<b>Function properties</b>	<b>17</b>
9.1	Injective, Surjective, Bijective . . . . .	17
9.2	Composition of Functions . . . . .	17
9.3	Identity function and inverses of functions . . . . .	17
<b>10</b>	<b>Inverse of a Function</b>	<b>18</b>
10.1	Bijection-Invertibility Equivalence . . . . .	18
10.2	Cardinality . . . . .	19
<b>11</b>	<b>Induction Principle</b>	<b>20</b>
11.1	Proving the principle of mathematical induction using the well-ordering principle . . . . .	20

# 1 Propositional Logic

Our goal is to replace words with symbols, and to avoid quantifiers.

A proposition is a sentence or assertion that is true (T) or false (F), but not both

A statement is a proposition, or two statements joined by a connective

## 1.1 Connectives

Connectives (or boolean operators) are functions that take one or more truth values and output a truth value

### Negation (not)

Let  $p$  be a proposition. The negation of  $p$ , denoted by  $\neg p$ , is the denial of  $p$

If  $p$  is  $T$ , then  $\neg p$  is  $F$

The negation or “not” gate is depicted by



### Conjunction (and)

The conjunction of  $p$  and  $q$  is denoted by  $p \wedge q$ . It can also be calculated by  $pq$

$p$	$q$	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

The conjunction gate is depicted by



### Disjunction (or)

The disjunction of  $p$  and  $q$  is denoted by  $p \vee q$ . It can also be calculated by  $p + q$

OR is true if at least one of the statements is true.

XOR is true if exactly one of the statements is true, but **not both**, and has the same truth table as  $\neg(p \leftrightarrow q)$

$p$	$q$	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

The disjunction gate is depicted by



### Conditional (if $p$ , then $q$ )

The conditional of  $p$  and  $q$  is denoted by  $p \rightarrow q$ , where  $p$  is called the antecedent and  $q$  is called the consequent of the conditional. This is the same as  $(\neg q \vee p)$

$p$	$q$	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Intuition: The conditional promises that whenever  $p$  holds,  $q$  must also hold. If  $p$  never happens (false), the promise is not broken, so the conditional is automatically true.

### Biconditional (iff)

The biconditional of  $p$  and  $q$  is denoted by  $p \leftrightarrow q$ , and can be thought of as “if and only if”. This can also be written as  $(p \rightarrow q) \wedge (q \rightarrow p)$ .

$p$	$q$	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

### More Definitions

The **converse** of  $p \rightarrow q$  is  $q \rightarrow p$ . The **inverse** of  $p \rightarrow q$  is  $\neg p \rightarrow \neg q$ . The **contrapositive** of  $p \rightarrow q$  is  $\neg q \rightarrow \neg p$ .

## 2 Valid Arguments

A **premise** is a statement (a declarative sentence, either T or F) that is assumed to be true within an argument

When writing a final solution, we write the premises, then the conclusion:

$$[\neg b \rightarrow (p \leftrightarrow r)] \wedge [\neg b \rightarrow r] \wedge [p \rightarrow \neg r]$$

Conclusion:  $\neg r$

### 2.1 Statement Definitions

A statement is called a **tautology** if it is always true (e.g.  $s = p \vee \neg p$ )

A statement is called a **fallacy** if it is always false (e.g.  $s = p \wedge \neg p$ )

### 2.2 Logical Relationships

Let  $s$  and  $q$  be two statement forms involving the same set of propositions

We say that  $s$  **logically implies**  $q$  and write  $s \Rightarrow q$  if whenever  $s$  is true,  $q$  is also true

We say that  $s$  logically equivalent  $q$  and write  $s \Leftrightarrow q$  if both  $s$  and  $q$  have identical truth tables

### 2.3 Important Tricks and Definitions

*a true statement cannot imply a false one*

**Contradiction (fallacy)**  $p \wedge \neg p \Leftrightarrow F$

**Tautologies** Law of excluded middle:  $P \vee \neg P = T$  Law of non-contradiction:  $\neg(P \wedge \neg P) = T$

$$p \wedge F \Leftrightarrow F \quad p \wedge T \Leftrightarrow p \quad p \vee T \Leftrightarrow T \quad p \vee F \Leftrightarrow p$$

*if the engine fails, then part p or part q is failing*  $\neg(p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$

**Distributivity**  $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$   $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

**Contrapositive** *if P implies Q, then not Q implies not P*  $P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$

**De Morgan's laws:**  $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$   $\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$

**Double negation**  $\neg(\neg P) \equiv P$

**Absorption** *if it rains, it is wet, but, if it isn't wet, it didn't rain*  $p \wedge (p \vee q) \Leftrightarrow p$   
 $p \vee (p \wedge q) \Leftrightarrow p$

**Modus ponens:**  $(P \rightarrow Q), P \therefore Q$ , means If  $P$  implies  $Q$ , and  $P$  is true, then  $Q$  must be true

Example: If it rains, then the ground is wet. So, when it rains, the ground is wet. However, if the ground is wet, it did not necessarily rain.

