情報数学 チートシート

情報数学は、情報工学・計算機科学で必要となる数学の基礎や、数学的に物事を扱う考え方を学ぶことを目的としています。連続的でなく離散的なもの、無限でなく有限なものを対象とする「離散数学」と密接に関連しています。

---

1. 論理 (Logic)

重要公式:

- **真理値表 (Truth Table):** 命題の真偽を示す表
  - 否定: $\neg p$
  - 論理積 (連言): $p \land q$
  - 論理和 (選言): $p \lor q$
  - 排他的論理和: $p \oplus q$
  - 含意: $p \to q$
  - 同値: $p \leftrightarrow q$
- **論理結合子の優先順位:** [高] $\neg, \land, \lor, (\oplus, \to, \leftrightarrow)$ [低]
- **命題の等価性（重要な恒真式）**:
  - 交換則: $p \land q \equiv q \land p$, $p \lor q \equiv q \lor p$
  - 結合則: $p \land (q \land r) \equiv (p \land q) \land r$, $p \lor (q \lor r) \equiv (p \lor q) \land (p \lor r)$
  - 分配則: $p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$, $p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$
  - べき等則: $p \lor p \equiv p$, $p \land p \equiv p$
  - 吸収則: $p \land (p \lor q) \equiv p$, $p \lor (p \land q) \equiv p$
  - 単位則: $\top \land p \equiv p$, $\bot \lor p \equiv p$
  - 支配則: $\bot \land p \equiv \bot$, $\top \lor p \equiv \top$
  - 二重否定則: $\neg(\neg p) \equiv p$
  - 矛盾則: $p \land \neg p \equiv \bot$
  - 排中則: $p \lor \neg p \equiv \top$
  - **ド・モルガンの法則:** $\neg(p \lor q) \equiv \neg p \land \neg q$, $\neg(p \land q) \equiv \neg p \lor \neg q$
  - **含意の規則:** $p \to q \equiv \neg p \lor q$
  - **対偶則:** $(p \to q) \equiv (\neg q \to \neg p)$
  - **同値の規則:** $(p \leftrightarrow q) \equiv (p \to q) \land (q \to p)$
- **限定子を含む否定**:
  - $\neg \forall x P(x) \leftrightarrow \exists x \neg P(x)$
  - $\neg \exists x P(x) \leftrightarrow \forall x \neg P(x)$
  - 全称限定子・存在限定子の交換則: $\forall x \forall y P(x, y) \leftrightarrow \forall y \forall x P(x, y)$, $\exists x \exists y P(x, y) \leftrightarrow \exists y \exists x P(x, y)$

基本用語:

- **命題 (Proposition):** 「真(true)」または「偽(false)」のいずれか一方に定まる文。
-
  - **命題関数 (Propositional Function) / 述語 (Predicate):** 変数を含む文で、変数を代入すると命題になるもの。* **述語 (Predicate):** 変数を含む文で、変数を代入すると命題になるもの。
- **限定子 (Quantifier):** 述語がどの範囲で真となるかを表す表現 (全称限定子 ∀、存在限定子 ∃)。

---

2. 集合 (Sets)

重要公式:

- **集合の包含・等価関係の論理式表現:**
- **部分集合:** $A \subseteq B \iff \forall x(x \in A \to x \in B)$
- **集合が等しい:** $A = B \iff (A \subseteq B) \wedge (B \subseteq A) \iff \forall x(x \in A \leftrightarrow x \in B)$
- **差集合:** $A - B = x \mid x \in A \wedge x \notin B$
- **和集合の濃度（包除原理）:** $|A \cup B| = |A| + |B| - |A \cap B|$ (有限集合の場合)
- **ド・モルガンの法則:** $\overline{A \cup B} = \bar{A} \cap \bar{B}$, $\overline{A \cap B} = \bar{A} \cup \bar{B}$

基本用語:

- **集合 (Set):** 対象物の集まり。
- **空集合 (Empty Set):** 要素を持たない集合 (記号: $\emptyset$ または)。
- **全体集合 (Universal Set):** 議論の対象となるすべての要素を含む集合 (記号: U)。
- **部分集合 (Subset):** 集合Aの任意の要素が集合Bの要素であるとき、AはBの部分集合である ($A \subseteq B$)。
- **べき集合 (Power Set):** 集合Sの全ての部分集合の集合 (記号: $\mathcal{P}(S)$ または 2^S)。$|S| = n$ のとき $|\mathcal{P}(S)| = 2^n$。
- **直積 (Cartesian Product):** 集合AとBの全ての順序対(a, b)の集合 (記号: $A \times B = (a, b) \mid a \in A \wedge b \in B$)。
- **和集合 (Union):** AまたはBの要素を含む集合 (記号: $A \cup B = x \mid x \in A \vee x \in B$)。
- **共通部分 (Intersection):** AとBいずれにも含まれる要素からなる集合 (記号: $A \cap B = x \mid x \in A \wedge x \in B$)。
- **差集合 (Difference):** Aには含まれるがBには含まれない要素からなる集合 (記号: $A - B = x \mid x \in A \wedge x \notin B$)。
- **補集合 (Complement):** 全体集合Uに対する集合Aの補集合 (記号: $\bar{A}$ または A^c, $A^c = U - A$)。

---

3. 関数 (Functions)

重要公式・定義:

- **関数であることの定義:** $\forall x \in A, \exists! y \in B(y = f(x))$
- **単射 (Injection) の定義:** $\forall x_1, x_2 \in A(f(x_1) = f(x_2) \to x_1 = x_2)$
- **全射 (Surjection) の定義:** $\forall y \in B, \exists x \in A(y = f(x))$
- **全単射 (Bijection):** 単射かつ全射であること。逆関数が存在するための必要十分条件。
- **関数の合成:** 関数 $g : A \to B$ と $f : B \to C$ に対して、合成関数 $(f \circ g)(a) = f(g(a))$。
- **逆関数:** $f : A \to B$ が全単射ならば逆関数 $f^{-1} : B \to A$ が存在する ($f(a) = b \implies f^{-1}(b) = a$)。

基本用語:

- **関数 (Function) / 写像 (Mapping):** 定義域の各要素に終集合の要素をちょうど1つ割り当てるもの。
- **定義域 (Domain):** 関数fの入力となる集合A。
- **終集合 (Codomain):** 関数fの出力が含まれる集合B。
- **値域 (Range):** fによる定義域の全ての要素の像の集合。

- **単射 (Injection) / 1対1関数:** 定義域の異なる要素が終集合の異なる要素に写像される関数。
- **全射 (Surjection) / 上への関数:** 終集合の全ての要素が定義域のいずれかの要素の像である関数。
- **全単射 (Bijection) / 1対1対応:** 単射かつ全射である関数。

---

4. 数学的証明法と再帰 (Mathematical Proof Methods and Recursion)

重要公式:

- **推論規則 (Rules of Inference):** (例として一部抜粋)
  - 構成的三段論法 (Modus Ponens): $p, p \to q \implies q$
  - 破壊的三段論法 (Modus Tollens): $\neg q, p \to q \implies \neg p$
  - 仮言三段論法 (Hypothetical Syllogism): $p \to q, q \to r \implies p \to r$

基本用語:

- **直接法 (Direct Proof):** p を真と仮定し、q が真であることを証明する ($p \to q$)。
- **対偶法 (Proof by Contraposition):** $\neg q$ を真と仮定し、$\neg p$ が真であることを証明する ($\neg q \to \neg p$)。
- **背理法 (Proof by Contradiction):** p を真と仮定し、矛盾を導くことでpが偽であることを示す。
- **数学的帰納法 (Mathematical Induction):** ある命題 $P(n)$ がすべての正の整数 n で真であることを証明する方法 (基底段階と帰納段階)。
- **再帰的定義 (Recursive Definition):** 対象を定義するために、それ自身を用いて定義すること。
  - **関数の再帰的定義:** 初期ステップと再帰ステップで関数値を定義。
  - **集合の再帰的定義:** 初期ステップで基本要素を指定し、再帰ステップで既知の要素から新しい要素を定義。

---

5. 関係 (Relations)

重要公式:

- **2項関係の性質の定義:**
  - **反射的 (Reflexive):** $\forall x \in A((x, x) \in R)$
  - **対称的 (Symmetric):** $\forall x, y \in A((x, y) \in R \to (y, x) \in R)$
  - **反対称的 (Anti-symmetric):** $\forall x, y \in A((x, y) \in R \wedge (y, x) \in R \to x = y)$
  - **推移的 (Transitive):** $\forall x, y, z \in A((x, y) \in R \wedge (y, z) \in R \to (x, z) \in R)$

