PPS Cheatsheet

Qianrui Li

May 11, 2023

1 Logic

Definitio 1.1 (Disjunction)**.** $A \vee B$ is true if either A or B is true.

Definitio 1.2 (Converse)**.** Converse to a conditional $A \implies B$ is $B \implies A$.

Definitio 1.3 (Contrapositive)**.** Contrapositive to a conditional $A \implies B$ is $\overline{B} \implies \bar{A}$.

2 Real Numbers

Definitio 2.1 (Field)**.** A field is a set F with two operations, addition and multiplication, such that

Addition

1. $a + b \in F$ for all $a, b \in F$.
2. $a + b = b + a$ for all $a, b \in F$.
3. $(a + b) + c = a + (b + c)$ for all $a, b, c \in F$.
4. There exists an element $0 \in F$ such that $a + 0 = a$ for all $a \in F$.
5. For each $a \in F$, there exists an element $-a \in F$ such that $a + (-a) = 0$.

Multiplication

1. $a \cdot b \in F$ for all $a, b \in F$.
2. $a \cdot b = b \cdot a$ for all $a, b \in F$.
3. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in F$.
4. There exists an element $1 \in F$ such that $a \cdot 1 = a$ for all $a \in F$.
5. For each $a \in F$, if $a \neq 0$, there exists an element $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$.

Distributive Law

1. $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

3 Inequality

Definitio 3.1 (Ordered Field)**.** An ordered field is a field F with a relation $<$ such that

1. Exactly one of is true: $a < 0$, $a = 0$, or $0 < a$
2. $b < a$ imples $-a < -b$.
3. If $a < b$, then $a + c < b + c$ for all $a, b, c \in F$.
4. $a > b$ and $b > 0$ implies that $ab > 0$.
5. If $a < b$ and $b < c$, then $a < c$ for all $a, b, c \in F$.

Theorema 3.1 (AM-GM Inequality)**.** *For any non-negative real numbers $a_1, a_2, \ldots, a_n$, we have*

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \ldots a_n} \tag{1}$$

Theorema 3.2 (Cauchy-Schwarz Inequality)**.** *For any real numbers $\boldsymbol{u} = [x_1, x_2, \ldots, x_n]$ and $\boldsymbol{v} = [y_1, y_2, \ldots, y_n]$, we have*

$$x_1y_1+x_2y_2+\cdots+x_ny_n \leq \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}\sqrt{y_1^2 + y_2^2 + \cdots + y_n^2} \implies \boldsymbol{u}\cdot\boldsymbol{v} \leq ||\boldsymbol{u}||||\boldsymbol{v}|| \tag{2}$$

Theorema 3.3 (Triangular Inequality)**.**

$$|x + y| \leq |x| + |y|; \qquad ||x| - |y|| \geq |x + y|$$

Theorema 3.4 (Formula for Geometric Series)**.** *For any real number x and integer $n \geq 0$, we have*

$$a + ax + ax^2 + \cdots + ax^n = \frac{a - x^{n+1}}{1 - x} \tag{3}$$

4 Completeness Axiom

Axioma 4.1 (Completeness of Real number)**.** Every nonempty set of real numbers that is bounded above has a least upper bound.

Definitio 4.1 (Monotone Sequence)**.** A sequence $(a_n)_{n=1}^{\infty}$ is increasing if $a_n \leq a_{n+1}$ for all $n \geq 1$. A sequence $(a_n)_{n=1}^{\infty}$ is decreasing if $a_n \geq a_{n+1}$ for all $n \geq 1$. A seqence is monotone if it is increasing or decreasing.

Theorema 4.1 (Monotone Convergence Theorem)**.** *A bounded above increasing sequence of real number converges; likewise a bounded below decreasing real sequence converges.*

Definitio 4.2 (Convergence of series (Partial Sum))**.** Given a sequence (a_j), the infinite series $\sum_{j=1}^{\infty} a_j$ converges to s if the sequence of partial sums

$$s_n = \sum_{j=1}^{n} a_j$$

converges as $n \to \infty$. If (s_n) converges we denote its limit by $\sum_{j=1}^{\infty} a_j$

Definitio 4.3 (Base of Natural Logarithm)**.**

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n \tag{4}$$

5 Polynomials

Definitio 5.1 (N-degree Complex Polynomial)**.** For $n \in \mathbb{N}$, an ***n-degree complex polynomial*** is a function of the form

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 \tag{5}$$

where $a_n \neq 0$ and $a_i \in \mathbb{C}$. A root of p is number α such that $p(\alpha) = 0$.