**Modus tollens:**  $(P \rightarrow Q), \neg Q \therefore \neg P$ , means if  $P$  implies  $Q$ , and  $Q$  is false, then  $P$  must also be false

Example: If it rains, then the ground is wet. If the ground is not wet, then it did not rain.

### 3 Proof Examples

A proof is an argument which shows that  $S \Rightarrow Q$ , where  $S$  and  $Q$  are statement forms

#### Proof 1

$S \Leftrightarrow Q$  if and only if  $S \leftrightarrow Q$  is a tautology

Forwards proof:

If  $S \leftrightarrow Q$  is a tautology, then it cannot be false. So, while one statement is true, the other cannot be false.  $\therefore$  if  $S$  and  $Q$  are  $T$  or  $F$  at the same time, then  $S \Leftrightarrow Q$

Backwards proof:

If  $S$  and  $Q$  are logically equivalent,  $S = T$  and  $Q = T$ , or  $S = F$  and  $Q = F$ , but no mixed case.  $\therefore$  we are always in case of  $T$  if  $S \leftrightarrow Q$ . Hence,  $S \leftrightarrow Q$  is a tautology

#### Proof 2

$S \Rightarrow Q$  iff  $S \rightarrow Q$  is a tautology

Forwards proof:

By definition, if  $S \Rightarrow Q$ , then whenever  $S$  is  $T$ ,  $Q$  is also  $T$

Consider the truth table of  $S \rightarrow Q$ , the only case where this is false is when  $S$  is  $T$  and  $Q$  is  $F$ . There is no interpretation of  $S \Rightarrow Q$  where  $S$  is  $T$  and  $Q$  is  $F$

Therefore, in every interpretation,  $S \rightarrow Q$  is  $T$ , and is a tautology

Backwards proof:

If  $S \rightarrow Q$  is a tautology, then the interpretation where  $S$  is  $T$  and  $Q$  is false is excluded

Thus, whenever  $S$  is  $T$ ,  $Q$  must also be  $T$ , and by definition, this means that  $S \Rightarrow Q$

$\therefore S \Rightarrow Q \Leftrightarrow (S \rightarrow Q)$  is a tautology  $\square$

#### 3.1 Proof with multiple premises

Definition: An argument with premises  $p_1, \dots, p_n$  and conclusion  $q$  is valid (true) if  $p_1 \wedge \dots \wedge p_n \Rightarrow q$

We can prove  $\neg b \rightarrow (p \leftrightarrow q) \wedge (r \rightarrow \neg b) \wedge (p \rightarrow \neg r) \Rightarrow \neg r$  by setting it equal to  $s$  and showing that it is a tautology

Instead of examining  $2^3 = 8$  possible values for statements  $b, p$ , and  $r$  (brute force), we can prove that  $s$  is a tautology **by contradiction**

If  $s$  is not a tautology, there must be a truth-assignment making  $\neg r = F$  and  $q_1 = q_2 = q_3 = T$

Proof:

$$\neg r = F, r = T$$

$$q_3 = T, p \rightarrow \neg r = T, p \rightarrow F = T, p = F$$

$$q_2 = T, r \rightarrow \neg b = T, F \rightarrow \neg b = T, b = F$$

$$q_1 = \neg b \rightarrow (p \leftrightarrow r), T \rightarrow (F \leftrightarrow T), T \rightarrow F = F, \text{ but } q_1 \text{ must be true}$$

So, this means that  $s = F$  cannot happen  $\therefore$  no truth assignment can make  $s = F$ , hence,  $s$  is a tautology  $\square$

### 3.2 Methods of proof

1. Directly solve it, i.e. show that  $P \rightarrow Q$  is a tautology
2. Proof by contraposition: show  $\neg Q \Rightarrow \neg P$ , i.e. show that  $\neg Q \rightarrow \neg P$  is a tautology
3. Proof by contradiction: show that  $\neg P \vee Q$  is a tautology

