『離散構造』 2章 (集合)
演習問題の (解説まじりの) 解答
亀山

問題 1 (集合の表現)

以下の集合を $\{x \in A \mid P(x)\}$ の形で記述せよ．(ただし，A は集合, $P(x)$ は命題である．)

(a) 約数を 3 つ以上もつ自然数の集合.

「m が n の約数である」ことを $D(m,n)$ と書くことにする．(注. 普通の数学の本では $m|n$ と書くが, 縦棒は，集合の定義で使いたいので，ここでは使わないことにする．)

すると,「x が y_1 と y_2 と y_3 を約数にもつ」という命題は,

$$D(y_1,x) \wedge D(y_2,x) \wedge D(y_3,x)$$

と書けそうであるが，これは間違いである．なぜなら，たとえば，$x=3$ に対しても (3 は当然ながら, 約数は 2 個しか持たない)，$y_1=y_2=y_3=3$ と取ると，$D(y_1,x) \wedge D(y_2,x) \wedge D(y_3,x)$ は成立してしまう．従って，以下のようにする必要がある．

$$D(y_1,x) \wedge D(y_2,x) \wedge D(y_3,x) \wedge y_1 \neq y_2 \wedge y_2 \neq y_3 \wedge y_3 \neq y_1$$

次に,「x が約数を 3 つ (以上) もつ」ということは,「x が**ある** y_1 と y_2 と y_3 に対して，それらを約数にもつ」ということなので,

$$\exists y_1.\exists y_2.\exists y_3.\ (D(y_1,x) \wedge D(y_2,x) \wedge D(y_3,x) \wedge y_1 \neq y_2 \wedge y_2 \neq y_3 \wedge y_3 \neq y_1)$$

となる．

これを用いて，求める集合は以下の通りである．

$$\{x \in \mathcal{N} \mid \exists y_1.\exists y_2.\exists y_3.(D(y_1,x) \wedge D(y_2,x) \wedge D(y_3,x) \wedge y_1 \neq y_2 \wedge y_2 \neq y_3 \wedge y_3 \neq y_1)\}$$

なお，集合 $\{x \in A \mid \exists y.P\}$ を記述するとき，右側の $\exists y.$ を省略しても良いという約束事により，以下のように書いてもよい.

$$\{x \in \mathcal{N} \mid D(y_1,x) \wedge D(y_2,x) \wedge D(y_3,x) \wedge y_1 \neq y_2 \wedge y_2 \neq y_3 \wedge y_3 \neq y_1\}$$

[補足] 上記のものが用意した解答であったが，演習で思いがけない解答があった.

$$\{x \in \mathcal{N} \mid \neg\mathrm{Prime}(x) \wedge x \neq 1\}$$

ここで $\mathrm{Prime}(x)$ は「x が素数である」ことを意味する。たしかに、1 でも素数でもない自然数は、すべて、約数を 3 個以上もつ. 素晴しい!

(b) 約数がちょうど 3 つである自然数の集合.

前問と同様にすれば,「約数がちょうど 4 つである自然数の集合」は以下のように書ける.

$$\{x \in \mathcal{N} \mid D(y_1, x) \wedge D(y_2, x) \wedge D(y_3, x) \wedge$$
$$y_1 \neq y_2 \wedge y_1 \neq y_3 \wedge y_1 \neq y_4$$
$$\wedge\, y_2 \neq y_3 \wedge y_2 \neq y_4 \wedge y_3 \neq y_4\}$$

もしくは，$\forall$ を使うと以下のように書ける．

$$\{x \in \mathcal{N} \mid D(y_1, x) \wedge D(y_2, x) \wedge D(y_3, x) \wedge D(y_4, x) \wedge \forall i.\forall j.(i \neq j \Rightarrow y_i \neq y_j)\}$$

そこで，前問の集合を A_3 とし，この集合 (どちらの表記でもよい) を A_4 とすると，求める集合は，$A_3 - A_4$ となる．

[補足] 上記のものが用意した解答であったが，演習で思いがけない解答があった．(またか‥)

$$\{x^2 \mid x \in \mathcal{N} \wedge x > 1\}$$

この集合を丁寧に書くと，$\{y \in \mathcal{N} \mid \exists x \in \mathcal{N}.\ (x = y^2 \wedge x > 1)\}$ となる．つまり，ある自然数の 2 乗の形になる自然数 (ただし 1 を除く) の集合ということである．たしかに,「約数をちょうど 3 つ持つ自然数」は必ずこういう形をしているので，これでも正解である．なるほど!

