離散数学演習１　解答例

1. (1) 任意の $x \in A$ に対して，$x \in B$.
   (2) $A \subseteq B$ かつ $B \subseteq A$.
   (3) $A \subseteq B$ かつ $A \neq B$.
   (4) $\{x \mid x \in A$ または $x \in B\}$
   (5) $\{x \mid x \in A$ かつ $x \in B\}$
   (6) $\{x \mid x \in A$ かつ $x \notin B\}$
   (7) $A \cap B = \phi$.
   (8) $U - A$
   (9) $\{S \mid S \subseteq A\}$
2. (1) 正.
   (2) 誤.
   (3) 誤.
   (4) 正.
   (5) 誤.
   (6) 正. B のすべての要素は a, b であり, $a, b \in A$.
   (7) 正. D のすべての要素は b, c であり, $b, c \in A$ だから, $D \subseteq A$. しかし, $a \in A$ に対して, $a \notin D$ だから, $D \neq A$.
   (8) 誤. $a \in A$ に対して, $a \notin C$.
   (9) 誤. $c \in D$ に対して, $c \notin E$.
   (10) 正.
   (11) 誤. $a \in E$ に対して, $a \notin F$.
   (12) 正
   (13) 誤. $a \in B$ に対して, $a \notin G$.
   (14) 正. $\{B\}$ のすべての要素は $B = \{a, b\}$ であり, $B \in G$.
   (15) 誤. $b \in D$ に対して, $b \notin G$.
   (16) 誤. $D = \{b, c\} \in \{D\}$ に対して, $D \notin G$.
   (17) 誤. $\{a, b\} \in G$ に対して, $\{a, b\} \notin A$.
   (18) 正. $\{\{c\}\}$ のすべての要素は $\{c\}$ であり, $\{c\} \in E$.
3. (1) 正.
   (2) 誤. $\{S\}$ の要素は S である.
   (3) 正. $\{S\}$ のすべての要素は S であり, $S \in \{S\}$.
   (4) $\{\{S\}\}$
4. A: (1) $\{x \mid x$ は正の 5 の倍数 $\}$
   (2)
   - $5 \in A$.
   - $x \in A$ ならば $x + 5 \in A$.
   - A は他の要素を含まない.

   B: (1) $\{x \mid x$ は 1 の位が 7 である自然数 $\}$
   (2)
   - $7 \in B$.
   - $x \in B$ ならば $x + 10 \in B$.
   - B は他の要素を含まない.

   C: (1) $\{x \mid x$ は 300 以上 400 以下の整数 $\}$
   (2)
   - $300 \in C$.
   - $x \in C$ かつ $x < 400$ ならば $x + 1 \in C$.
   - C は他の要素を含まない.

   D: (1) $\{x \mid x$ または $x + 1$ は正の 4 の倍数 $\}$
   (2)
   - $3 \in D, 4 \in D$.
   - $x \in D$ ならば $x + 4 \in D$.
   - D は他の要素を含まない.

   E: (1) $\{x \mid x$ は 0, または正および負の 2 の倍数 $\}$
   (2)
   - $0 \in E$.
   - $x \in E$ ならば $x + 2 \in E$.
   - $x \in E$ ならば $-x \in E$.
   - E は他の要素を含まない.

   F: (1) $\{x \mid x = \frac{1}{2^n}, n$ は負でない整数 $\}$
   (2)
   - $1 \in F$.
   - $x \in F$ ならば $\frac{x}{2} \in F$.
   - F は他の要素を含まない.

5. (1) S_2, S_3, S_7
   (2) $S_1, S_3, S_4, S_5, S_6, S_8$
   (3) S_6, S_7
   (4) S_6, S_7, S_8, S_9
   (5) S_3
   (6) S_4, S_6

6. (1) $\{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$
   (2) $\{\phi, \{a\}\}$
   (3) $\{\phi\}$
   (4) $\{\phi, \{\phi\}\}$
   (5) $\mathcal{P}(\{\phi, \{a\}, \{b\}, \{a, b\}\}) = \{\ \phi,\ \{\phi\},\ \{\{a\}\},\ \{\{b\}\},\ \{\{a, b\}\},\ \{\phi, \{a\}\},\ \{\phi, \{b\}\},\ \{\phi, \{a, b\}\},$
   $\{\{a\}, \{b\}\}, \{\{a\}, \{a, b\}\}, \{\{b\}, \{a, b\}\}, \{\phi, \{a\}, \{b\}\}, \{\phi, \{a\}, \{a.b\}\}, \{\phi, \{b\}, \{a, b\}\}, \{\{a\}, \{b\}, \{a, b\}\},$
   $\{\phi, \{a\}, \{b\}, \{a, b\}\}\ \}$

7. (1) $\{a, b, c, 2\}$
   (2) $\{a, b, c, 2, 3, 4\}$
   (3) $\{b, c, a, \{c\}\}$
   (4) $\{a, b, \{a, b\}, \{c, 2\}\}$
   (5) $\{b, c\}$
   (6) $\{a, b\}$
   (7) $\{a, b\}$
   (8) $\{c\}$
   (9) ϕ
   (10) ϕ
   (11) ϕ
   (12) $\{c, 2, 3, 4\}$
   (13) ϕ
   (14) $\{2\}$
   (15) $\{a, b, \{c\}\}$
   (16) ϕ
   (17) $\{\{a, b\}, \{c, 2\}\}$

8. $U = \{a, b, c, 2, 3, 4, \{c\}, \{a, b\}, \{c, 2\}\}$
   (1) $\{a, b\} \cup C = \{a, b, c, 2\}$
   (2) $A \cap \{a, b, c, 2\} = \{a, b, c, 2\}$
   (3) $\{a, b, c, 2\} - \{c, 2, b\} = \{a\}$
   (4) $A \cap \{2\} = \{2\}$
   (5) $\{c, 2\} - \{b, c\} = \{2\}$
   (6) $\{a, b, c, 2, 3, 4, \{c\}\}$
   (7) $\{b\}^c = \{a, c, 2, 3, 4, \{c\}, \{a, b\}, \{c, 2\}\}$
   (8) $(D \cup \{c, 2, 3, 4, \{a, b\}, \{c, 2\}\})^c = \{a, \{c\}\}$
   (9) $F \cap \{c, 2, 3, 4\} = \phi$
   (10) $\{a, b\} \cup U = \{a, b, c, 2, 3, 4, \{c\}, \{a, b\}, \{c, 2\}\}$
   (11) $\{c, 2, b\} \cap U = \{c, 2, b\}$
   (12) $C \cap \{a, 2, 3, 4, \{c\}, \{a, b\}, \{c, 2\}\} = \{2\}$
   (13) $G \cup U = \{a, b, c, 2, 3, 4, \{c\}, \{a, b\}, \{c, 2\}\}$
   (14) $\phi^c = U = \{a, b, c, 2, 3, 4, \{c\}, \{a, b\}, \{c, 2\}\}$