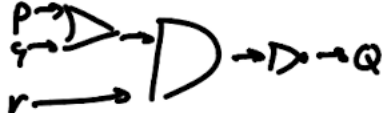
### 3.3 Logic Gates

#### Logic Gates:

a) gate AND  $p \rightarrow q \Rightarrow D \rightarrow p \wedge q$

gate OR  $p \rightarrow q \Rightarrow D \rightarrow p \vee q$

gate NOT  $p \rightarrow D \rightarrow \neg p$

ex:  $\neg[(p \wedge q) \wedge r] = Q$ : 

ex:  $Q = ((a \vee c) \wedge \neg a) \wedge b$

$$Q \Leftrightarrow ((a \vee c) \wedge \neg a) \wedge b$$

$$\Leftrightarrow ((a \wedge \neg a) \vee (c \wedge \neg a)) \wedge b \quad : a \wedge \neg a = F$$

$$\Leftrightarrow (F \vee (c \wedge \neg a)) \wedge b \quad : F \vee (...) = (...)$$

$$\Leftrightarrow (c \wedge \neg a) \wedge b$$





## 4 Set Theory

### 4.1 Quantifiers and definitions

: stands for “such that”  $\exists$  stands for “there exists”  $\forall$  stands for “for all”

Let  $X$  be the set of all sets which do not contain themselves:  $X = \{Y : Y \notin Y\}$ . Is  $X$  a member of itself? If it is, then it shouldn't be. If it's not, then it should.

We can also apply De Morgan's law for quantifiers (we can distribute  $\neg$ ):

$$\neg(\exists x, P(x)) \Leftrightarrow \forall x, \neg P(x) \quad \neg(\forall x, P(x)) \Leftrightarrow \exists x, \neg P(x)$$

The statement  $P_A(x)$  is defined as:  $P_A(x) =$

$$\begin{cases} T & \text{if } x \in A, \\ F & \text{if } x \notin A \end{cases}$$

### 4.2 Sets

A set  $S$  is a collection of objects Subset:  $A \subseteq B$  if every element  $\in A$  is  $\in B$  Equal sets:  $A = B \Leftrightarrow \forall x \in U, P_A(x) \Leftrightarrow P_B(x)$

The universal set  $U$  is the set that contains all the objects under consideration in a given context

**Note:** in Zermelo-Fraenkel set theory (ZFC), there is actually no absolute universal set. This would lead to Russell's paradox

$\mathbf{N} = \{0, 1, 2, \dots\}$   $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$   $\mathbf{Q} = \left\{\frac{a}{b} : a, b \in \mathbf{Z}, b \neq 0\right\}$   $\mathbf{R}$ , real numbers  
 $\mathbf{C} = \{a + bi : a, b \in \mathbf{R}, i = \sqrt{-1}\}$

The following holds:  $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$

## 5 Operations on Sets

Sets are unordered.

### 5.1 Definitions

The union of sets, denoted by  $X \cup Y$ ,  $= \{x : x \in X \vee x \in Y\}$ : **everything that's either in  $X$  or  $Y$**

The intersection of sets, denoted by  $X \cap Y$ ,  $= \{x : x \in X \wedge x \in Y\} = \{x \in X : x \in Y\}$ , **only the elements that  $X$  and  $Y$  have in common**

The set difference of sets, denoted by  $XY$ ,  $= \{x \in X : x \notin Y\}$  or  $X \cap X^c$ : **\*\*the elements that are in  $X$  but not in  $Y$**

The symmetric difference of sets, denoted by  $X \Delta Y$ ,  $= (X \cup Y) \setminus (X \cap Y)$  or  $(XY) \cup (YX)$ : **the elements that are in either  $X$  or  $Y$ , but not in both**

A **family** of elements of  $X$  is an indexed collection  $(x_i)_{i \in A}$  where  $A$  is out index set and each  $x_i \in X$

**Further:**

$A \cup \emptyset = A$   $A \cup U = U$   $A \cup (B \cap C) = (A \cup B) \cap C$   $A \cap U = A$  If  $Y \subseteq X$ , then we sometimes write  $Y^c = XY$  for the complement of  $Y$  in  $X$  **## Proof:**  $A \subseteq B \Leftrightarrow A \cap B = A$

