離散数学及び演習
（Discrete Mathematics）

工学部専門系科目　（専門基礎科目）

電気電子・情報工学科
Bクラス
2014年度前期

離散数学クラス分け

- 別途掲示で指定されたクラスで受講すること.
  - 指定以外のクラスでの受講は認めない.
- 間違いなく受講申請すること.

- 3年次編入者・2013年度以前入学の再履修者
  - 学籍番号の学科内番号部分（08-1Z-3-XXX-Y）を3で割り,
    - 割り切れる場合：　Aクラス
    - 1余る場合　：　Bクラス
    - 2余る場合　：　Cクラス

離散数学及び演習
第 1 回　　2014. 4.17（木）

講義概要
集合・集合演算
（教科書　pp.1-3, 5-9）

教科書・・・野崎昭弘：離散系の数学、近代科学社

講義の内容

- 離散的対象の性質や離散的対象の間に存在する関係についての議論
- 離散的対象の表現手法（解析・設計手法）

  - 集合論（set theory）
  - 整数論（number theory）
  - 代数系（algebraic system）

講義の目的

- 離散的対象に関する知識の習得
- 様々な分野に対する基礎的知識の習得
  - 理論計算機科学，ソフトウェア基礎論など
- 概念を客観的かつ論理的に表現，論証するための手法・技術の習得
  - 数学のための日本語表現
    - 記号の使い方
    - 論理的表現・言い回し
      - 「任意の…」，「ある…」，「一意的」
      - 「かつ」，「または」，「…であるとき，かつそのときに限り，…」，etc.
  - 論証技術
    - 証明の記述＝論理的思考の洗練
    - 数学の体系的記述
      - 定義，定理，補題，系，証明

講義・演習予定

週	月日	講義		演習	
1	4/17	1	講義の概要，集合・集合演算	1	集合・集合演算
2	4/24	2	直積・関係，2項関係の性質	2	直積・関係
3	5/ 1	3	同値関係，半順序	3	2項関係の性質
4	5/ 8	4	束	4	同値関係
5	5/15	5	関数	5	半順序
6	5/22		（講義なし）	6 7	束 関数
7	5/29	 6	中間試験（範囲：講義1～5） 約数・倍数		（演習なし）
8	6/ 5	7	素数	8	約数・倍数
9	6/12	8 9	1次不定方程式，合同式 合同式（続き）		（演習なし）
10	6/19		（講義なし）	9 10	素数，1次不定方程式 合同式
11	6/26	10	多項式，環	11	多項式，環
12	7/ 3	11	環（続き），群	12	環（続き），群
13	7/10	12 13	部分系，準同型 商系		（演習なし）
14	7/17		（講義なし）	13 14	部分系，準同型 商系
15	7/24 ??	期末試験（範囲：講義1～13）			

講義の進め方

- 原則として1時限目
- 教科書
  - 野崎昭弘：離散系の数学，近代科学社（1980）．
  - 事前に該当部分を読んでおくこと
- 講義資料
  - PowerPoint 使用
  - http://www.kl.i.is.nagoya-u.ac.jp/~toyama/lecture/risan14/
    - pdf 版をダウンロード可能
- 参考書
  - 佐藤文広：数学ビギナーズマニュアル［第2版］，日本評論社（2014）．
  - 結城浩：数学文章作法 基礎編，筑摩書房（2013）．

  - リュー（成嶋・秋山訳）：コンピュータサイエンスのための離散数学入門，オーム社（1986）．
  - 小倉久和：情報の基礎離散数学，近代科学社（1999）．
  - 楫元：工科系のための初等整数論入門，培風館（2000）．
  - 新妻弘・木村哲三：群・環・体入門，共立出版（1999）．

演習の進め方

- 原則として2時限目
- 教室
  - 143教室　…　1年（B−1クラス），2年，4年
  - 144教室　…　1年（B−2クラス），3年

- 小テスト
  - 前回演習の内容（解答用紙は次回返却）
- 問題解答
  - 指定された問題を解答
  - 解答を板書・解説
  - 解答用紙を提出（次回返却）
  - 指定外の問題は自学自習
- 演習問題解答例
  - http://www.kl.i.is.nagoya-u.ac.jp/~toyama/lecture/risan14/
    - pdf 版をダウンロード可能