9. (1) i) $\{a, b, c, d\}$
   ii) $\{c\}$
   iii) $\{a, b, c, d\}$
   iv) $\{a, b, c, d, e, f\}$
   v) $\{c, d\}$
   vi) ϕ
   vii) $\{a, b\}$
   (2) 成り立たない. $\{A, B\}$ のすべての要素は A, B である.
   (3) 成り立つ.

10. (1) 任意の $x \in A$ に対して, $x \in A$ または $x \in B$. すなわち, $x \in A \cup B$. ゆえに, $A \subseteq A \cup B$.
   (2) 任意の $x \in A \cup B$ に対して, $x \in A$ または $x \in B$. いずれの場合も $x \in C$ だから, $A \cup B \subseteq C$.
   (3) (a) $A \subseteq B$ ならば $A \cup B = B$ と (b) $A \cup B = B$ ならば $A \subseteq B$ を示せばよい.
      (a) 任意の $x \in A \cup B$ に対して, $x \in A$ または $x \in B$. いずれの場合も $x \in B$ だから, $A \cup B \subseteq B$.
      また, (1) より $B \subseteq A \cup B$.
      以上から, $A \cup B = B$.
      (b) 任意の $x \in A$ に対して, (1) より $x \in A \cup B = B$. ゆえに, $A \subseteq B$.
   (4) 任意の $x \in A \cap B$ に対して, $x \in A$ かつ $x \in B$. すなわち, $x \in A$ である. ゆえに, $A \cap B \subseteq A$.
   (5) 任意の $x \in C$ に対して, $x \in A$ かつ $x \in B$. すなわち, $x \in A \cap B$ だから, $C \subseteq A \cap B$.
   (6) (a) $A \subseteq B$ ならば $A \cap B = A$ と (b) $A \cap B = A$ ならば $A \subseteq B$ を示せばよい.
      (a) (4) より $A \cap B \subseteq A$.
      一方, 任意の $x \in A$ に対して, $x \in B$ だから, $x \in A \cap B$. ゆえに, $A \subseteq A \cap B$.
      以上から, $A \cap B = A$.
      (b) 任意の $x \in A$ に対して, $x \in A \cap B$ だから, $x \in B$. ゆえに, $A \subseteq B$.

11. (1)
   - 任意の $x \in A \cup A^c$ に対して, $x \in A \subseteq U$ または $x \in U - A$. 後者のとき, $x \in U$ かつ $x \notin A$. いずれの場合も, $x \in U$ だから, $A \cup A^c \subseteq U$.
   一方, 任意の $x \in U$ に対して, $x \in A$ または $x \in A^c$ だから, $x \in A \cup A^c$. ゆえに, $U \subseteq A \cup A^c$.
   以上から, $A \cup A^c = U$.

- $x \in A \cap A^c$ となる x は存在しないので, 任意の $x \in A \cap A^c$ に対して, $x \in \phi$ は明らか. ゆえに, $A \cap A^c \subseteq \phi$.
  一方, 明らかに, $\phi \subseteq A \cap A^c$.
  以上から, $A \cap A^c = \phi$.

(2) 任意の $x \in B^c$ に対して, $x \notin B$. ここで, $x \in A$ と仮定すると, $A \subseteq B$ だから, $x \in B$. これは矛盾. すなわち, $x \notin A$. ゆえに, $x \in A^c$ だから, $B^c \subseteq A^c$.

(3) 任意の $x \in A-B$ に対して, $x \in A$ かつ $x \notin B$. すなわち, $x \in A$ かつ $x \in B^c$ だから, $x \in A \cap B^c$. ゆえに, $A - B \subseteq A \cap B^c$.
一方, 任意の $x \in A \cap B^c$ に対して, $x \in A$ かつ $x \in B^c$ だから, $x \in A$ かつ $x \notin B$. すなわち, $x \in A - B$. ゆえに, $A \cap B^c \subseteq A - B$.
以上から, $A - B = A \cap B^c$.

(4)
- $U^c = U - U$ だから, $x \in U^c$ である x は存在しない. ゆえに, 任意の $x \in U^c$ に対して, $x \in \phi$ であることは明らか.
  一方, 明らかに, $\phi \subseteq U^c$.
  以上から, $U^c = \phi$.
- 任意の $x \in \phi^c$ に対して, $x \in U$ かつ $x \notin \phi$. すなわち, $\phi^c \subseteq U$.
  一方, 任意の $x \in U$ に対して, $x \notin \phi$ だから, $x \in U - \phi = \phi^c$. ゆえに, $U \subseteq \phi^c$.
  以上から, $\phi^c = U$.

(5) $(A^c)^c = U - A^c$ だから, 任意の $x \in (A^c)^c$ に対して, $x \in U$ かつ $x \notin A^c$. すなわち, $x \in A$. ゆえに, $(A^c)^c \subseteq A$.
一方, 任意の $x \in A$ に対して, $x \in U$ かつ $x \notin A^c$. すなわち $x \in (A^c)^c$. ゆえに, $A \subseteq (A^c)^c$.
以上から, $(A^c)^c = A$.

12. (1) 任意の $x \in (A \cup B)^c$ に対して, $x \notin A \cup B$. ゆえに, $x \notin A$ かつ $x \notin B$ だから, $x \in A^c$ かつ $x \in B^c$. すなわち, $x \in A^c \cap B^c$. したがって, $(A \cup B)^c \subseteq A^c \cap B^c$.
一方, 任意の $x \in A^c \cap B^c$ に対して, $x \in A^c$ かつ $x \in B^c$. ゆえに, $x \notin A$ かつ $x \notin B$ だから, $x \notin A \cup B$. すなわち, $x \in (A \cup B)^c$. したがって, $A^c \cap B^c \subseteq (A \cup B)^c$.
以上から, $(A \cup B)^c = A^c \cap B^c$.