**Forward:** Assume that  $A \subseteq B$ . That means if  $x \in A$ , then  $x \in B$

So if  $x \in A$ , then  $x \in A$  and  $x \in B$ , which means  $x \in (A \cap B)$ , hence  $A \subseteq (A \cap B)$

Besides, if  $x \in A \cap B$ , then by definition  $x \in A$ , hence  $A \cap B \subseteq A$

Since  $A \subseteq (A \cap B)$  and  $(A \cap B) \subseteq A$ , we get  $A \cap B = A$

**Backward:** Assume  $A \cap B = A$

Take any  $x \in A$ . Then  $x \in A \cap B$  since they are equal

By definition of intersection,  $x \in B$  as well

Thus every element of  $A$  is also in  $B$ , i.e.  $A \subseteq B$

**Conclusion:**  $A \subseteq B$  if and only if  $A \cap B = A$

### 5.2 Finite and Disjoint Sets

**Finite sets:** Sets  $X, Y$  and  $Z$  are finite sets if the number of distinct elements in these sets is given by a natural number (rather than some "infinite cardinal"). When a set is finite, we use  $|X|$  to denote its size

**Disjoint sets:** Two sets  $A$  and  $B$  are disjoint if they have no elements in common. Essentially, they are non-overlapping

**Pairwise disjoint sets:** A collection of sets is pairwise disjoint if **every pair** of distinct sets in the collection is disjoint, i.e.  $A_i \cap A_j = \emptyset$  for all  $i \neq j$

If  $X_1, \dots, X_n$  are pairwise disjoint then  $|X_1 \cup \dots \cup X_n| = |X_1| + \dots + |X_n|$

### 5.3 Inclusion-Exclusion Theorem

If sets  $X, Y$  and  $Z$  are not disjoint, then:

$$|X \cup Y| = |X| + |Y| - |X \cap Y|$$

The last term leaves if the sets are disjoint, because the intersection of disjoint sets is 0

**Proof:**

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

We want to express  $A \cup B$  as a union of disjoint sets.

We can start by expression  $A$  and  $B$  as a union of disjoint sets. Here we are essentially saying that every set can be split into two disjoint parts using another set

$$A = (A \cap B) \cup (A \cap B^c) \text{ and } B = (A \cap B) \cup (A^c \cap B)$$

Now, we can express  $A \cup B$  as a union of three disjoint pieces:  $A \cup B = (A \cap B) \cup (A \cap B^c) \cup (A^c \cap B)$

These three sets are pairwise disjoint. So:  $|A \cup B| = |A \cap B| + |A \cap B^c| + |A^c \cap B|$

From earlier, we can now rewrite:  $|A| = |A \cap B| + |A \cap B^c|$  and  $|B| = |A \cap B| + |A^c \cap B|$

$$|A| + |B| = (|A \cap B| + |A \cap B^c|) + (|A \cap B| + |A^c \cap B|)$$

$$|A| + |B| = 2|A \cap B| + |A \cap B^c| + |A^c \cap B|$$

We can now rearrange and see that the RHS is exactly  $|A \cup B|$  from earlier:  $|A| + |B| - |A \cap B| = |A \cap B| + |A \cap B^c| + |A^c \cap B|$

Therefore:  $|A \cup B| = |A| + |B| - |A \cap B|$

## 6 Equivalence Relations and Functions

### 6.1 Cartesian Product

**Definition:** For two objects  $a, b$ , we write  $(a, b)$  for the ordered pair  $a$  and  $b$

**Definition:** The Cartesian product of sets  $A, B$  is  $A \times B = \{(a, b) | a \in A, b \in B\}$

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

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

### 6.2 Binary Relation

**Definition:** If  $X$  and  $Y$  are sets, then a **binary relation** from  $X$  to  $Y$  is a subset  $R \subseteq X \times Y$ . Whenever  $(x, y) \in R$ , we write  $xRy$  and say that “ $x$  is related to  $y$  under  $R$ ”

**The divisibility relation:** Let  $X = \{1, 2, 3, 4\}$ , then  $D$  on  $X$  is the subset  $D \subseteq X \times X$  given by  $D = \{(2, 2), (2, 4), (2, 6), (3, 3), \dots\}$ . We say  $a|b$  if  $b = Ra$  for some  $R \in \mathbf{Z}$

**The equality relation:** Is the subset  $E \subseteq X \times X$  given by  $D = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$

### 6.3 Orderings

A set  $X$  can be ordered with either a partial order or a total order.

