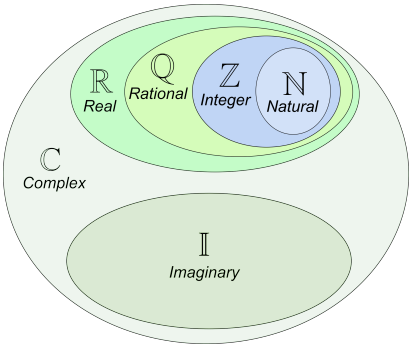
MATH 300 Notes

Contents

1 Terminology

1.1 Set Notations



- $\mathbb{Z}^+$: set of positive integers $1, 2, 3, ...$
- $\mathbb{Z}$: set of integers $0, 1, 2, -1, -2, ...$
- $\mathbb{N}$: set of natural numbers $0, 1, 2, ...$
- $\mathbb{Q}$: set of rational numbers $\frac{1}{2}, 1, 0, -\frac{3}{4}, ...$
- $\mathbb{R}$: set of real numbers π,$\sqrt{2}, e, 0, -1, 2, ...$

1.2 Connectives

$\wedge$	and	conjunction
$\vee$	or	disjunction
$\neg$	not	negation
$\oplus$	xor	
$\Rightarrow$	implication	
$\Leftrightarrow$	biconditional	

1.3 Quantifiers

$\forall$	for all / every
$\exists$	there exists
$\exists!$	there exists a unique

1.4 Additional Symbols

$\equiv$	equivalent

1.5 Implication

Given $P \Rightarrow Q$

- $Q \Rightarrow P \equiv \neg P \Rightarrow \neg Q$ is the inverse
- $P \wedge \neg Q$ is the negation
- $\neg Q \Rightarrow \neg P$ is the contrapositive, which is logically equivalent to $P \Rightarrow Q$

If $P \Rightarrow Q$ is true

- P is sufficient for Q
  - If P is true, then Q must be true
  - Knowing that P is true is *sufficient* to know that Q is true
- Q is necessary for P
  - Q must be true for P to be true
  - It is *necessary* for Q to be true for P to be true

1.6 Biconditional

Given $P \Leftrightarrow Q$

- $(P \wedge \neg Q) \vee (\neg P \wedge Q)$ is the negation
- $\neg P \Leftrightarrow \neg Q$ is the contrapositive, which is logically equivalent to $P \Leftrightarrow Q$

1.7 Logical Equivalences

- Equivalence is when two propositions have the same truth value
- Tautology is when a proposition is always true
- Contradiction is when a proposition is always false
- Contingency is when a proposition can either be true or false

1.8 Propositions

Propositions are statements that are either true or false

- Atomic propositions are simple statements
- Complicated propositions are built using atomic statements and joined together by connectives
- Usually denoted by statement variables $P, Q, R, ...$

1.9 Predicates

Predicates are open statements containing free variables

1.10 Axioms

Axioms are statements that are assumed to be true and do not require proofs

1.11 Inference

Inference is a set of related axioms that allows the deduction of new assertions or the determination of whether an assertion is true

1.12 Proofs

A rigorous argument that convinces an audience that a statement is either true or false

- Every statement in the proof is either an axiom or a statement inferred from the preceding axioms

1.13 Elementary Equivalences

- Identity

$$Q \wedge T \equiv Q$$
$$Q \vee F \equiv Q$$

- Domination

$$Q \vee T \equiv T$$
$$Q \wedge F \equiv F$$

- Idempotent

$$Q \vee Q \equiv Q$$
$$Q \wedge Q \equiv Q$$

- Commutative

$$Q \vee R \equiv R \vee Q$$
$$Q \wedge R \equiv R \wedge Q$$

- De Morgan's Laws

$$\neg(Q \wedge R) \equiv \neg Q \vee \neg R$$
$$\neg(Q \vee R) \equiv \neg Q \wedge \neg R$$

- Inverse De Morgan's Laws

$$Q \vee R \equiv \neg(\neg Q \wedge \neg R)$$
$$Q \wedge R \equiv \neg(\neg Q \vee \neg R)$$

- Associative

$$(Q \vee R) \vee S \equiv Q \vee (R \vee S)$$
$$(Q \wedge R) \wedge S \equiv Q \wedge (R \wedge S)$$

- Distributive

$$Q \wedge (R \vee S) \equiv (Q \wedge R) \vee (Q \wedge S)$$
$$Q \vee (R \wedge S) \equiv (Q \vee R) \wedge (Q \vee S)$$

