MTHE 217 - Lecture Notes
Algebraic Structures with Applications

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

Contents

1   Division Algorithm

1.1   Division Algorithm

For any two integers n, d with $d \geq 1$, there exist unique integers q and r such that $n = qd + r$, with $0 \leq r < d$

Where: n is the dividend, d is the divisor, q is the quotient, r is the remainder

Proof:

Consider the set $R = \{n - ad : a \in \mathbb{Z}, n - ad \geq 0\}$

By the well-ordering principle, R has a smallest element r such that $r = n - qd$

The proof argues that $r < d$. By contradiction, we take $r \geq d$, then $r - d = n - qd - d = n - (q+1)d \geq 0$

Thus comparing $r - d$ and r, we get that $n - (q+1)d < n - qd \Rightarrow r - d < r$, but this contradicts that r was the smallest element in r, therefore $r < d$

For uniqueness, we supposed that there is another pair (q', r') such that $n = q'd + r'$ with $0 \leq r' < d$

By equating with n, we get that $r - r' = (q' - q)d$

By the division algorithm, d divides $r - r'$, but the latter is bounded between 0 and $d - 1$, because the largest r value bounded in between integers $[0, d]$ is $d - 1$. Thus, the largest value for $r - r'$ is $0 - (d - 1) = -(d - 1)$ and the smallest value is $(d - 1) - 0 = d - 1$

So, $r - r'$ ranges from $-(d - 1)$ to $d - 1$, or simply $-d < r - r' < d$, where the only multiple of d in that range is 0, thus $r = r'$ and $q = q'$, so they are unique

1.2   Greatest Common Divisor

The greatest common divisor $n, m \in \mathbb{Z}$ is the unique integer $gcd(n, m) \in \mathbb{N}$ The gcd of two integers is unique

Identities:

For $a, b, m \in \mathbb{Z}$, $gcd(am, bm) = m\,gcd(a, b)$ If $a, b, c \in \mathbb{Z}$ have $gcd(a, c) = 1$ and $c | ab$ then $c | b$ If $a, b \in \mathbb{Z}$ and p is prime then if $p | ab$ then $p | a$ or $p | b$

Bezout's Identity. For $n, m \in \mathbb{N}$, there exists $a, b \in \mathbb{Z}$ with $gcd(n, m) = an + bm$

If we take a smallest element $d \in W$ (set is $an + bm$), then we may write $d = sn + tm$ and $d = gcd(n, m)$ by its remainder $r = n - qd = n - q(sn + tm) = (1 - qs)n + qtm$

Thus, r is a linear combination of n and m and is smaller than d, thus r must be zero because d is the smallest positive linear combination.

Thus, $n = qd + 0 \Rightarrow d | n$ and $d | m$

2   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

2.1   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 conjuction 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 $p \to q$, 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	$p \to q$
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 $(p \to q) \wedge (q \to p)$

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

More Definitions

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

3   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:

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

Conclusion: $\neg r$

3.1   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. $s = p \wedge \neg p$)

3.2   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

3.3   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: $\neg(P \wedge \neg P) = T$

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

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* $P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P)$

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: $(P \to Q), P \therefore Q$, 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.

4   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 $S \to Q$ 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 $S \to Q$, 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, $S \to Q$ is T, and is a tautology

Backwards proof:

If $S \to Q$ 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 $S \Rightarrow Q$

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

4.1   Proof with multiple premises

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

We can prove $\neg b \to (p \leftrightarrow q) \wedge (r \to \neg b) \wedge (p \to \neg r) \Rightarrow \neg r$ 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:

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

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

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

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

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

4.2   Methods of proof

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

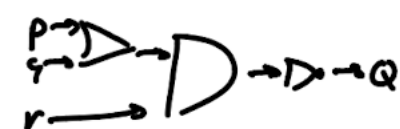## 4.3   Logic Gates

5 Set Theory

5.1 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 $\neg$):

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

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

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

5.2 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

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

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

6   Operations on Sets

Sets are unordered.

6.1   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 $X\Delta Y$, $= (X \cup Y)(X \cap Y)$ 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:

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

6.2   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 $A \cap B = A$

6.3   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 $X_1, \ldots, X_n$ are pairwise disjoint then $|X_1 \cup \cdots \cup X_n| = |X_1| + \cdots + |X_n|$

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

7   Equivalence Relations and Functions

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

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

7.2   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 $D = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$

7.3   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 $y \leq x$

7.4   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 $a, b \in Z$ are congruent modulo n and write $a \equiv b \bmod n$. Basically, n divides the difference in a and b. Or, $a - b$ is a multiple of n

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

Example 2: $9 \not\equiv 2 \bmod 3$ because $\frac{9-2}{3} \in \mathbf{Z}$

8 Equivalence class and congruence classes

8.1 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:

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

Symmetric:

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

Transitive:

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

8.2 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 collections of bins is called a partition of the LEGO set.