**Definition:** A partial order on  $X$  is a binary relation  $\leq$  on  $X$  that is **reflexive, anti-symmetric, and transitive**

A **total order** is a partial order where every pair  $x, y \in X$  satisfies either  $x \leq y$  or  $y \leq x$

### 6.4 Equivalence Relations

**Definition:** A relation  $E$  on a set  $X$  is an equivalence relation if it is **reflexive, symmetric, and transitive**

**Reflexive:**  $xEx$  for all  $x \in X$  Everyone is related to themselves

**Symmetric:**  $xEy$  implies  $yEx$  for all  $x, y \in X$  If you’re related to me, then I’m related to you. Both directions are always allowed.

**Transitive:**  $xEy$  and  $yEz$  implies  $xEz$  for all  $x, y, z \in X$ , If A is related to B, and B is related to C, then A is related to C

**Antisymmetric:**  $x \leq y$  and  $y \leq x$  implies  $x = y$  for all  $x, y \in X$  The only way two different things can both be related in both directions is if they’re actually the same thing. Both directions are only allowed when it’s the same element.

**Equivalence Relation (and Classes) Example**

Pg. 115, Problem 7

7. Let  $X$  be the set  $\{1, 2, 3, 4\}$  and let

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}.$$

Show that  $R$  is an equivalence relation and write down its equivalence classes.

**Reflexive:** if  $(x, x) \in R$  for all  $x \in X$

$(1, 1), (2, 2), (3, 3), (4, 4)$  are all present, so  $R$  is reflexive

**Symmetric:** if whenever  $(a, b) \in R$ , then  $(b, a) \in R$

$(1, 2)$  and  $(2, 1)$  are both in  $R$   $(3, 4)$  and  $(4, 3)$  are both in  $R$ , so  $R$  is symmetric

**Transitive:** if whenever  $(a, b) \in R$  and  $(b, c) \in R$ , then  $(a, c) \in R$

From  $(1, 2)$  and  $(2, 1)$ , we need  $(1, 1)$ , true From  $(1, 2)$  and  $(2, 2)$ , we need  $(1, 2)$ , true From  $(2, 1)$  and  $(2, 2)$ , we need  $(2, 2)$ , true etc.,  $R$  is transitive

**Equivalence classes:** equivalence class of  $a$  is the set of all elements in  $X$  that are related to  $a$  under relation  $R$

$a = 1$ , all pairs starting with 1 :  $(1, 1), (1, 2) \therefore [1] = \{1, 2\}$   $a = 2$ , all pairs starting with 2 :  $(2, 1), (2, 2) \therefore [2] = \{1, 2\} = [1]$ , as expected in an equivalence relation  $a = 3$ , all pairs starting with 3 :  $(3, 3), (3, 4) \therefore [3] = \{3, 4\}$   $a = 4$ , all pairs starting with 4 :  $(4, 3), (4, 4) \therefore [4] = \{3, 4\} = [3]$ , as expected

The equivalence classes group the elements into disjoint sets:  $\{1, 2\}, \{3, 4\}$ , this is exactly the partition of  $X$  induced by  $R$

### Congruent modulo

This is an example of an equivalence relation but also its own definition, as follows:

**Definition of Congruence modulo  $n$ :** Fix  $n \in \mathbf{Z}$ . We say  $a, b \in \mathbf{Z}$  are congruent modulo  $n$  and write  $a \equiv b \pmod{n}$ . Basically,  $n$  divides the difference in  $a$  and  $b$ . Or,  $a - b$  is a multiple of  $n$

**Example 1:**  $10 \equiv 2 \pmod{4}$  because  $\frac{10-2}{4} \in \mathbf{Z}$

**Example 2:**  $9 \not\equiv 2 \pmod{3}$  because  $\frac{9-2}{3} \notin \mathbf{Z}$

## 7 Equivalence class and congruence classes

### 7.1 Congruence is an equivalence relation proof

**Definition:** Two integers are congruent mod  $n$ ,  $n > 0$ , if the integers leave the same remainder upon division by  $n$

Congruence is an equivalence relation:

**Reflexive:**

$$a \in \mathbf{Z}, a - a = 0 = 0n, \therefore a \equiv a \pmod{n}$$

**Symmetric:**

$\forall a, b \in \mathbf{Z}$  with  $a \equiv b \pmod{n}$ , then  $a - b = qn$  for some  $q \in \mathbf{Z}$ . Thus,  $b - a = (-q)n$  and hence  $b \equiv a \pmod{n}$ ,  $\therefore$  symmetric