- Absorption

$$Q \vee (Q \wedge R) \equiv Q$$
$$Q \wedge (Q \vee R) \equiv Q$$

- Negation

$$Q \vee \neg Q \equiv T$$
$$Q \wedge \neg Q \equiv F$$

- Double Negation

$$\neg(\neg Q) \equiv Q$$

- Law of Implication

$$Q \Rightarrow R \equiv \neg Q \vee R$$

- Law of Biconditional

$$Q \Leftrightarrow R \equiv (Q \Rightarrow R) \wedge (R \Rightarrow Q)$$

2 Proof Methods

2.1 Direct Method

Assume $P(x)$ is true and show that $Q(x)$ is true, that is prove $P(x) \Rightarrow Q(x)$

2.2 Contraposition

Assume $Q(x)$ is false and show that $P(x)$ is false, that is prove $\neg Q(x) \Rightarrow \neg P(x)$

2.3 Contradiction

To prove a statement S, assume S is false and show that a contradiction arises

2.4 Proof Formatting

Assume ..., that is ... for some ..., then ... therefore ...

2.5 Classic Induction

Classic induction is used to prove statements of the form $\forall n \geq n_0\ P(n)$ where we need to show that $P(n_0)$, $P(n_0+1)$, $P(n_0+2)$,... are true

1. Prove base case, that $P(n_0)$ is true
2. Prove induction step, that $P(k) \Rightarrow P(k+1)$ for any arbitrary k
3. If $P(k)$ is true, then the rules of implication state that $P(k+1)$ is also true

2.6 Strong Induction

Strong induction is used to prove statements of the form $\forall n \geq n_0\ P(n)$ where we need to show that $P(n_0)$, $P(n_0+1)$, $P(n_0+2)$,... are true

1. Prove base case, that $P(n_0)$ is true
2. Prove induction step, that $P(n_0) \wedge P(n_0+1) \wedge ... \wedge P(k) \Rightarrow P(k+1)$ for all $k \geq n_0$
3. If $P(n_0) \wedge P(n_0+1) \wedge ... \wedge P(k)$ is true, then the rules of implication state that $P(k+1)$ is also true

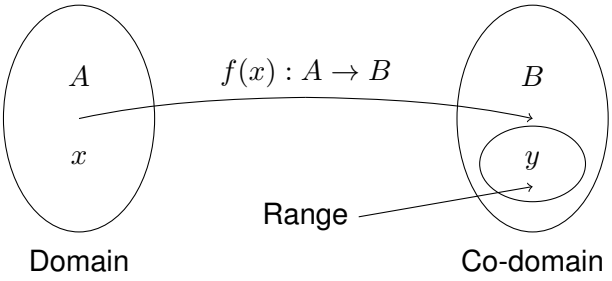
2.7 Modified Induction

Modified induction is used to prove statements of the form $\forall n \geq n_0\ P(n)$ where we need to show that $P(n_0)$, $P(n_0+1)$, $P(n_0+2)$,... are true

1. Prove base case, that $P(n_0)$ and $P(n_0+1)$ is true
2. Prove induction step, that $P(k-1) \wedge P(k) \Rightarrow P(k+1)$ for any arbitrary k
3. If $P(k-1) \wedge P(k)$ is true, then the rules of implication state that $P(k+1)$ is also true

3 Functions

3.1 Functions



A function $f : A \to B$ consists of:

1. A non-empty set A called the domain
    - Set of values that can enter the function
    - Also known as the pre-image
2. A non-empty set B called the co-domain
    - Set of values that can exit the function
    - Distinct from the range/image, which is the set of values that do exit the function
3. A rule that every element $x \in A$ maps onto an element $y \in B$

3.2 Identity Functions

Given $A \neq \varnothing$

$$Id_A : A \to A$$
$$Id_A(x) = x$$

3.3 Composition Functions

Given $f : A \to B$ and $g : B \to C$

$$g \circ f : A \to C$$
$$g(x) \circ f(x) : g(f(x))$$

3.4 Self Composing Functions

Given f is a function

$$f^2 : f \circ f$$
$$f^2(x) : f(f(x))$$

3.5 Restricted Functions

Given $f : A \to B$ and $S, S \subseteq A$

$$f_s : S \to B$$
$$f_s = f(x)$$

3.6 Inverse Functions

Given $f : A \to B$ the inverse of f is $f^{-1} : B \to A$

- $y = f(x) \Leftrightarrow f^{-1}(y) = x$
- A function f is invertible if and only if f is bijective

3.7 Well-Defined Functions

Given a function $f : A \to B$, f is well-defined if its image is unique, that is

$$\forall x_1, x_2 \in A,\ x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$$