成績評価

- 中間試験　——　約30%
- 期末試験　——　約40%
- 小テスト
- 演習解答
- 演習板書

（小テスト・演習解答・演習板書）　約30%

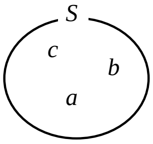
- 評価区分
  - 2011年度以降入学者
    S：100〜90，A：89〜 80，B：79〜70，C：69〜60，F：59〜0
  - 2010年度以前入学者
    優：100〜80，良：79〜70，可：69〜60，不可：59〜0
  - 期末試験を欠席した場合は，「欠席」とする．

- 不合格の場合
  - 来年度も同じクラスで受講

集合論
（set theory）

集合（set）

- 集合
  - （素朴な定義）　相異なる対象の集まり



Venn 図

- 対象　…　要素，元（element）
- 対象 a は集合 S の要素である
  （対象 a は集合 S に属する）　…　$a \in S$
- 対象 a は集合 S の要素でない
  （対象 a は集合 S に属さない）　…　$a \notin S$

例：
- 要素 a, b, c からなる集合　…　$\{ a, b, c \}$
- すべての自然数からなる集合　…　$\{ 1, 2, 3, \ldots \}$

集合（続き）

- 集合は相異なる要素のみを含む
  例：$\{ a, a, b, c \} = \{ a, b, c \}$
- 集合の要素を並べる順序は問わない
  例：$\{ b, c, a \} = \{ a, b, c \}$

文字の使い方（原則）：
- 集合　…　大文字　（$A, B, C, S, R, T, \ldots$）
- 要素　…　小文字　（$a, b, c, x, y, z, \ldots$）

集合の要素を記述する方法

- すべての要素を列挙する
  例：$S=\{2, 4, 6, 8, \ldots\}$
- すべての要素を一意的に特徴付ける性質を述べる
  例：$S=\{x \mid x$ は正の偶数$\}$
- すべての要素を生成する 1 組の規則を述べる
  例：$\begin{cases} 2 \in S, \\ x \in S \text{ ならば, } x+2 \in S, \\ (S \text{ は他の要素を含まない}). \end{cases}$

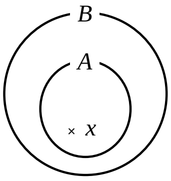
集合の要素数

- 空集合（empty set）　ϕ（$=\{\ \}$）
  - 要素をひとつも含まない集合
- 有限集合（finite set）
  - 要素が有限個である集合
  - 有限集合 A の要素数　…　A の大きさ（size）　$|A|$
  例：　$|\{a, b, c\}|=3$
  $|\phi|=0$
- 無限集合（infinite set）
  - 要素が無限個である集合

部分集合（subset）

- 集合 A は集合 B の部分集合である　（$A \subseteq B$）
  集合 A は集合 B に含まれる
  - 任意の $x \in A$ に対して，$x \in B$ である

例：　$A=\{b, 2\}$，$B=\{y, 2, b, 3, a\}$
$A \subseteq B$
- $b \in B$, $2 \in B$



例：　$\{x \mid x$ は正の偶数$\} \subseteq \{1, 2, 3, \ldots\}$

定理

集合 A, B, C に対して，次の（1）～（3）が成り立つ．

（1）　$A \subseteq A$

（2）　$\phi \subseteq A$

（3）　$A \subseteq B$,　$B \subseteq C$ ならば，$A \subseteq C$

等しい集合

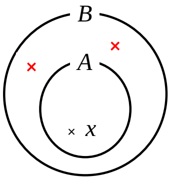
- 集合 A と集合 B は等しい（equal）（$A=B$）
  - $A \subseteq B$ かつ $B \subseteq A$
  - 任意の $x \in A$ に対して $x \in B$，
    かつ，
    任意の $x \in B$ に対して $x \in A$

例：　$\{x \mid x$ は正の偶数$\}=\{2, 4, 6, \ldots\}$
- $\{x \mid x$ は正の偶数$\} \subseteq \{2, 4, 6, \ldots\}$
  かつ
  $\{2, 4, 6, \ldots\} \subseteq \{x \mid x$ は正の偶数$\}$