(2) 任意の $x \in (A \cap B)^c$ に対して, $x \notin A \cap B$. ゆえに, $x \notin A$ または $x \notin B$ だから, $x \in A^c$ または $x \in B^c$. すなわち, $x \in A^c \cup B^c$. したがって, $(A \cap B)^c \subseteq A^c \cup B^c$.
一方, 任意の $x \in A^c \cup B^c$ に対して, $x \in A^c$ または $x \in B^c$. ゆえに, $x \notin A$ または $x \notin B$ だから, $x \notin A \cap B$. すなわち, $x \in (A \cap B)^c$ である. したがって, $A^c \cup B^c \subseteq (A \cap B)^c$.
以上から, $(A \cap B)^c = A^c \cup B^c$.

離散数学演習２　解答例

1. (1) $a = c$ かつ $b = d$.
   (2) $\{(x, y) \mid x \in A$ かつ $y \in B\}$
   (3) $R \subseteq A \times B$.
   (4) $(a, b) \in R$.
   (5) $\{x \in A \mid$ ある $y \in B$ に対して, $xRy\}$
   (6) $\{y \in B \mid$ ある $x \in A$ に対して, $xRy\}$
   (7) $\{(y, x) \mid (x, y) \in R\}$
   (8) $(A \times B) - R$
   (9) $\{(x, z) \mid$ ある $y \in B$ に対して, $(x, y) \in R$ かつ $(y, z) \in S\}$

2. (1) i) $\{(b, 2), (b, 3), (c, 2), (c, 3)\}$
   ii) $\{(2, b), (2, c), (3, b), (3, c)\}$
   iii) $\{(b, b), (b, c), (c, b), (c, c)\}$
   iv) $\{b, c, 2, 3\} \times B = \{(b, 2),\ (b, 3),\ (c, 2),\ (c, 3),\ (2, 2),\ (2, 3),\ (3, 2),\ (3, 3)\}$
   v) $\phi \times B = \phi$
   vi) $A^2 = \{(b, b), (b, c), (c, b), (c, c)\}$
   vii) $\{(b, 2, \alpha),\ (b, 2, \beta),\ (b, 3, \alpha),\ (b, 3, \beta),\ (c, 2, \alpha),\ (c, 2, \beta),\ (c, 3, \alpha),\ (c, 3, \beta)\}$
   viii) $\{(b, 2), (b, 3), (c, 2), (c, 3)\} \times C = \{((b, 2), \alpha),\ ((b, 2), \beta),\ ((b, 3), \alpha),\ ((b, 3), \beta),\ ((c, 2), \alpha),\ ((c, 2), \beta),\ ((c, 3), \alpha),\ ((c, 3), \beta)\}$
   ix) $A \times \{(2, \alpha), (2, \beta), (3, \alpha), (3, \beta)\} = \{(b, (2, \alpha)),\ (b, (2, \beta)),\ (b, (3, \alpha)),\ (b, (3, \beta)),\ (c, (2, \alpha)),\ (c, (2, \beta)),\ (c, (3, \alpha)),\ (c, (3, \beta))\}$

   (2) i) 誤. $(A \times B) \cup (B \times A) = \{(b, 2),\ (b, 3),\ (c, 2),\ (c, 3),\ (2, b),\ (2, c),\ (3, b),\ (3, c)\} \neq \phi$
   ii) 誤. $(b, b) \in A \times A$ に対して, $(b, b) \notin A \times B$.
   iii) 誤. $(c, c) \in A \times A$.
   iv) 正. $(b, 3) \in A \times B, (3, b) \in B \times A$.
   v) 正.
   vi) 正. $b, c \in A, 2, 3 \in B$ だから, $\{(b, 2), (c, 3)\} \subseteq A \times B$.
   vii) 正. $b \in A$ だから, $\{(b, b)\} \subseteq A^2$.

3. $\begin{aligned} R \cup S &= \{(1, a), (3, a), (2, b), (3, b), (1, b)\} \\ R \cap S &= \{(2, b)\} \\ R^c &= \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\} - R \\ &= \{(1, b), (2, a)\} \end{aligned}$

4. (1) 定義域 $\{b, c\}$, 値域 $\{b, 2, 3\}$
   (2) $A \times (A \cup B) =\{(b, b),\ (b, c),\ (b, 2),\ (b, 3),\ (c, b),\ (c, c),\ (c, 2),\ (c, 3)\}$ だから,
   $\begin{aligned} R^c &= A \times (A \cup B) - R \\ &= \{(b, c), (b, 3), (c, b), (c, c)\} \\ R^{-1} &= \{(b, b), (2, b), (2, c), (3, c)\} \end{aligned}$

   (3)
   $\begin{aligned} (R^c)^{-1} &= \{(c, b), (3, b), (b, c), (c, c)\} \\ (R^{-1})^c &= ((A \cup B) \times A) - R^{-1} \\ &= \{(b, b), (b, c), (c, b), (c, c), (2, b), (2, c), (3, b), (3, c)\} - R^{-1} \\ &= \{(b, c), (c, b), (c, c), (3, b)\} \end{aligned}$
   ゆえに, $(R^c)^{-1} = (R^{-1})^c$.

5. $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 6), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (6, 6)\}$

6. (1) $\begin{aligned} S \circ R &= \{(1, 2), (1, 4), (1, 3), (2, 2), (2, 4), (2, 3), (3, 4), (4, 2), (4, 4), (4, 3)\} \\ R \circ S &= \{(3, 4), (3, 1), (1, 1), (1, 2), (1, 4), (2, 4), (2, 3), (2, 1), (1, 3)\} \end{aligned}$

(2) $R^{-1} = \{(1,1),(1,2),(4,3),(2,2),(3,3),(4,4),(1,4)\}$
$R^{-1} \circ R = \{(1,1),(1,2),(1,4),(2,1),(2,2),(2,4),(3,3),(3,4),(4,3),(4,4),(4,1),(4,2)\}$
$(1,2) \in R^{-1} \circ R$ に対して, $(1,2) \notin I$ だから, $R^{-1} \circ R \neq I$.

(3) $S^{-1} = \{(4,3),(2,1),(4,1),(3,2),(4,2),(3,1)\}$
$S^{-1} \circ S = \{(3,3),(3,1),(3,2),(1,1),(1,3),(1,2),(2,2),(2,1),(2,3)\}$
$(3,1) \in S^{-1} \circ S$ に対して, $(3,1) \notin I$ だから, $S^{-1} \circ S \not\subseteq I$.