3.8 Injective Functions

Given a function $f : A \to B$, f is injective if it is one-to-one, that is

$$\forall x_1, x_2 \in A,\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

3.9 Surjective Functions

Given a function $f : A \to B$, f is surjective if it is onto, that is

$$\forall y \in B,\ \exists x \in A,\ y = f(x)$$

3.10 Bijective Functions

Given a function $f : A \to B$, f is bijective if it is injective (one-to-one) and surjective (onto)

4 Set Theory

4.1 Sets

A set is a collection of distinct objects, such as $\{1, 2, 3\}$ and $\varnothing$

- A set has no repeated elements
- $\{1\}$ is distinct from $\{\{1\}\}$
  - 1 is an element of $\{1\}$ but not of $\{\{1\}\}$

4.2 Null Set

The null set $\varnothing$ is the set containing nothing, equivalent to $\{\}$

- The null set is a subset of every set
- The null set is not necessarily an element of a set
- $\varnothing$ is distinct from $\{\varnothing\}$

4.3 Subsets

A set A is a subset of a set B, $A \subseteq B$, if all elements of A are also elements of B

- $A \subseteq B$ if $\forall x,\ x \in A \Rightarrow x \in B$

4.4 Equivalent Sets

A set A is equivalent to B, $A = B$, if all elements of A are also elements of B and vice-versa

- $A = B$ if $\forall x,\ x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in A$

4.5 Complementary Sets

The complement of a set A^c is the set of all elements not in A

4.6 Sequential Set Operators

$$\bigcup_{i=1}^{n} A_i = \{x \mid \forall i, 1 \leq i \leq n \mid x \in A_i\} = A_1 \cup A_2 \cup ... \cup A_n$$

$$\bigcap_{i=1}^{n} A_i = \{x \mid \forall i, 1 \leq i \leq n \mid x \in A_i\} = A_1 \cap A_2 \cap ... \cap A_n$$

4.7 Power Sets

The power set of a set A is the set of all subsets of A, including the empty set and A itself

- $P(A) = \{S \mid S \subseteq A\}$
- $P(\varnothing) = \{\varnothing\}$
- $P(\{x, y\}) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$

Power set manipulation

- $\{x, y\} \in P(A) \equiv x, y \in A$
- $\{x, y\} \in P(A) \equiv \{x, y\} \subseteq A$

A set with n elements has 2^n power sets

4.8 Cartesian Products

The Cartesian product of two sets A and B is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

- The Cartesian product is not commutative, $(a, b) \neq (b, a)$

4.9 Cardinality

The cardinality of a set is a measure of a set's size, that is the number of elements in the set

- A set S with cardinality n can be expressed as $|S| = n$
- A set A has the same cardinality as B, $|A| = |B|$, if $f : A \to B$ is bijective
  - $f : A \to B$ is bijective $\Rightarrow |A| = |B|$
  - A and B are said to be equipotent
- A set A has a cardinality smaller than or equal to B, $|A| \leq |B|$, if $f : A \to B$ is injective
  - $f : A \to B$ is injective $\Rightarrow |A| \leq |B|$
- A set A has a cardinality greater than or equal to B, $|B| \leq |A|$, if $f : A \to B$ is surjective
  - $f : A \to B$ is surjective $\Rightarrow |B| \leq |A|$

4.10 Denumerable Sets

A set A is denumerable if it is equipotent to $\mathbb{Z}^+$, that is $f : \mathbb{Z}^+ \to A$ is bijective

4.11 Countable Sets

A set is countable if it is finite or denumerable

- Countably infinite sets are denumerable

5 Number Theory

5.1 Division Theorem

a divided by b

For $a \in \mathbb{Z},\ d \in \mathbb{Z}$ with $d > 0$:

There exists unique integers q, r with $0 \leq r < d$ such that $a = dq + r$

5.2 Modular Arithmetics

a is congruent to b modulo m

$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b)$

$a \equiv b \pmod{m} \Leftrightarrow (a - b) \equiv 0 \pmod{m}$

$a \equiv b \pmod{m} \Leftrightarrow a \pmod{m} = b \pmod{m}$

$a \equiv b \pmod{m} \ \wedge \ c \equiv d \pmod{m} \Rightarrow (a + c) \equiv (b + d) \pmod{m}$

$a \equiv b \pmod{m} \ \wedge \ c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$

$a \equiv b \pmod{m} \Leftrightarrow ak \equiv bk \pmod{mk}$ ← for some $k > 0$ and m, k coprime

$a \equiv b \pmod{m} \Leftrightarrow \frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{\gcd(k,m)}}$ ← for some $k = \text{factor}(a, b)$

$a \equiv b \pmod{m} \Leftrightarrow a + k \equiv b + k \pmod{m}$

$a \equiv b \pmod{m} \Leftrightarrow -a \equiv -b \pmod{m}$

5.3 Congruence Class of $a \bmod m$

The congruence class of $a \bmod m$, denoted $[a]_m$, is the set of all integers that are congruent to $a \bmod m$