**Transitive:**

Take  $a, b, c \in \mathbf{Z}$  with  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$ , we want to show that  $a \equiv c \pmod{n}$ . First,  $a - b = qn$  and  $b - c = rn$  for some  $q, r \in \mathbf{Z}$ . Adding these two expressions gives  $a - c = qn + rn = (q + r)n$ ,  $\therefore a \equiv c \pmod{n}$  and it is transitive

### 7.2 Equivalence class and congruence class

Given an equivalence relation  $\sim$  on  $X$ , the equivalence class of  $a \in X$  is the set  $[a] = \{b \in X : b \sim a\}$ . This is the group of all things in  $X$  that are related to  $a$

If our equivalence relation is congruence modulo  $n$  on  $\mathbf{Z}$ , then equivalence classes of integers are called *congruence classes*.

#### Congruence classes LEGO analogy

Say we have a set of bricks, and the equivalence relation is that two bricks are equivalent if they have the same colour

The green bricks will form an equivalence class.

So, every brick is in exactly one bin, thus the bins don't overlap. This collection of bins is called a partition of the LEGO set.

#### Congruence classes example

Suppose we have integers  $\dots, -2, -1, 0, 1, 2, \dots$

Pick a number  $n$ . Suppose  $n = 4$ . Now we build 4 buckets, labeled 0, 1, 2, 3

Bucket 0: all integers that leave remainder 0 when divided by 4  $[0] = \{b \in \mathbf{Z} : b \equiv 0 \pmod{4}\} = \dots, -8, -4, 0, 4, 8, \dots$

Bucket 1: all integers that leave remainder 1 when divided by 4  $[1] = \{b \in \mathbf{Z} : b \equiv 1 \pmod{4}\} = \dots, -7, -3, 1, 5, 9, \dots$

Bucket 2: all integers that leave remainder 2 when divided by 4  $[2] = \{b \in \mathbf{Z} : b \equiv 2 \pmod{4}\} = \dots, -6, -2, 2, 6, 10, \dots$

Bucket 3: all integers that leave remainder 3 when divided by 4  $[3] = \{b \in \mathbf{Z} : b \equiv 3(\text{mod } 4)\} = \dots, -5, -1, 3, 7, 11, \dots$

These equivalence classes satisfy:  $\mathbf{Z} = [0] \cup [1] \cup [2] \cup [3]$  This quotient set is exactly the integers modulo 4

### 7.3 Partition

Let  $X$  be a set, and  $P(x)$  be the power set of  $X$ , meaning the set of all subsets of  $X$

$Y \subseteq P(X)$  means that  $Y$  is some collection of subsets of  $X$

A singular partition is the entire set of equivalence classes grouped together such that:

- every element of  $X$  is in exactly one class
- the classes don't overlap
- and together they cover all of  $X$

**Formal Definition:**  $Y$  is a partition of  $X$  if:

- **Pairwise Disjoint:** No two different subsets in  $Y$  overlap. Formally, if  $A, B \in Y$  and  $A \neq B$ , then  $A \cap B = \emptyset$
- **Union equals  $X$ :** All the subsets in  $Y$ , taken together, cover  $X$ . That is,  $\bigcup_{a \in Y} A = X$

## 8 Functions

### 8.1 Definition

**Definition:** A function  $f : X \rightarrow Y$  is a relation  $Gr(f) \subseteq X \times Y$  which satisfies the following condition: for all  $x \in X$ , there exists a unique  $y \in Y$  with  $(x, y) \in Gr(f)$

For  $x \in X$ , the unique element  $y \in Y$  such that  $(x, y) \in Gr(f)$  is denoted  $y = f(x)$  and called the *image* of  $x$  under  $f$

In english, a relation means you can pair elements denoted by  $(x, y)$  and collected into a set  $Gr(f) \subseteq X \times Y$ . A function holds of every input has some output, and the output is unique. **Informally**, a function is a rule that assigns to every element  $x \in X$  exactly one element  $y \in Y$

The set  $X$  is the domain while of  $f$  while  $Y$  is the range or codomain of  $f$ .  $Gr(f)$  is the graph of  $f$

### 8.2 Images

Let  $f : X \rightarrow Y$

The **image** of a set  $A$  under  $f$  is the set of all outputs of  $f$  when the input comes from  $A$

The **pre-image** of a set  $B$  is the set of all inputs that map into  $B$

**Pre-image of an element:** If we take a single element  $a \in X$ , then its image:  $f(a) \in Y$ . If we take a single element  $b \in Y$ , then its *pre-image* is:  $f^{-1}(\{b\}) = \{x \in X | f(x) = b\}$

The image of an element is a single point, while the pre-image of an element can be empty, one element, or many elements.