7. $\mathcal{P}(B) = \{X | X \subseteq B\}$
$= \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{c,a\}, \{a,b,c\}\}$
$\subseteq = \{(X,Y) \in \mathcal{P}(B)^2 | X \subseteq Y\}$
$= \{ (\phi,\phi), (\phi,\{a\}), (\phi,\{b\}), (\phi,\{c\}), (\phi,\{a,b\}), (\phi,\{b,c\}), (\phi,\{c,a\}), (\phi,\{a,b,c\}),$
$(\{a\},\{a\}), (\{a\},\{a,b\}), (\{a\},\{c,a\}), (\{a\},\{a,b,c\}),$
$(\{b\},\{b\}), (\{b\},\{a,b\}), (\{b\},\{b,c\}), (\{b\},\{a,b,c\}),$
$(\{c\},\{c\}), (\{c\},\{b,c\}), (\{c\},\{c,a\}), (\{c\},\{a,b,c\}),$
$(\{a,b\},\{a,b\}), (\{a,b\},\{a,b,c\}), (\{b,c\},\{b,c\}), (\{b,c\},\{a,b,c\}),$
$(\{c,a\},\{c,a\}), (\{c,a\},\{a,b,c\}), (\{a,b,c\},\{a,b,c\}) \}$

8. (1) 任意の $(x,y) \in A \times (B \cap C)$ に対して, $x \in A$, $y \in B \cap C$. すなわち, $y \in B$ かつ $y \in C$. ゆえに, $(x,y) \in A \times B$ かつ $(x,y) \in A \times C$ だから, $(x,y) \in (A \times B) \cap (A \times C)$. したがって, $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.
一方, 任意の $(x,y) \in (A \times B) \cap (A \times C)$ に対して, $(x,y) \in A \times B$ かつ $(x,y) \in A \times C$. すなわち, $x \in A$ で, $y \in B$ かつ $y \in C$. ゆえに, $y \in B \cap C$ だから, $(x,y) \in A \times (B \cap C)$. したがって, $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$.
以上から, $(A \times B) \cap (A \times C) = A \times (B \cap C)$.

(2) 任意の $(x,y) \in A \times (B \cup C)$ に対して, $x \in A$, $y \in B \cup C$. すなわち, $y \in B$ または $y \in C$. ゆえに, $(x,y) \in A \times B$ または $(x,y) \in A \times C$ だから, $(x,y) \in (A \times B) \cup (A \times C)$. したがって, $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.
一方, 任意の $(x,y) \in (A \times B) \cup (A \times C)$ に対して, $(x,y) \in A \times B$ または $(x,y) \in A \times C$. すなわち, $x \in A$ で, $y \in B$ または $y \in C$. ゆえに, $y \in B \cup C$ だから, $(x,y) \in A \times (B \cup C)$. したがって, $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$.
以上から, $(A \times B) \cup (A \times C) = A \times (B \cup C)$.

9. (1) 任意の $(x,y) \in (R^{-1})^{-1}$ に対して, $(y,x) \in R^{-1}$. ゆえに, $(x,y) \in R$. したがって, $(R^{-1})^{-1} \subseteq R$.
一方, 任意の $(x,y) \in R$ に対して, $(y,x) \in R^{-1}$. ゆえに, $(x,y) \in (R^{-1})^{-1}$. したがって, $R \subseteq (R^{-1})^{-1}$.
以上から, $(R^{-1})^{-1} = R$.

(2) 任意の $(x,y) \in R^{-1}$ に対して, $(y,x) \in R \subseteq S$. ゆえに, $(x,y) \in S^{-1}$ だから, $R^{-1} \subseteq S^{-1}$.

(3) 任意の $(x,y) \in (R \cup S)^{-1}$ に対して, $(y,x) \in R \cup S$. すなわち, $(y,x) \in R$ または $(y,x) \in S$. ゆえに, $(x,y) \in R^{-1}$ または $(x,y) \in S^{-1}$. したがって, $(x,y) \in R^{-1} \cup S^{-1}$ だから, $(R \cup S)^{-1} \subseteq R^{-1} \cup S^{-1}$.
一方, 任意の $(x,y) \in R^{-1} \cup S^{-1}$ に対して, $(x,y) \in R^{-1}$ または $(x,y) \in S^{-1}$. すなわち, $(y,x) \in R$ または $(y,x) \in S$. ゆえに, $(y,x) \in R \cup S$ だから, $(x,y) \in (R \cup S)^{-1}$. したがって, $R^{-1} \cup S^{-1} \subseteq (R \cup S)^{-1}$.
以上から, $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$.

(4) 任意の $(x,y) \in (R \cap S)^{-1}$ に対して, $(y,x) \in R \cap S$. すなわち, $(y,x) \in R$ かつ $(y,x) \in S$. ゆえに, $(x,y) \in R^{-1}$ かつ $(x,y) \in S^{-1}$. したがって, $(x,y) \in R^{-1} \cap S^{-1}$ だから, $(R \cap S)^{-1} \subseteq R^{-1} \cap S^{-1}$.
一方, 任意の $(x,y) \in R^{-1} \cap S^{-1}$ に対して, $(x,y) \in R^{-1}$ かつ $(x,y) \in S^{-1}$. すなわち, $(y,x) \in R$ かつ $(y,x) \in S$. ゆえに, $(y,x) \in R \cap S$ だから, $(x,y) \in (R \cap S)^{-1}$. したがって, $R^{-1} \cap S^{-1} \subseteq (R \cap S)^{-1}$.
以上から, $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$.

(5) 任意の $(x,y) \in (R - S)^{-1}$ に対して, $(y,x) \in R - S$. すなわち, $(y,x) \in R$ かつ $(y,x) \notin S$. ゆえに, $(x,y) \in R^{-1}$ かつ $(x,y) \notin S^{-1}$. したがって, $(x,y) \in R^{-1} - S^{-1}$ だから, $(R-S)^{-1} \subseteq R^{-1} - S^{-1}$.
一方, 任意の $(x,y) \in R^{-1} - S^{-1}$ に対して, $(x,y) \in R^{-1}$ かつ $(x,y) \notin S^{-1}$. すなわち, $(y,x) \in R$ かつ $(y,x) \notin S$. したがって, $(y,x) \in R - S$ だから, $(x,y) \in (R-S)^{-1}$ であり, $R^{-1} - S^{-1} \subseteq (R-S)^{-1}$.
以上から, $(R-S)^{-1} = R^{-1} - S^{-1}$.