基本用語:

- **2項関係 (Binary Relation):** 順序対の集合。
- **同値関係 (Equivalence Relation):** 反射的、対称的、推移的である関係。
- **同値類 (Equivalence Class):** 同値関係Rにおいて、aと同値関係にある要素の集合 $[a] = b \in A | aRb$。
- **商集合 (Quotient Set):** 集合Aと同値関係Rに対し、Rに関する同値類の集合 $A/R = [a] | a \in A$。
- **半順序関係 (Partial Order Relation):** 反射的、反対称的、推移的である関係。
- **半順序集合 (Partially Ordered Set / Poset):** 半順序関係が定義された集合。
  - **例:** べき集合 $\mathcal{P}(S)$ と包含関係 $\subseteq$ の組 $(\mathcal{P}(S), \subseteq)$ は半順序集合である。
- **ハッセ図 (Hasse Diagram):** 有限半順序集合を図示する方法。反射的・推移的な矢印は省略する。
- **最大元/最小元:** 集合内の他のどの元よりも大きい/小さい元。存在すれば一意。
- **極大元/極小元:** それより大きい/小さい元が集合内に存在しない元。複数存在しうる。

- **上界/下界:** ある部分集合の全ての元以上/以下の元。
- **上限(sup)/下限(inf):** 上界の集合の最小元 / 下界の集合の最大元。
- **関係の閉包 (Closure of a Relation):**
    - 関係Rに特定の性質を持たせるために、Rに追加する必要がある**最小の**順序対の集合を含む関係。
    - **反射閉包:** Rに、Rに含まれていない対角線上の順序対 (x, x) をすべて追加して得られる関係。
    - **推移閉包:** Rに、推移律を満たすために必要な順序対 (x, z) をすべて追加して得られる関係。Warshallアルゴリズムなどで計算できる。

---

6. 代数 (Algebra)

重要公式:

- **演算の性質:**
    - 結合則 (Associative Law): $\forall x, y, z \in A(x \circ (y \circ z) = (x \circ y) \circ z)$
    - 交換則 (Commutative Law): $\forall x, y \in A(x \circ y = y \circ x)$
- **束の性質 (代数として):** (上記結合則、交換則に加えて)
    - べき等則: $a \vee a = a$, $a \wedge a = a$
    - 吸収則: $(a \vee b) \wedge b = b$, $(a \wedge b) \vee b = b$
- **分配律 (Distributive Law):**
    - $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
    - $a \wedge (b \vee c) = (a \wedge b) \vee (a \vee c)$
- **ブール束の性質 (ブール代数):**
    - 単位元: $a \vee 0 = a$, $a \wedge 1 = a$
    - 補元: $a \vee \bar{a} = 1$, $a \wedge \bar{a} = 0$
    - ド・モルガンの法則: $\overline{a \vee b} = \bar{a} \wedge \bar{b}$, $\overline{a \wedge b} = \bar{a} \vee \bar{b}$
- **準同型写像の定義:** $f : A \to B$ が $f(x \circ y) = f(x) * f(y)$ を満たす。

主要アルゴリズム: なし

基本用語:

- **2項演算 (Binary Operation):** 集合Aの2つの元に対し、Aの1つの元を与えるもの。
- **閉じている (Closed):** 集合Aの任意の2つの要素に対する演算の結果が、必ずその集合Aの要素になること。
- **単位元 (Identity Element):** $e \in A$ で、$\forall x \in A(e \circ x = x \circ e = x)$ を満たすもの。
- **逆元 (Inverse Element):** 単位元 e がある代数において、$x \circ y = y \circ x = e$ を満たす y を x の逆元という。
- **半群 (Semigroup):** 結合法則を満たす代数。
- **モノイド (Monoid):** 結合法則を満たし、単位元をもつ代数。
- **群 (Group):** 結合法則を満たし、単位元を持ち、すべての元が逆元をもつ代数。
- **可換群 (Abelian Group):** 交換則も満たす群。
- **分配束 (Distributive Lattice):** 束の性質に加えて分配則を満たす束。
- **ブール束 (Boolean Lattice) / ブール代数 (Boolean Algebra):** 相補的な分配束。
- **準同型写像 (Homomorphism):** 2つの代数間で演算を保存する関数。
- **同型写像 (Isomorphism):** 全単射な準同型写像。