## 9 Function properties

### 9.1 Injective, Surjective, Bijective

**Injective:** A function is injective (one-to-one) if for every  $a, b \in X$  with  $a \neq b$  we have  $f(b) \neq f(a)$ . We can also say  $f$  is injective if  $\forall a, b \in X, f(a) = f(b)$  implies  $a = b$ . This means that *no two different inputs collapse to the same output*

**Surjective:** A function is surjective (onto) if for every  $c \in Y$  there exists some  $a \in X$  with  $f(a) = c$ . We can also say that  $\text{Im}(f) = Y$ . This means that *a surjective function has every element of its codomain  $Y$  “hit” by at least one input*

**Bijective:** A function which is both injective and surjective is called bijective

#### Geometric Test

$\alpha : \mathbf{R} \rightarrow \mathbf{R}$

If  $\alpha$  is injective, then every horizontal line intersects the graph of  $\alpha$  *at exactly* one point

If  $\alpha$  is surjective, then every horizontal line intersects the graph of  $\alpha$  at *at least* one point

#### Fixing surjectivity

**Example:** Let  $f : \mathbf{N} \rightarrow \mathbf{N}, f(n) = 2n + 1$

This function is not surjective, because for example,  $f(n) \neq 4$ . The  $\text{Im}(f)$  is just odd natural numbers  $\{1, 3, 5, \dots\}$

But, if we define  $f : \mathbf{R} \rightarrow \mathbf{R}$  instead, then the image of  $f$  can be achieved, thus the function is now surjective

### 9.2 Composition of Functions

Given  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$ , then  $(g \circ f)(x) = g(f(x))$  is  $X \rightarrow Z$

Note: composition is not commutative:  $g \circ f \neq f \circ g$ , but it is associative:  $h \circ (g \circ f) = (h \circ g) \circ f$

### 9.3 Identity function and inverses of functions

**Definition:** The identity function  $id_X(x) = x$  acts like “do nothing”, meaning if you compose it with any function, nothing changes

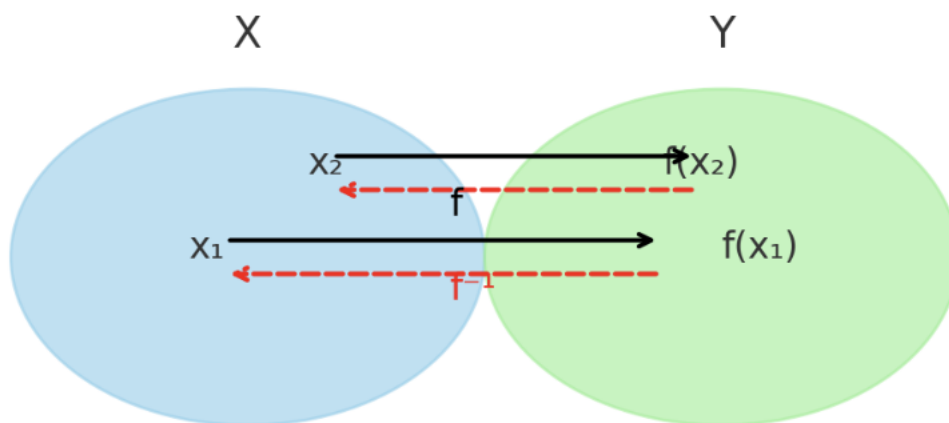
$$f \circ id_X = f = id_Y \circ f$$

**Definition:** The function  $g : Y \rightarrow X$  is the inverse of  $f : X \rightarrow Y$  if  $f \circ g = id_Y$  and  $g \circ f = id_X$ . Thus, *only bijective functions have inverses*.

## 10 Inverse of a Function

Let  $f : X \rightarrow Y$  and  $g : Y \rightarrow X$  are functions.  $g$  is a compositional inverse of  $f$  if both  $f \circ g = id_Y$  and  $g \circ f = id_X$

Function  $f: X \rightarrow Y$  and its Inverse  $f^{-1}: Y \rightarrow X$



If there is a composition inverse of  $f$ , then that compositional inverse is unique

**Example:** for the function  $f : \{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3, 4\}$ , its compositional inverse is given below:

If  $f(1) = 3$ , then  $f^{-1}(3) = 1$

### 10.1 Bijection-Invertibility Equivalence

Let  $f : S \rightarrow T$  be a function between sets  $S$  and  $T$ . Then  $f$  is a bijection **if and only if**  $f$  is invertible.