10. 任意の $(x,y) \in (T \circ S) \circ R$ に対して, ある $z \in B$ が存在して, $(x,z) \in R$ かつ $(z,y) \in T \circ S$. さらに, ある $w \in C$ が存在して, $(z,w) \in S$ かつ $(w,y) \in T$. $(x,z) \in R$, $(z,w) \in S$ だから, $(x,w) \in S \circ R$. さらに, $(w,y) \in T$ だから, $(x,y) \in T \circ (S \circ R)$. したがって, $(T \circ S) \circ R \subseteq T \circ (S \circ R)$.

一方, 任意の $(x,y) \in T \circ (S \circ R)$ に対して, ある $z \in C$ が存在して, $(x,z) \in S \circ R$ かつ $(z,y) \in T$. さらに, ある $w \in B$ が存在して, $(x,w) \in R$ かつ $(w,z) \in S$. $(w,z) \in S$, $(z,y) \in T$ だから, $(w,y) \in T \circ S$. さらに, $(x,w) \in R$ だから, $(x,y) \in (T \circ S) \circ R$. したがって, $T \circ (S \circ R) \subseteq (T \circ S) \circ R$.

以上から, $(T \circ S) \circ R = T \circ (S \circ R)$.

離散数学演習 3　解答例

1. (1) 任意の $x \in A$ に対して, $(x,x) \in R$.
   (2) 任意の $x,y \in A$ に対して, $(x,y) \in R$ ならば $(y,x) \in R$.
   (3) 任意の $x,y \in A$ に対して, $(x,y) \in R$ かつ $(y,x) \in R$ ならば $x = y$.
   (4) 任意の $x,y,z \in A$ に対して, $(x,y) \in R$ かつ $(y,z) \in R$ ならば $(x,z) \in R$.
   (5) $\{(x,x) \mid x \in A\}$
   (6) $\bigcup_{n=1}^{\infty} R^n$
   （別解）$\{(x,y) \mid$ ある $x_0, x_1, \cdots, x_n$ $(n \geq 1)$ に対して, $x_0 = x, x_n = y, (x_i, x_{i+1}) \in R$ $(i = 0,1,\cdots,n-1)\}$
   (7) $\bigcup_{n=0}^{\infty} R^n$
   （別解）$I_A \cup R^+$
   （別解）$\{(x,y) \mid$ ある $x_0, x_1, \cdots, x_n$ $(n \geq 0)$ に対して, $x_0 = x, x_n = y, (x_i, x_{i+1}) \in R$ $(i = 0,1,\cdots,n-1)\}$

2. R: $(2,2) \notin R$ だから, R は反射的でない.
   $(1,2) \in R$ に対して, $(2,1) \notin R$ だから, R は対称的でない.
   $(1,1),(1,1) \in R$ に対して, $(1,1) \in R$.
   $(1,1),(1,2) \in R$ に対して, $(1,2) \in R$.
   $(1,1),(1,3) \in R$ に対して, $(1,3) \in R$.
   $(1,3),(3,3) \in R$ に対して, $(1,3) \in R$.
   $(3,3),(3,3) \in R$ に対して, $(3,3) \in R$.
   以上から, 任意の $x,y \in A$ に対して, $(x,y),(y,z) \in R$ ならば $(x,z) \in R$ だから, R は推移的である.
   $(1,1),(1,1) \in R$ に対して, $1 = 1$.
   $(3,3),(3,3) \in R$ に対して, $3 = 3$.
   以上から, 任意の $x,y \in A$ に対して, $(x,y),(y,x) \in R$ ならば $x = y$ だから, R は反対称的である.

   S: $(1,1),(2,2),(3,3) \in S$ だから, S は反射的である.
   $(1,1) \in S$ に対して, $(1,1) \in S$.
   $(1,2) \in S$ に対して, $(2,1) \in S$.
   $(2,1) \in S$ に対して, $(1,2) \in S$.
   $(2,2) \in S$ に対して, $(2,2) \in S$.
   $(3,3) \in S$ に対して, $(3,3) \in S$.
   以上から, 任意の $x,y \in A$ に対して, $(x,y) \in S$ ならば $(y,x) \in S$ だから,S は対称的である.
   $(1,1),(1,1) \in S$ に対して, $(1,1) \in S$.
   $(1,1),(1,2) \in S$ に対して, $(1,2) \in S$.
   $(1,2),(2,1) \in S$ に対して, $(1,1) \in S$.
   $(1,2),(2,2) \in S$ に対して, $(1,2) \in S$.
   $(2,1),(1,1) \in S$ に対して, $(2,1) \in S$.
   $(2,1),(1,2) \in S$ に対して, $(2,2) \in S$.
   $(2,2),(2,1) \in S$ に対して, $(2,1) \in S$.
   $(2,2),(2,2) \in S$ に対して, $(2,2) \in S$.
   $(3,3),(3,3) \in S$ に対して, $(3,3) \in S$.
   以上から, 任意の $x,y \in A$ に対して, $(x,y),(y,z) \in S$ ならば $(x,z) \in S$ だから, S は推移的である.
   $(1,2),(2,1) \in S$ に対して, $1 \neq 2$ だから, S は反対称的でない.

   T: $(3,3) \notin T$ だから, T は反射的でない.
   $(1,2) \in T$ に対して, $(2,1) \notin T$ だから, T は対称的でない.
   $(1,2),(2,3) \in T$ に対して, $(1,3) \notin T$ だから, T は推移的でない.
   $(1,1),(1,1) \in T$ に対して, $1 = 1$.
   $(2,2),(2,2) \in T$ に対して, $2 = 2$.

以上から, 任意の $x, y \in A$ に対して, $(x, y) \in T$ かつ $(y, x) \in T$ ならば $x = y$ だから, T は反対称的である.