(c) 整数を係数とする 2 次方程式の根 (解) となる実数の集合.

$$\{x \in \mathcal{R} \mid ax^2 + bx + c = 0 \wedge a \in \mathcal{N} \wedge b \in \mathcal{N} \wedge c \in \mathcal{N} \wedge a \neq 0\}$$

「2 次方程式」という場合，通常,「1 次」以下の方程式は含まないので，$a \neq 0$ という条件を追加した．

[補足] もちろん、根の公式を用いて、x を具体的に a, b, c の式で表現してもよいが、ここではその必要はない。

問題 2 (集合の演算)

集合 $A = \{1, 2, 3\}$,$B = \{1, 3, 5\}$, $C = \{2, 3, 6\}$ に対して，以下の集合を計算して，それらが等しいかどうか求めよ．

(以下の解答では，等しいものを明示した．明示されていないものは等しくない．)

(a) $A - B = A - (A \cap B) = \{2\}$.
$A - (A \cup B) = \{\}$. (空集合)

(b) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C) = \{2, 3\}$.
$(A \cap C) \cup B = \{1, 2, 3, 5\}$.

(c) $2^{A-B} = \{\{\}, \{2\}\}$.
$2^A - 2^B = \{\{2\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$.

(d) $A \times B = \{\langle 1, 1\rangle, \langle 1, 3\rangle, \langle 1, 5\rangle, \langle 2, 1\rangle, \langle 2, 3\rangle, \langle 2, 5\rangle, \langle 3, 1\rangle, \langle 3, 3\rangle, \langle 3, 5\rangle\}$.
$\{\} \times (A \times B)$,
$B \times A = \{\langle 1, 1\rangle, \langle 3, 1\rangle, \langle 5, 1\rangle, \langle 1, 2\rangle, \langle 3, 2\rangle, \langle 5, 2\rangle, \langle 1, 3\rangle, \langle 3, 3\rangle, \langle 5, 3\rangle\}$.

問題 3 (有限集合の要素数)

A が有限集合のとき，$\#A$ は A の要素数をあらわす．このとき，$\#(2^A) = 2^{\#A}$ が成立する理由を述べよ．

ここでは、2 つの理由付けを行う。皆さんはどちらが好みであろうか。

1. 情報科学らしい理由: A の要素が n 個のとき、$A = \{a_1, \ldots, a_n\}$ の形である。ここで n ビットの数 (2 進法で n けたの数) と、A の部分集合の間の以下のような対応付けを考える。(以下の例は $n = 5$ のときである。

$$
\begin{array}{lcl}
00000 & \Leftrightarrow & \{\} \\
10010 & \Leftrightarrow & \{a_1\} \\
10101 & \Leftrightarrow & \{a_1, a_3, a_5\} \\
01111 & \Leftrightarrow & \{a_2, a_3, a_4, a_5\}
\end{array}
$$

この対応付けにより、すべての n ビットの数 (n けたの 2 進数) と、A の部分集合が 1 対 1 に対応することがわかるだろう。(あらゆる n ビットの数に A の部分集合 1 つが対応する。異なる n ビット数には、異なる部分集合が対応する。)

したがって、2^A の要素の数は、n ビットの数の総数である。これは明らかに 2^n である。すなわち、$\#(2^A) = 2^{\#A}$ である。

2. 数学的な理由: A の要素数 n に関する数学的帰納法を使う。

$n = 0$ のとき、A は空集合なので、$2^A = \{\{\}\}$ であり、たしかに成立する。

$n = k + 1$ のとき、A から要素を 1 つ除いた集合を B とする。このとき $A = B \cup \{a\}$ という形に書ける。ただし、$a \notin B$.