( $\Rightarrow$ ) if  $f$  is a bijection, then  $f$  is invertible

Suppose  $f$  is a bijection. Then:

- $f$  is **injective**: each element of  $T$  has *at most one* pre-image in  $S$ .
- $f$  is **surjective**: each element of  $T$  has *at least one* pre-image in  $S$ .

Together, this means **each**  $y \in T$  **has exactly one pre-image**  $x \in S$  such that  $f(x) = y$ .

Define  $g : T \rightarrow S$  by setting  $g(y) = x$ , where  $x$  is the unique element in  $S$  such that  $f(x) = y$ .

Now check compositions:

- For any  $y \in T$ :

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

so  $f \circ g = id_T$ .

- For any  $x \in S$ :

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

so  $g \circ f = id_S$ .

Thus  $g$  is the inverse of  $f$ , so  $f$  is invertible.

( $\Leftarrow$ ) if  $f$  is invertible, then  $f$  is a bijection

Suppose  $f$  is invertible. Then there exists  $g : T \rightarrow S$  such that:

$$g \circ f = id_S \quad \text{and} \quad f \circ g = id_T.$$

- **Injectivity:** If  $f(x_1) = f(x_2)$ , apply  $g$ :

$$g(f(x_1)) = g(f(x_2)) \Rightarrow x_1 = x_2.$$

Hence  $f$  is injective.

- **Surjectivity:** For any  $y \in T$ , we have  $y = (f \circ g)(y)$ . Let  $x = g(y)$ . Then  $f(x) = y$ . Thus every  $y \in T$  has a preimage in  $S$ .

Therefore  $f$  is bijective.

## 10.2 Cardinality

Two sets have the same cardinality (number of elements it contains) if there exists a bijection between the two sets. If two sets  $X$  and  $Y$  have the same cardinality, we write  $|X| = |Y|$

**Contrapositive:**

Let  $|A| = n, |B| = m, m \neq n$

If  $m < n$ , then at least one element  $\in B$  has no preimage, so not surjective. If  $m > n$ , then two elements  $\in A$  maps to one  $\in B$ , so not injective

## 11 Induction Principle

**Axiom of infinity** (define the natural numbers recursively):  $\forall A \subset \mathbb{N}, A \neq \emptyset, \exists a_0 \in A$  s.t.  $a \in A, a \geq a_0$

**Well-Ordering Principle:** Any non-empty set  $X \subseteq \mathbb{N}$  of natural numbers has a least element  $m \in X$  such that  $m \leq x$  for all  $x \in X$

In words, the set  $\mathbb{N}$  of natural numbers is the smallest set containing the integer 0 and the integer  $n + 1$  whenever  $n \in \mathbb{N}$

**Weak induction:** A proof by *mathematical induction* is a proof that covers the *base case*  $p(0)$  is true, and the *inductive case*  $p(n) \Rightarrow p(n + 1)$  for an arbitrary  $n \in \mathbb{N}$

Or, we can introduce an *arbitrary base*  $N$  where  $p(k) \Rightarrow p(k + 1)$  for an arbitrary integer  $k \geq N$

**Strong induction:** To prove a statement  $P(n)$  with a base case  $P(n_0)$  and assume *all previous cases*  $P(n_0), P(n_0 + 1), \dots, P(k)$  are all true to prove  $P(k + 1)$  is true

### 11.1 Proving the principle of mathematical induction using the well-ordering principle

Define:  $X = \{x \in \mathbb{N} : p(x) = F\}$ . If induction is correct, then  $X$  should be empty

Contradiction: suppose  $X \neq \emptyset$

Assume  $p(0)$  is true,  $0 \notin X$ , so  $m \geq 1$ . Then  $m - 1 \geq 0$ . Since  $m$  is the smallest counterexample,  $m - 1 \notin X$ , that means  $p(m - 1)$  is true

If  $p(m - 1)$  is true, then by induction,  $p(m)$  is true, but  $m \in X$  means  $p(m)$  is false, thus there is a contradiction

$\therefore X \neq \emptyset$  is wrong.  $X = \emptyset$  means  $p(n)$  is true for all  $n \geq 0$