3. ϕ: ある $x \in A$ に対して, $(x, x) \notin \phi$ である. ゆえに, 任意の $x \in A$ に対して $(x, x) \in \phi$ ではないから, ϕ は反射的でない.
$(x, y) \in \phi$ かつ $(y, x) \notin \phi$ である $x, y \in A$ は存在しない[1]. ゆえに, 任意の $x, y \in A$ に対して, $(x, y) \in \phi$ ならば $(y, x) \in \phi$ だから, ϕ は対称的である.
$(x, y), (y, x) \in \phi$ かつ $x \neq y$ である $x, y \in A$ は存在しない[2]. ゆえに, 任意の $x, y \in A$ に対して, $(x, y), (y, x) \in \phi$ ならば $x = y$ だから, ϕ は反対称的である.
$(x, y), (y, z) \in \phi$ かつ $(x, z) \notin \phi$ である $x, y, z \in A$ は存在しない[3]. ゆえに, 任意の $x, y, z \in A$ に対して, $(x, y), (y, x) \in \phi$ ならば, $(x, z) \in \phi$ だから, ϕ は推移的である.
(任意の $x, y \in A$ に対して, $(x, y) \notin \phi$ だから, ϕ が対称的, 推移的, 反対称的であることはそれぞれ (空虚に) 成り立つ.)

   A^2: 任意の $x \in A$ に対して, $(x, x) \in A^2$ だから, A^2 は反射的である.
任意の $x, y \in A$ に対して, $(x, y) \in A^2$ とすると, $(y, x) \in A^2$ だから, A^2 は対称的である.
$A = \{1, 2\}$ のとき, $(1, 2), (2, 1) \in A^2$ に対して, $1 \neq 2$ だから, A^2 は反対称的でない.
任意の $x, y, z \in A$ に対して, $(x, y), (y, z) \in A^2$ とすると, $(x, z) \in A^2$ だから, A^2 は推移的である.

   I_A: 任意の $x \in A$ に対して, $(x, x) \in I_A$ だから, I_A は反射的である.
任意の $x, y \in A$ に対して, $(x, y) \in I_A$ とすると, $x = y$ だから, $(y, x) \in I_A$. ゆえに, I_A は対称的である.
任意の $x, y \in A$ に対して, $(x, y), (y, x) \in I_A$ とすると, $x = y$ だから, I_A は反対称的である.
任意の $x, y, z \in A$ に対して, $(x, y), (y, z) \in I_A$ とすると, $x = y = z$ だから, $(x, z) \in I_A$. ゆえに, I_A は推移的である.

4. (1) R, S は反射的だから, 任意の $x \in A$ に対して, $(x, x) \in R$, $(x, x) \in S$. ゆえに, $(x, x) \in R \cap S$ だから, $R \cap S$ は反射的である.

   (2) 任意の $x, y \in A$ に対して, $(x, y) \in R \cap S$ とする. このとき, $(x, y) \in R$ かつ $(x, y) \in S$. R は対称的だから, $(x, y) \in R$ ならば, $(y, x) \in R$. また, S は対称的だから, $(x, y) \in S$ ならば, $(y, x) \in S$. ゆえに, $(y, x) \in R$ かつ $(y, x) \in S$ だから, $(y, x) \in R \cap S$. したがって, $R \cap S$ は対称的である.

   (3) 任意の $x, y, z \in A$ に対して, $(x, y), (y, z) \in R \cap S$ とする. このとき, $(x, y), (y, z) \in R$ かつ $(x, y), (y, z) \in S$. R は推移的だから, $(x, y), (y, z) \in R$ ならば, $(x, z) \in R$. また, S は推移的だから, $(x, y), (y, z) \in S$ ならば, $(x, z) \in S$. ゆえに, $(x, z) \in R$ かつ $(x, z) \in S$ だから, $(x, z) \in R \cap S$. したがって, $R \cap S$ は推移的である.

   (4) 任意の $x, y \in A$ に対して, $(x, y), (y, x) \in R^{-1}$ とする. このとき, $(y, x), (x, y) \in R$. R は反対称的だから, $x = y$. したがって, R^{-1} は反対称的である.

   (5) 任意の $x, y \in A$ に対して, $(x, y) \in R \cup R^{-1}$ とする. このとき, $(x, y) \in R$ または $(x, y) \in R^{-1}$. ゆえに, $(y, x) \in R^{-1}$ または $(y, x) \in R$. すなわち, $(y, x) \in R \cup R^{-1}$. したがって, $R \cup R^{-1}$ は対称的である.

5. 「…任意の x, y に対して, xRy ならば yRx である. このとき, xRy, yRx から, …」の部分が誤り. 「xRy ならば yRx」が成り立つとしても, このとき「xRy かつ yRx」が成り立つとは限らない.
実際, $A = \{a, b\}$, $R = \{(a, a)\} \subseteq A^2$ とすると, R は対称的かつ推移的であるが, 反射的ではない.

6. (1) R は反射的であるとする. ゆえに, 任意の $x \in A$ に対して, $(x, x) \in R$. $I_A = \{(x, x) \mid x \in A\}$ だから, $I_A \subseteq R$.
   $I_A \subseteq R$ とする. 任意の $x \in A$ に対して, $(x, x) \in I_A \subseteq R$ だから, R は反射的である.

   (2) R は対称的であるとする. 任意の $(x, y) \in R^{-1}$ に対して, $(y, x) \in R$. R は対称的だから, $(x, y) \in R$. ゆえに, $R^{-1} \subseteq R$.
   $R^{-1} \subseteq R$ とする. また, 任意の $x, y \in A$ に対して, $(x, y) \in R$ とする. このとき, $(y, x) \in R^{-1} \subseteq R$ だから, R は対称的である.

   (3) R は推移的であるとする. 任意の $(x, y) \in R^2$ に対して, $R^2 = R \circ R$ だから, ある $z \in A$ に対して, $(x, z) \in R$ かつ $(z, y) \in R$. R は推移的だから, $(x, y) \in R$. ゆえに, $R^2 \subseteq R$.

[1] すなわち, ϕ が対称的であることの定義に対する反例は存在しない.
[2] すなわち, ϕ が反対称的であることの定義に対する反例は存在しない.
[3] すなわち, ϕ が推移的であることの定義に対する反例は存在しない.