- The set of all integers x where $a \bmod m = x \bmod m$
- There are m congruence classes in $\mathbb{Z}_m$, $[0]_m$ $[1]_m$ ... $[m-1]_m$
- $[a]_m + [b]_m = [a + b]_m$

5.4 Linear Diophantine Equations

Takes the form $ax + by = c$

- Has no solutions if $\gcd(a, b)$ does not divide c
- Has infinitely many solutions if $\gcd(a, b)$ divides c
- Given a solution where $x = x_0$, $y = y_0$, and $d = \gcd(a, b)$

$x = x_0 + \frac{b}{d}k$

$y = y_0 - \frac{a}{d}k$

5.5 Associated Linear Diophantine Equations

The associated equation of $ax \equiv b \bmod m$ is $ax + my = b$

- Can be used to solve for x
  - Has no solutions if $\gcd(a, m)$ does not divide b
  - Has infinite solutions if $\gcd(a, m)$ divides b
  - Has $\gcd(a, m)$ number of solutions in $\mathbb{Z}_m$

5.6 Euclidean Algorithm

$\gcd(a, b) = \gcd(b, a \,\%\, b)$
$\gcd(a, 0) = a$

Example:

$$\begin{aligned}\gcd(660, 126) &= \gcd(126, 660 \,\%\, 126) &&= \gcd(126, 30)\\ &= \gcd(30, 126 \,\%\, 30) &&= \gcd(30, 6)\\ &= \gcd(6, 30 \,\%\, 6) &&= \gcd(6, 0)\\ &= 6\end{aligned}$$

$$\begin{aligned}660 &= 5 * 126 + 30\\ 126 &= 4 * 30 + 6\\ 30 &= 5 * 6 + 0\end{aligned}$$

5.7 Bézout's Theorem

If a and b are positive integers:

Then there exists integers u and v such that $\gcd(a, b) = ua + vb$

Example (continuing 5.6):

$$\begin{aligned}126 &= 4 * 30 + 6\\ 6 &= 126 - 4 * 30\\ 660 &= 5 * 126 + 30\\ 30 &= 660 - 5 * 126\\ 6 &= 126 - 4 * (660 - 5 * 126)\\ 6 &= 126 - 4 * 660 + 20 * 126\\ 6 &= 21 * 126 - 4 * 660\end{aligned}$$

5.8 Modular Multiplicative Inverses

a is invertible in $\mathbb{Z}_m$ if and only if $ax \equiv 1 \bmod m$ has integer solutions

- a is invertible if and only if $\gcd(a, m) = 1$

5.9 Bijective Functions in $\mathbb{Z}_m$

Given $f : \mathbb{Z}_m \to \mathbb{Z}_m$, $f(x) = ax$, if $\gcd(a, m) = 1$ then f is a bijection

5.10 Distribution of Prime Numbers

Given $n \in \mathbb{N}$, there are $\pi(n) \approx \frac{n}{\ln(n)}$ number of primes less than n

5.11 Fermat's Little Theorem

Given p is prime

- if $\gcd(a, p) = 1$, then $a^p \equiv a \mod p \Leftrightarrow a^{p-1} \equiv 1 \mod p$ by cancellation law
- if $\gcd(a, p) \neq 1$, then $a^p \equiv a \equiv 0 \mod p$

5.12 Pseudoprimes

Given n is composite, if $a^n \equiv a \mod n$ or $a^{n-1} \equiv 1 \mod n$, then n is called a pseudoprime to the base a

5.13 Wilson's Theorem

Given p is prime, $(p-1)! \equiv -1 \mod p$

6 Equivalence Classes and Relations

6.1 Partitions

A partition of A is a family of disjoint subsets of A such that their union is A

6.2 Relations

A relation R from set A to set B is a subset of $A \times B$

- If $(a, b) \in R$, where R is a relation from some set A to some set B, we can write $a \ R \ b$
- A relation R on a set A is a subset of $A \times A$

6.3 Equivalence Relations

An equivalence relation is a relation that has the properties

- Reflexive: $\forall a \in A, \ a \ R \ a$
- Symmetric: $\forall a, b \in A, \ a \ R \ b \Leftrightarrow b \ R \ a$
- Transitive: $\forall a, b, c \in A, \ (a \ R \ b \wedge b \ R \ C) \Rightarrow a \ R \ c$

6.4 Equivalence Classes

Given an equivalence relation R on A and $a \in A$, the equivalence class of a is
$[a]_R = \{b \in A \mid a \ R \ b\}$