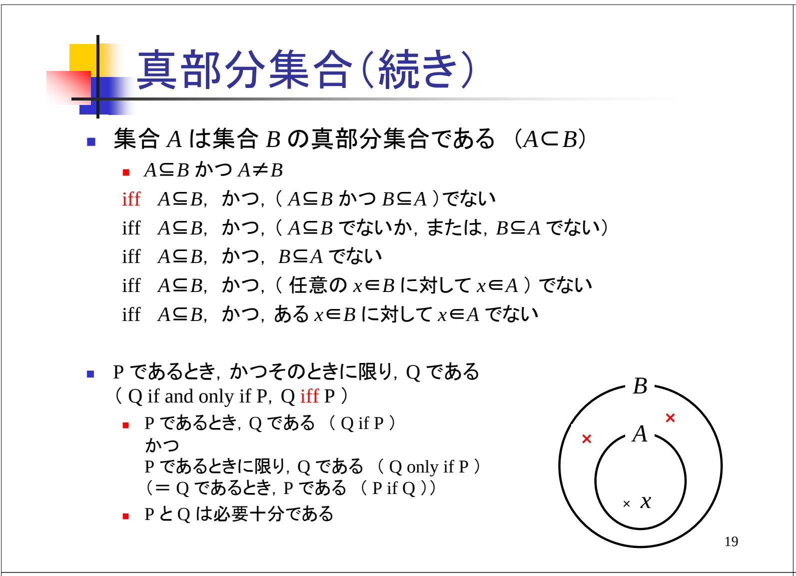
真部分集合（proper subset）

- 集合 A は集合 B の真部分集合である　（$A \subset B$）
  - $A \subseteq B$ かつ $A \neq B$

例：　$A=\{b, 2\}$，$B=\{y, 2, b, 3, a\}$
$A \subset B$
- $A \subseteq B$
- $y \in B$, $y \notin A$



例：　$\{x \mid x$ は正の偶数$\} \subset \{1, 2, 3, \ldots\}$



真部分集合（続き）

- 集合 A は集合 B の真部分集合である （$A \subset B$）
  - $A \subseteq B$ かつ $A \neq B$

  iff　$A \subseteq B$，かつ，（$A \subseteq B$ かつ $B \subseteq A$）でない

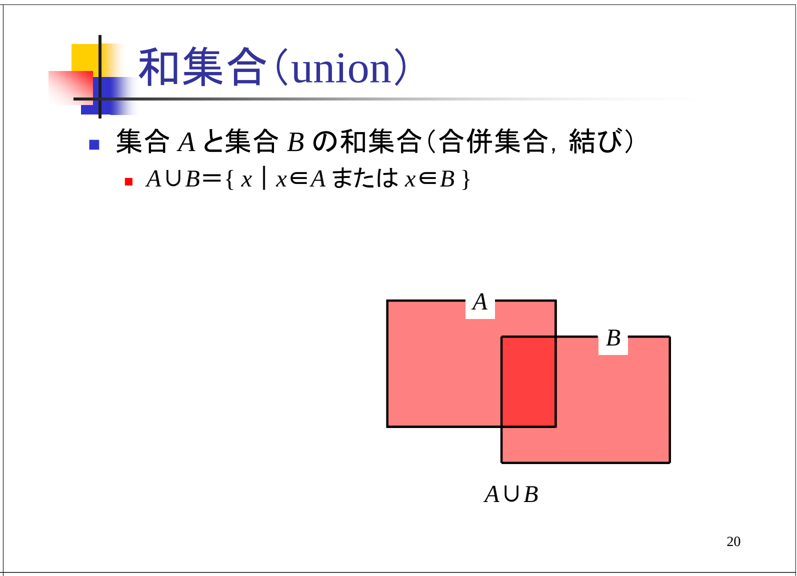
  iff　$A \subseteq B$，かつ，（$A \subseteq B$ でないか，または，$B \subseteq A$ でない）

  iff　$A \subseteq B$，かつ，$B \subseteq A$ でない

  iff　$A \subseteq B$，かつ，（任意の $x \in B$ に対して $x \in A$）でない

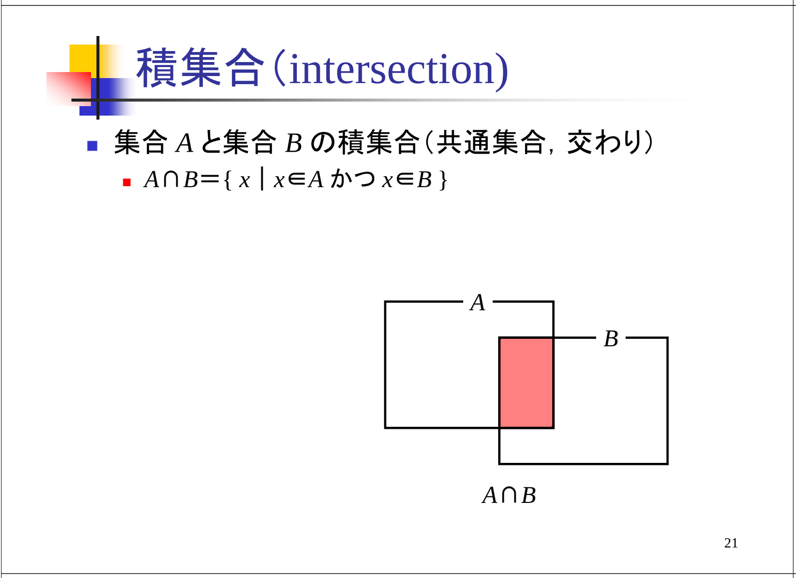
  iff　$A \subseteq B$，かつ，ある $x \in B$ に対して $x \in A$ でない