$R^2 \subseteq R$ とする．また，任意の $x, y, z \in A$ に対して，$(x, y), (y, z) \in R$ とする．このとき，$(x, z) \in R^2 \subseteq R$ だから，R は推移的である．

7. $A = \{1, 2, \cdots, n\}$ とし，$R \subseteq A^2$ とする．

   (1) R が反射的であるためには，$I_A = \{(1, 1), (2, 2), \cdots, (n, n)\} \subseteq R$ であればよい．ゆえに，$R - I_A$ を定めると，反射的な関係 R が一つ定まる．
   $R - I_A \subseteq A^2 - I_A$ だから，求める数は $A^2 - I_A$ の部分集合の総数 $|\mathcal{P}(A^2 - I_A)|$ である．
   ここで，$I_A \subset A^2$，$|I_A| = n$，$|A^2| = n^2$ だから，$|A^2 - I_A| = |A^2| - |I_A| = n^2 - n$．したがって，$|\mathcal{P}(A^2 - I_A)| = 2^{n^2-n}$．

   (2) R が対称的であるためには，$(x, y) \in R$ ならば，$(y, x) \in R$ であればよい．ゆえに，$B = \{(x, y) \in A^2 \mid x \leq y\}$ に対して，$R \subseteq B$ を定めると，R は対称的である．
   ゆえに，求める数は B の部分集合の総数 $|\mathcal{P}(B)|$ である．
   ここで，$|B| = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ だから，$|\mathcal{P}(B)| = 2^{\frac{n(n+1)}{2}}$．

   (3) (1), (2) から，$B - I_A = \{(x, y) \in A^2 \mid x < y\}$ に対して，$R \subseteq B$ を定めると，反射的かつ対称的な関係 $R \cup I_A$ が一つ定まる．
   ゆえに，求める数は $B - I_A$ の部分集合の総数 $|\mathcal{P}(B - I_A)|$ である．
   ここで，$|B - I_A| = 1 + 2 + \cdots + (n - 1) = \frac{n(n-1)}{2}$ だから，$|\mathcal{P}(B - I_A)| = 2^{\frac{n(n-1)}{2}}$．

8. (1) 任意の x, y, z に対して，$(x, y), (y, z) \in R^*$ とする．$(x, y) \in R^*$ だから，ある $x_0, x_1, \cdots, x_n$ $(n \geq 0)$ に対して，$x_0 = x, x_n = y, (x_i, x_{i+1}) \in R$ $(i = 0, 1, \cdots, n - 1)$．また，$(y, z) \in R^*$ だから，ある $x_n, x_{n+1}, \cdots, x_m$ $(m \geq n)$ に対して，$x_n = y, x_m = z, (x_i, x_{i+1}) \in R$ $(i = n, n+1, \cdots, m-1)$．ゆえに，$x_0, x_1, \cdots, x_n, x_{n+1}, \cdots, x_m$ に対して，$x_0 = x, x_m = z, (x_i, x_{i+1}) \in R$ $(i = 0, 1, \cdots, m - 1)$．したがって，$(x, z) \in R^*$ であるから，R^* は推移的である．

   (2) R は推移的であるとする．
   明らかに，$R \subseteq R^+$．
   一方，任意の x, y に対して，$(x, y) \in R^+$ とする．このとき，ある $x_0, x_1, \cdots, x_n$ $(n \geq 1)$ に対して，$x_0 = x, x_n = y, (x_i, x_{i+1}) \in R$ $(i = 0, 1, \cdots, n - 1)$．$(x_0, x_1), (x_1, x_2) \in R$ で，R は推移的だから，$(x_0, x_2) \in R$．さらに，$(x_0, x_2), (x_2, x_3) \in R$ で，R は推移的だから，$(x_0, x_3) \in R$．同様に繰り返すと，$(x_0, x_n) \in R$．すなわち，$(x, y) \in R$．ゆえに，$R^+ \subseteq R$．
   以上から，$R = R^+$．

   (3) R は反射的であるとする．このとき，任意の x に対して，$(x, x) \in R \subseteq R^+$．ゆえに，$R^+$ は反射的である．

   (4) R は対称的であるとする．
   また，任意の x, y に対して，$(x, y) \in R^*$ とする．このとき，ある $x_0, x_1, \cdots, x_n$ $(n \geq 0)$ に対して，$x_0 = x, x_n = y, (x_i, x_{i+1}) \in R$ $(i = 0, 1, \cdots, n - 1)$．$R$ は対称的だから，$(x_{i+1}, x_i) \in R$ $(i = 0, \cdots, n - 1)$．ゆえに，$x_n, x_{n-1}, \cdots, x_0$ に対して，$x_n = y, x_0 = x, (x_{i+1}, x_i) \in R$ $(i = 0, 1, \cdots, n - 1)$ であるから，$(y, x) \in R^*$．したがって，R^* は対称的である．

   (5) $R \subseteq S$ とする．
   また，任意の x, y に対して，$(x, y) \in R^*$ とする．このとき，ある $x_0, x_1, \cdots, x_n$ $(n \geq 0)$ に対して，$x_0 = x, x_n = y, (x_i, x_{i+1}) \in R$ $(i = 0, \cdots, n-1)$．$R \subseteq S$ だから，$(x_i, x_{i+1}) \in S$ $(i = 0, 1, \cdots, n-1)$．ゆえに，$x_0, x_1, \cdots, x_n$ に対して，$x_0 = x, x_n = y, (x_i, x_{i+1}) \in S$ $(i = 0, 1, \cdots, n - 1)$ であるから，$(x, y) \in S^*$．したがって，$R^* \subseteq S^*$．

   (6) $R \subseteq S$，かつ，S は推移的であるとする．
   また，任意の x, y に対して，$(x, y) \in R^+$ とする．このとき，ある $x_0, x_1, \cdots, x_n$ $(n \geq 1)$ に対して，$x_0 = x, x_n = y, (x_i, x_{i+1}) \in R$ $(i = 0, 1, \cdots, n - 1)$．$R \subseteq S$ だから，$(x_i, x_{i+1}) \in S$ $(i = 0, 1, \cdots, n - 1)$．$(x_0, x_1), (x_1, x_2) \in S$ で，S は推移的だから，$(x_0, x_2) \in S$．さらに，$(x_0, x_2), (x_2, x_3) \in S$ で，S は推移的だから，$(x_0, x_3) \in S$．同様に繰り返すと，$(x_0, x_n) \in S$．すなわち，$(x, y) \in S$．ゆえに，$R^+ \subseteq S$．