Congruence classes example

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

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 $[0] = \{b \in \mathbf{Z} : b \equiv 0 (\bmod 4)\} = \ldots, -8, -4, 0, 4, 8, \ldots$

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

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

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

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

8.3   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, $\bigcup_{a \in Y} A = X$

9   Functions

9.1   Definition

Definition: A function $f : X \to Y$ 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

9.2   Images

Let $f : X \to Y$

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.

10   Function properties

10.1   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

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

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

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

Fixing surjectivity

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

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 $f : \mathbf{R} \to \mathbf{R}$ instead, then the image of f can be achieved, thus the function is now surjective

10.2   Composition of Functions

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

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

10.3   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
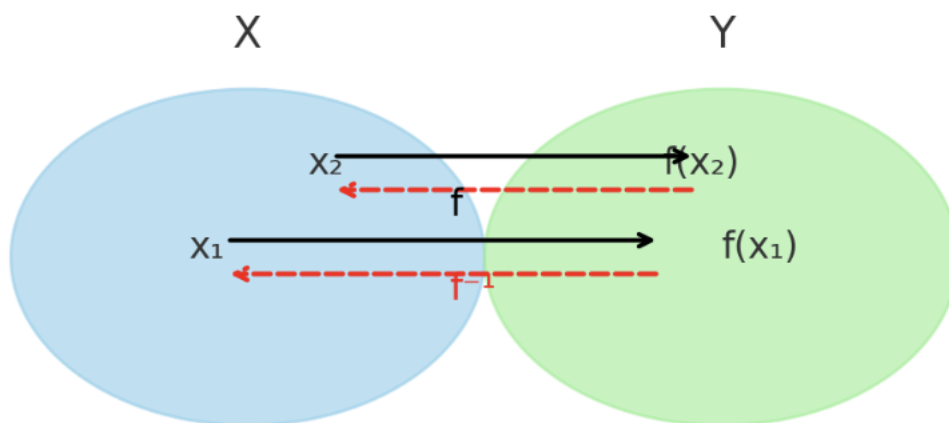
$f \circ id_X = f = id_Y \circ f$

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

11   Inverse of a Function

Let $f : X \to Y$ and $g : Y \to X$ 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 → Y and its Inverse f⁻¹: Y → X

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

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

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

11.1   Bijection-Invertibility Equivalence

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

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

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

$g \circ f = id_S \quad$ 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.

11.2   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

12   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* $P(n_0), P(n_0 + 1), \ldots, P(k)$ are all true to prove $P(k + 1)$ is true

12.1   Proof by Induction

Define the base case $n = n_0$, where n_0 is the smallest value for which you claim the statement holds

Write an *Inductive Hypothesis*: Assume $P(k)$ is true for $k \geq n_0$, where k is typically $\in \mathbb{Z}$

Inductive Step: Using the assumption from above, prove $P(k + 1)$ is true.

- Start with the LHS for $n = k + 1$, plug in what you know from the hypothesis (e.g. substitution expressions, add the next term to a series)

- Simplify, show clearly how the assumption leads to the next case

- At the end, ensure the result matches the original claimed formula/form for $n = k+1$

End with a *summary line*: By induction, $P(n)$ is true for all $n \geq n_0$

13   Factorization

a divides b, and we write $a|b$, if there exists an integer q with $b = qa$, and a is a divisor/factor of b

Lemma: If $a|(b+c)$, then $a|b$ and $a|c$ because $b + c = qa \Rightarrow c = qa - b \Rightarrow c = qa - ra = (q-r)a$

An integer $p > 1$ is prime if its only positive divisors are 1 and p. Otherwise, p is called **composite**

Theorem: every integer $n > 1$ can be written as a product of one or more primes

Induction base case: $n = 2$, since 2 is prime, the claim holds

Inductive hypothesis: Fix $k \geq 2$, and assume the claim holds for every integer m with $2 \leq m \leq k$

Inductive step: prove the claim for $n = k + 1$

If prime, we are done. If composite, then it can be written as a product of two integers a and b with $1 < a \leq b < k + 1$, in particular, $2 \leq a \leq k$ and $2 \leq b \leq k$

By the inductive hypothesis, a, b can be written as a product of primes. Multiplying those prime factorizations gives a prime factorization for $k + 1$

Theorem: Every positive integer can be expressed as a product of primes in a unique way, up to reordering the factors

Let $N = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$

p_1 divides N, so it must divide the right-hand product. If $p_1 = q_k$, then we can cancel that common prime and get $\frac{N}{p_1} = p_2 \ldots p_r = q_1 \ldots q_{k-1} q_{k+1} q_s$

But, $\frac{N}{p_1} < N$, so this smaller integer would have two distinct prime factorizations, contradicting the minimality of N, therefore $p_1 \neq$ any q_j

Thus, every integer > 1 has a prime factorization, and that factorization is unique up to ordering.

14   The Euclidean Algorithm

The Euclidean algorithm is an efficient algorithm for computing greatest common divisors.