- P であるとき，かつそのときに限り，Q である
  （Q if and only if P，Q iff P）
  - P であるとき，Q である （Q if P）
    かつ
    P であるときに限り，Q である （Q only if P）
    （＝Q であるとき，P である （P if Q））
  - P と Q は必要十分である



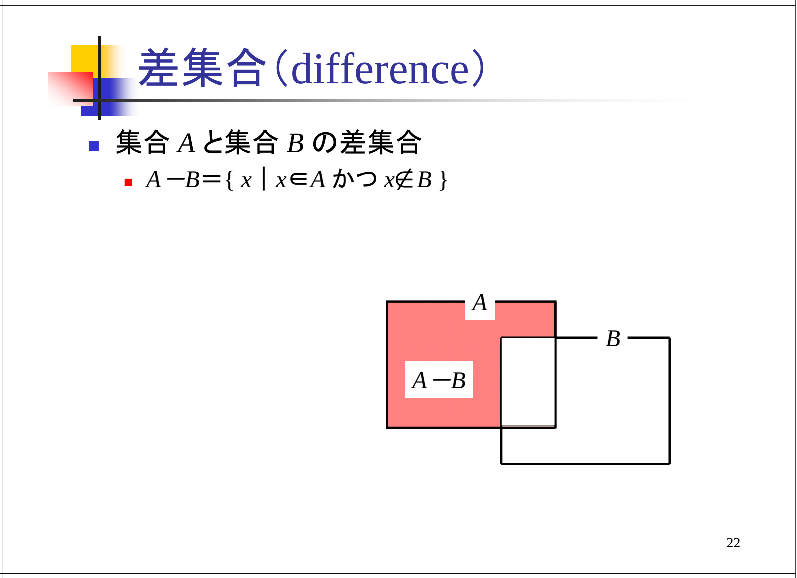
和集合（union）

- 集合 A と集合 B の和集合（合併集合，結び）
  - $A \cup B = \{ x \mid x \in A$ または $x \in B \}$



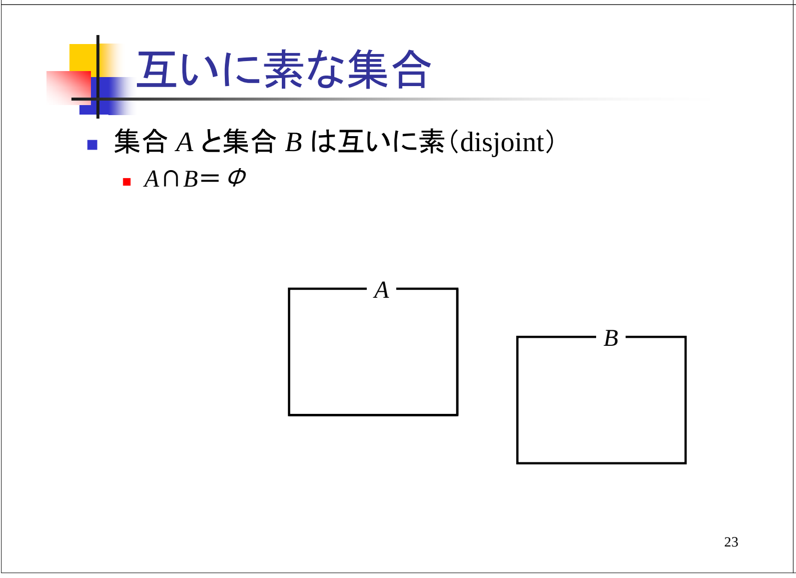
積集合（intersection）

- 集合 A と集合 B の積集合（共通集合，交わり）
  - $A \cap B = \{ x \mid x \in A$ かつ $x \in B \}$



差集合（difference）

- 集合 A と集合 B の差集合
  - $A - B = \{ x \mid x \in A$ かつ $x \notin B \}$



互いに素な集合

- 集合 A と集合 B は互いに素（disjoint）
  - $A \cap B = \emptyset$

定理

集合 A，B，C に対して，次の（1）～（6）が成り立つ．

（1）　$A \subseteq A \cup B$.