Theorema 5.1 (Root Coefficient Theorem)**.** *Let $p(z) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ have roots $r_1, r_2, \cdots r_n$, then*

$$r_1 + r_2 + \cdots + r_n = -a_{n-1}; \qquad r_1 r_2 \cdots r_n = (-1)^n a_0 \tag{6}$$

In general, let s_j denote the sum of all products of j-tuples of the roots (e.g., $s_2 = r_1 r_2 + r_1 r_3 + r_2 r_3 \cdots$), then

$$s_j = (-1)^j a_{n-j} \tag{7}$$

Theorema 5.2 (Fundamental Theorem of Arithmetic)**.** *Let $n \leq 2$ be an integer.*

Existance *n is equal to the product of prime number $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, where $p_1 < p_2 < \cdots < p_k$ and $r_i > 0$ for all i.*

Uniqueness *The factorisation is unique, i.e., if $q_1^{s_1} q_2^{s_2} \cdots q_l^{s_l} = n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ are "two" prime factorisations, then $k = l$ and $p_i = q_i$, $r_i = s_i$ for all i.*

6 Number Theory

Theorema 6.1. *Let $m \geq 2$ be a natural number, $\mathbb{Z}/m$ is a field if and only if m is a prime.*

Theorema 6.2 (Fermat's Little Theorem)**.** *Let p be a prime number, then for any integer a, if p does not divide a, we have*

$$a^{p-1} \equiv 1 \mod p \tag{8}$$

Theorema 6.3. *Let $n \in \mathbb{N}$ and p be a prime. If n and $p-1$ are coprime and p divides not b, the equation*

$$x^n \equiv b \mod p \tag{9}$$

has exactly one solution $x \in \{0, 1, \cdots, p-1\}$.

7 Relation and Function

Definitio 7.1 (Cartesian Product)**.** Let X and y be sets; their Cawrtesian Product is the set of ordered pairs

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

Definitio 7.2 (Injectivity and Surjectivity)**.** Let $f : X \to y$ be a function.

1. It is ***injective*** if and only if $f(a) = f(b) \implies a = b$

2. It is ***surjective*** if and only if for all $y \in Y$ we have $x \in X$ such that $f(x) = y$

3. It is ***bijective*** if and only if it is both injective and surjective.

Definitio 7.3 (Images and Preimages)**.** Let $f : X \to Y$ be a function. For $A \subseteq X$, the ***image*** of A

$$f(A) = \{f(x) : x \in A\} \subseteq Y$$

For $B \subseteq Y$, the ***preimage*** of B is

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

Definitio 7.4 (Cardinality)**.** Tow sets A, B have the same cardinality, (i.e., isomorphic) if there is a bijection $f : A \to B$. We write $|A|= |B|$ or $A \cong B$. If there is an injective map, we write $|A|\leq |B|$, and if $|A|\leq |B|$ and there is no injective map from B to A, we write $|A|< |B|$.

When $|A|\leq \mathbb{N}$, we say A is countable.

Definitio 7.5. Let $S = \{a_1, a_2, \cdots, a_n\}$ be a set of n distinct objects. An ordering (or arrangement) of S is a sequence $(a_1, \cdots, a_n$ in which each element of S appears exactly once.

Theorema 7.1. *For* $n \geq 0$*,*

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

Definitio 7.6. Given $n \in \mathbb{N}, k \in \mathbb{N}$, with $k \geq 2$ and non-negative integers $r_1, r_2, \cdots r_k$ such that $r_1 + \cdots r_k = n$, we denote the number of ordered partitions $(A_1, \cdots, A_k)$ of set S such that $|A_i|= r_i$ by

$$\binom{n}{r_1, r_2, \cdots, r_k} = \frac{n!}{r_1!\, r_2! \cdots r_k!}$$

8 Permutaion

Definitio 8.1. Given $n \in \mathbb{N}$, denote by S_n the set of all bijections $\{1, 2, 3, 4, \cdots, n\} \to \{1, 2, 3, \cdots, 4\}$. We call S_n permutation of the set $\{1, 2, 3, \cdots, n\}$. (Which is also called the symmetric group of degree n)