By the lemma: If $n = qm + r$ for any integers then $gcd(n, m) = gcd(m, r)$, we have
$gcd(n, m) = gcd(m, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_{k-1}, r_k)$

The algorithm must terminate in at most $m + 1$ steps, as the last step $gcd(r_{k-1}, r_k)$ is where the gcd can be computed explicitly as r_k with remainder 0

Example: compute $gcd(100, 28)$

$$100 = 3(28) + 16$$
$$28 = 1(16) + 12$$
$$16 = 1(12) + 4$$
$$12 = 3(4) + 0$$

Now, find a, b such that $an + bm = gcd(100, 28)$

We can reverse the algorithm, for example take $16 = 1(12) + 4 \Rightarrow 4 = 16 - 1(12)$

$$16 = 1(12) + 4 \Rightarrow 4 = 16 - 1(12)$$
$$28 = 1(16) + 12 \Rightarrow= 16 - 1(28 - 1(16))$$
$$100 = 3(28) + 16 \Rightarrow= 2(100 - 3(28)) - 1(28) \Rightarrow= 2(100) - 7(28)$$

We can verify that the last term equals 4

15   Cheat Sheet

15.1   Propositional Logic

- Conditional: $p \rightarrow q$ (false only if $p = T$, $q = F$)

- Biconditional: $p \leftrightarrow q$ (iff)

- **Equivalences:**

  - Contrapositive: $(p \rightarrow q) \equiv (\neg q \rightarrow \neg p)$

  - De Morgan: $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$,
    $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$

  - Law of Excluded Middle: $p \vee \neg p = T$

Inference rules:
- Modus Ponens: $(p \rightarrow q)$, $p \Rightarrow q$
- Modus Tollens: $(p \rightarrow q)$, $\neg q \Rightarrow \neg p$

**Converse vs Contrapositive Statements

- Converse of $P \rightarrow Q$ is $Q \rightarrow P$. Simply switch the hypothesis and the conclusion of the original statement. This may change whether the statement is T/F

- Contrapositive to $P \rightarrow Q$ is $\neg Q \rightarrow \neg P$

15.2   Proof Techniques

General Strategy:

- restate in your own words

- list known facts

- clarity the goal

- look for patterns/theorems

- try examples, use concrete numbers or finite sets to test ideas

- break into sub-parts

- don't forget both sides of $\Leftrightarrow: \Rightarrow \wedge \Leftarrow$ and $=: \subset \wedge \supset$

- try to visualize (e.g. sets)

- **Direct Proof:** Show $P \rightarrow Q$.

- **Contrapositive:** Show $\neg Q \rightarrow \neg P$.

- **Contradiction:** Assume $\neg Q$ and derive a falsehood.

15.3   Set Theory

- **Common Sets:**
  $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Operations on Sets

- Union: $A \cup B = \{x : x \in A \vee x \in B\}$

- Intersection: $A \cap B = \{x : x \in A \wedge x \in B\}$

- Difference: $A \setminus B = \{x : x \in A \wedge x \notin B\}$

- Symmetric Difference: $A \Delta B = (A \setminus B) \cup (B \setminus A)$

- **Inclusion-Exclusion:**
  $|A \cup B| = |A| + |B| - |A \cap B|$

15.4   Relations

- **Cartesian Product:** $A \times B = \{(a, b) : a \in A, b \in B\}$

- **Relation:** $R \subseteq A \times B$

- **Equivalence Relation:** Reflexive, Symmetric, Transitive.

- **Partial Order:** Reflexive, Antisymmetric, Transitive.

- **Total Order:** Partial order + comparability $(\forall x, y : x \leq y \vee y \leq x)$.

15.5   Equivalence Classes

- Equivalence class of a: $[a] = \{x \in X : x \sim a\}$

- **Partition:** Disjoint classes covering X.

- **Congruence mod n:**
  $a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$

Example: $10 \equiv 2 \pmod{4}$

15.6   Functions

- Function $f : X \to Y$: $\forall x \in X, \exists! y \in Y$ with $f(x) = y$

- **Image:** $f(A) = \{f(x) : x \in A\}$

- **Preimage:** $f^{-1}(B) = \{x \in X : f(x) \in B\}$

- **Injective (1–1):** $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ no two inputs map to the same output

- **Surjective (onto):** $\forall y \in Y, \exists x \in X : f(x) = y$ every output is hit by some input $\Leftrightarrow \mathrm{Im}(f) = Y$

- **Bijective:** Both injective & surjective.

- **Identity:** $\mathrm{id}_X(x) = x$

- **Inverse:** f^{-1} exists $\Leftrightarrow f$ is bijective.

15.7 Inverses & Cardinality

- **Bijection $\Leftrightarrow$ Invertible.**

- If $|A| = n, |B| = m$:
    - If $m < n$: not surjective

    - If $m > n$: not injective

- **Equal cardinality:** $|X| = |Y| \Leftrightarrow \exists$ bijection $f : X \to Y$

15.8 Induction Principle

- **Well-Ordering Principle:** Every non-empty $X \subseteq \mathbb{N}$ has a least element.

- **Weak Induction:**
    1. Base Case: prove $P(0)$.

    2. Inductive Step: $P(n) \Rightarrow P(n+1)$.

- **Strong Induction:** Assume $P(k)$ true for all $k \leq n$, then prove $P(n+1)$.