（2）　$A \subseteq C$，$B \subseteq C$ ならば，$A \cup B \subseteq C$.

（3）　$A \cup B = B$であるとき，かつそのときに限り，$A \subseteq B$.

（4）　$A \cap B \subseteq A$.

（5）　$C \subseteq A$，$C \subseteq B$ ならば，$C \subseteq A \cap B$.

（6）　$A \cap B = A$であるとき，かつそのときに限り，$A \subseteq B$.

- P であるとき，かつそのときに限り，Q である（Q if and only if P，Q iff P）
  - P であるとき，Q である （Q if P）
    かつ
    P であるときに限り，Q である （Q only if P）
    （＝Q であるとき，P である （P if Q））
  - P と Q は必要十分である

証明

（1）　$A \subseteq A \cup B$

- 「任意の $x \in A$ に対して，$x \in A \cup B$」を示す．

任意の $x \in A$ に対して，$x \in A$ または $x \in B$ だから
$x \in A \cup B$.
ゆえに，$A \subseteq A \cup B$.

証明

（2）　$A \subseteq C$，$B \subseteq C$ ならば，$A \cup B \subseteq C$

- $A \subseteq C$，$B \subseteq C$ を仮定して，$A \cup B \subseteq C$ を示す．
  - 「任意の $x \in A \cup B$ に対して，$x \in C$」を示す．

$A \subseteq C$，$B \subseteq C$ とする．
任意の $x \in A \cup B$ に対して，$x \in A$ または $x \in B$.
$x \in A$ のとき，$A \subseteq C$ だから，$x \in C$.
$x \in B$ のとき，$B \subseteq C$ だから，$x \in C$.
いずれの場合も $x \in C$.
ゆえに，$A \cup B \subseteq C$.

証明

（3）　$A \cup B = B$であるとき，かつそのときに限り，$A \subseteq B$

- a）「$A \cup B = B$ ならば $A \subseteq B$」と
- b）「$A \subseteq B$ ならば $A \cup B = B$」の両方を示す．
- a）　$A \cup B = B$ を仮定して，$A \subseteq B$ を示す．
  - 「任意の $x \in A$ に対して，$x \in B$」を示す．

a）$A \cup B = B$ とする．
　任意の $x \in A$ に対して，（1）$A \subseteq A \cup B$から，$x \in A \cup B = B$.
　ゆえに，$A \subseteq B$.

証明（続き）

（3）　$A \cup B = B$であるとき，かつそのときに限り，$A \subseteq B$

- a）「$A \cup B = B$ ならば $A \subseteq B$」と
- b）「$A \subseteq B$ ならば $A \cup B = B$」の両方を示す．
- b）　$A \subseteq B$ を仮定して，$A \cup B = B$ を示す．
  - 「 $A \cup B \subseteq B$ 」かつ「 $B \subseteq A \cup B$ 」を示す．
    - b-1)「任意の $x \in A \cup B$ に対して，$x \in B$ 」を示す．

b）$A \subseteq B$ とする．
b-1）任意の $x \in A \cup B$ に対して，$x \in A$ または $x \in B$.
　　$A \subseteq B$ だから，$x \in A$ のときも $x \in B$.
　　ゆえに，$A \cup B \subseteq B$.
b-2）（1）から，$B \subseteq A \cup B$.
したがって，$A \cup B = B$.

定理

集合 A，B，C に対して，次の（1）～（5）が成り立つ．

（1）　$A \cup A \subseteq A$,
　　　$A \cap A \subseteq A$
　　　　　　　　冪（べき）等則（idempotent law）

（2）　$A \cup B = B \cup A$,
　　　$A \cap B = B \cap A$
　　　　　　　　交換則（commutative law）

（3）　$(A \cup B) \cup C = A \cup (B \cup C)$,
　　　$(A \cap B) \cap C = A \cap (B \cap C)$
　　　　　　　　結合則（associative law）

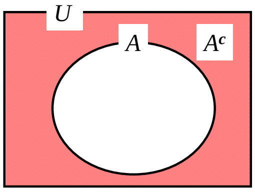
定理（続き）

（4）　$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$,
　　　$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
　　　　　　　　分配則（distributive law）

（5）　$A \cap (A \cup B) = A$,
　　　$A \cup (A \cap B) = A$
　　　　　　　　吸収則（absorptive law）

全体集合･補集合

- 全体集合（universe）　U
  - すべての対象からなる集合
- 集合 A（$\subseteq U$）の補集合（complement）
  - $A^c = U - A$



定理

集合 A, B に対して，次の（1）～（5）が成り立つ.