さて、B は要素数が k なので、帰納法の仮定により、$\#(2^B) = 2^{\#B} = 2^k$ である。

さて、B の部分集合は、そのままで、A の部分集合である。また、B の部分集合に、それぞれ a を追加した集合も、A の部分集合である。さらに、これらの部分集合たちは、互いに相異なる。その上、A の部分集合は、これらで全てである。

以上から、$\#(2^A) = 2^k + 2^k = 2^{k+1}$ となり、$n = k + 1$ のときも、与えられた命題が成立する。

以上より、数学的帰納法により、任意の n に対して与えられた命題は成立する。(証明終わり)

補足: 数学的帰納法については、まだ離散構造の授業ではとりあつかっていないので、「数学的な理由」の方は理解できなくてよい。6 章「帰納」において詳しく勉強する。

問題 4 (集合に関する推論)

集合 A, B, C に対して，以下の命題が成立することをそれぞれ証明せよ．

(a) $(A \cup B) - C \subset (A - C) \cup (B - C)$ の証明.

$x \in (A \cup B) - C$ を満たす任意の x を取る．

すると，$(x \in (A \cup B)) \wedge (x \notin C)$ である．

これを，書き換えると，$((x \in A) \vee (x \in B)) \wedge (x \notin C)$ である．

この命題は，$((x \in A) \wedge (x \notin C)) \vee ((x \in B) \wedge (x \notin C))$ と同値である．(命題 $(X \vee Y) \wedge Z$ と命題 $(X \wedge Z) \vee (Y \wedge Z)$ が同値であることは，真理値表を使って証明できる．)

従って，$(x \in A - C) \vee (x \in B - C)$ である．

よって，$x \in (A - C) \cup (B - C)$ である．

結局，$x \in (A \cup B) - C$ を満たす任意の x を取ると，$x \in (A - C) \cup (B - C)$ であることが示せたので，$((A \cup B) - C) \subset ((A - C) \cup (B - C))$ である．(証明終わり).

(b) $(A \cup B) - C \supset (A - C) \cup (B - C)$.

(本問は，基本的に前問と同じことを逆方向にたどれば解けるが，練習のため，逐一証明する．)

$x \in (A - C) \cup (B - C)$ を満たす任意の x を取る．

すると，$(x \in (A - C)) \vee (x \in (B - C))$ である．

よって，$((x \in A) \wedge (x \notin C)) \vee ((x \in B) \wedge (x \notin C))$ である．

これは，$((x \in A) \vee (x \in B)) \wedge (x \notin C)$ と同値である．

よって，$(x \in (A \cup B)) \wedge (x \notin C)$ である．

よって，$x \in (A \cup B) - C$ である．

結局，$x \in (A - C) \cup (B - C)$ を満たす任意の x を取ると，$x \in (A \cup B) - C$ であることが示せたので，$((A \cup B) - C) \supset ((A - C) \cup (B - C))$ である．(証明終わり).

問題 5 (発展課題; 興味がある人のみ)

「すべての x に対して，$x \in R \Leftrightarrow x \notin x$」を満たす集合 R が存在すると仮定して，以下の 2 つを導きなさい．

(a) $R \in R$ ならば，$R \notin R$ である．したがって，矛盾する．

「すべての x に対して，$x \in R \Leftrightarrow x \notin x$」であるので，この x として R を取ると，$R \in R \Leftrightarrow R \notin R$ となるので,「$R \in R$ ならば $R \notin R$」が成立する．

ところで，$R \in R$ と $R \notin R$ は矛盾するので結局，$R \in R$ ならば矛盾する．

(b) $R \notin R$ ならば，$R \in R$ である．したがって，矛盾する．

上と同様に，$R \in R \Leftrightarrow R \notin R$ ということから，$R \notin R$ ならば，$R \in R$ となる．

再び，$R \in R$ と $R \notin R$ は矛盾するので結局，$R \notin R$ ならば矛盾する．

以上のように，$R \in R$ の場合も $R \notin R$ の場合も矛盾する．

これは，最初の仮定がまずかったせいであり，このような集合 R は存在しない．なお，R の定義を，内包的定義に似せて書くと，

$$R = \{x \mid x \notin x\}$$

となるが，このような形の集合定義を許してしまうと矛盾する，ということである．(テキストに記載した，集合の定義は，$\{x \in A \mid P(x)\}$ の形であり，あらかじめ集合とわかっている A から，新しい集合を構成する方法であった．)

上記の R を Russell set と呼び，このような形で矛盾で生じることを「Russell Paradox (ラッセルの逆理)」と呼ぶ．(実際には，集合ではないとわかったので set と呼ぶのはおかしいが，当時は集合と思われていた．)
詳細は，集合論の文献を参考にしてほしい．