（1）　$A \cup A^c = U$,

　　　$A \cap A^c = \phi$

（2）　$A \subseteq B$ ならば，$B^c \subseteq A^c$.

（3）　$A - B = A \cap B^c$.

（4）　$U^c = \phi$,

　　　$\phi^c = U$.

（5）　$(A^c)^c = A$.

定理（de Morgan の法則）

集合 A, B に対して，次の（1），（2）が成り立つ.

（1）　$(A \cup B)^c = A^c \cap B^c$

（2）　$(A \cap B)^c = A^c \cup B^c$

A. de Morgan
（英，1806-1871）

証明

（1）　$(A \cup B)^c = A^c \cap B^c$

- a）「$(A \cup B)^c \subseteq A^c \cap B^c$」と
- b）「$A^c \cap B^c \subseteq (A \cup B)^c$」の両方を示す.
- a）「任意の $x \in (A \cup B)^c$ に対して，$x \in A^c \cap B^c$」を示す.
- b）「任意の $x \in A^c \cap B^c$ に対して，$x \in (A \cup B)^c$」を示す.

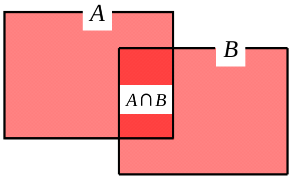
---

a）　任意の $x \in (A \cup B)^c$ に対して，$x \notin A \cup B$.
　$x \notin A$ かつ $x \notin B$ だから，$x \in A^c$ かつ $x \in B^c$.
　ゆえに，$x \in A^c \cap B^c$.
　したがって，$(A \cup B)^c \subseteq A^c \cap B^c$.
b）　任意の $x \in A^c \cap B^c$ に対して，$x \in A^c$ かつ $x \in B^c$.
　$x \notin A$ かつ $x \notin B$ だから，$x \notin A \cup B$.
　ゆえに，$x \in (A \cup B)^c$.
　したがって，$A^c \cap B^c \subseteq (A \cup B)^c$.

定理（包除原理）

有限集合 A, B に対して，

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



$A \cup B$

集合を要素とする集合

- 集合は相異なる対象（要素）の集まり
  - 要素が集合である場合も考えられる

例：　$S = \{ x, 2, \{ 1, x, a \} \}$
　　　$= \{ x, 2, T \}$　　　　　（$T = \{ 1, x, a \}$）

- $|S| = 3$

例：　$A = \{ a, b, c \}$
　　　$B = \{ a, b, c, \{ a, b, c \} \}$
　　　$= \{ a, b, c, A \}$

- $|B| = 4$
- $A \in B$
- $A \subseteq B$

集合を要素とする集合（続き）

- ϕ（＝{ }）
  - 空集合　… 要素をひとつも含まない集合 （$|\phi|=0$）
- {ϕ}　（＝{ { } }）
  - 空集合を唯一の要素とする集合
    … 要素を1つだけ含む集合 （$|\{\phi\}|=1$）
- $\phi\neq\{\phi\}$
- 集合のクラス（集合族（family））
  - 要素が集合である集合

冪（べき）集合（power set）

- 集合 A の冪集合
  - $\boldsymbol{P}(A)=\mathbf{2}^{A}=\{S \mid S\subseteq A\}$
  - A のすべての部分集合を要素とする集合

例：　$A=\{1, 2, 3\}$

$\boldsymbol{P}(A)$

$=\{\phi,$

$\{1\}, \{2\}, \{3\},$

$\{1, 2\}, \{1, 3\}, \{2, 3\},$

$\{1, 2, 3\}\}$

定理

有限集合 A に対して，

$|\boldsymbol{P}(A)|=|\mathbf{2}^{A}|=2^{|A|}$

例：　$A=\{1, 2, 3\}$

$\boldsymbol{P}(A)=\{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\},$
$\{2, 3\}, \{1, 2, 3\}\}$

$|\boldsymbol{P}(A)|=8$

$2^{|A|}=2^{3}=8$

まとめ

- 今回の講義
  - 集合
  - 集合演算
- 次回の講義
  - 直積・関係，2 項関係の性質（教科書　pp.9-12）
- 今回の演習
  - 集合・集合演算