9. (1) n に関する帰納法を用いて示す．
   （基底段階）$n = 2$ のとき．このとき $k = 1$ である．

$$\begin{aligned} R^{n-k} \circ R^k &= R^{2-1} \circ R^1 \\ &= R \circ R \\ &= R^2 \\ &= R^n \end{aligned}$$

だから，$n = 2$ のとき，命題は成り立つ．
（帰納段階）$n = m$ のときに命題は成り立つと仮定する．$n = m + 1$ のときを考え，k に関する帰納法を用いて示す[1] ．

i) （基底段階）$k = 1$ のとき．

$$\begin{aligned} R^{n-k} \circ R^k &= R^{(m+1)-1} \circ R^1 \\ &= R^m \circ R \\ &= R^{m+1} \\ &= R^n \end{aligned}$$

ii) （帰納段階）$2 \leq k \leq n - 1 = m$ のとき．このとき，$k - 1$ に対して命題は成り立つと仮定する．

$$\begin{aligned} R^{n-k} \circ R^k &= R^{(m+1)-k} \circ R^k \\ &= R^{(m+1)-k} \circ (R^{k-1} \circ R^1) \quad (R^k \text{ の定義}) \\ &= R^{m-(k-1)} \circ (R^{k-1} \circ R^1) \\ &= (R^{m-(k-1)} \circ R^{k-1}) \circ R^1 \quad (\text{関係の合成に関する結合則}) \\ &= R^m \circ R \quad (k \text{ に関する帰納法の仮定}) \\ &= R^{m+1} \\ &= R^n \end{aligned}$$

ゆえに，任意の k に対して，命題は成り立つ．
以上から，$n = m + 1$ のときも命題は成り立つ．
すなわち，任意の n に対して，命題は成り立つ．

(2) 任意の $(x, y), (y, z) \in R^+$ に対して，$R^+ = \bigcup_{n=1}^{\infty} R^n$ だから，n, m (≥ 1) が存在して，$(x, y) \in R^n, (y, z) \in R^m$．ゆえに，$(x, z) \in R^m \circ R^n$．
(1) から $R^m \circ R^n = R^{m+n}$ だから，$(x, z) \in R^{m+n} \subseteq R^+$．
ゆえに，R^+ は推移的である．

(3) 任意の $x \in A$ に対して，$(x, x) \in I_A \subseteq R^*$．ゆえに，$R^*$ は反射的である．
任意の $(x, y), (y, z) \in R^*$ に対して，$R^* = I_A \cup R^+$ だから，次の i)〜iv) の場合が考えられる．

i) $(x, y), (y, z) \in I_A$ のとき．
このとき，$x = y = z$ だから $(x, z) \in I_A \subseteq R^*$．ゆえに，$R^*$ は推移的である．

ii) $(x, y), (y, z) \in R^+$ のとき．
このとき，(2) から R^+ は推移的だから，$(x, z) \in R^+ \subseteq R^*$．ゆえに，$R^*$ は推移的である．

iii) $(x, y) \in I_A$, $(y, z) \in R^+$ のとき．
このとき，$x = y$ だから，$(x, z) \in R^+ \subseteq R^*$．ゆえに，$R^*$ は推移的である．

iv) $(x, y) \in R^+$, $(y, z) \in I_A$ のとき．
(iii) と同様に，R^* は推移的である．

以上から，R^* は推移的である．

10. 集合 A に対して，$R \subseteq A^2$ とする．

（例）連続的 (serial) ：任意の $x \in A$ に対して，$y \in A$ が存在して，xRy である．
比較可能（comparable）（完全 (total)）：任意の $x, y \in A$ に対して，xRy または yRx である．
非反射的 (irreflexive) ：任意の $x \in A$ に対して，xRx でない．
非対称的 (asymmetric) ：任意の $x, y \in A$ に対して，xRy ならば，yRx でない．
Euclid 的 (Euclidean) ：任意の $x, y, z \in A$ に対して，xRy かつ xRz ならば，yRz である．
合流的 (confluent) ：任意の $x, y, z \in A$ に対して，xRy かつ xRz ならば，$w \in A$ が存在して，yRw かつ zRw である．

11. 略．

[1] 二重帰納法であることに注意せよ．すなわち，n に関する帰納法の中で，k に関する帰納法を用いる．

離散数学演習 4　解答例

1. (1) R は反射的, 対称的, かつ推移的である.

   (2) ある整数 d に対して, $m - n = d \cdot p$.
   （別解）m と n は p で割ったときの余りが等しい.
   （別解）$m - n$ は p の倍数である.

   (3) $\{x \in A \mid (a, x) \in R\}$

   (4) $\{\ [x]_R \mid x \in A\}$

   (5) 次の i)〜iii) を満たす集合のクラス $\pi = \{A_1, \cdots, A_n\}$

   i) 任意の $A_i \in \pi$ に対して, $A_i \neq \phi$.

   ii) $\bigcup_{i=1}^{n} A_i = A$.

   iii) 任意の $A_i, A_j \in \pi$ に対して, $A_i \neq A_j$ ならば $A_i \cap A_j = \phi$.

   (6) $\{(x, y) \mid$ ある $A_i \in \pi$に対して, $x, y \in A_i\}$

   (7) π_1, π_2 がそれぞれ定める A 上の同値関係 R_{π_1}, R_{π_2} に対して, $R_{\pi_1} \subseteq R_{\pi_2}$.

2. $(1,1), (2,2), (3,3) \in R$ だから, R は反射的である.
   $(1,1) \in R$ に対して, $(1,1) \in R$.
   $(1,2) \in R$ に対して, $(2,1) \in R$.
   $(2,1) \in R$ に対して, $(1,2) \in R$.
   $(2,2) \in R$ に対して, $(2,2) \in R$.
   $(3,3) \in R$ に対して, $(3,3) \in R$.
   以上から, R は対称的である.
   $(1,1), (1,1) \in R$ に対して, $(1,1) \in R$.
   $(1,1), (1,2) \in R$ に対して, $(1,2) \in R$.
   $(1,2), (2,1) \in R$ に対して, $(1,1) \in R$.
   $(1,2), (2,2) \in R$ に対して, $(1,2) \in R$.
   $(2,1), (1,1) \in R$ に対して, $(2,1) \in R$.
   $(2,1), (1,2) \in R$ に対して, $(2,2) \in R$.
   $(2,2), (2,2) \in R$ に対して, $(2,2) \in R$.
   $(2,2), (2,1) \in R$ に対して, $(2,1) \in R$.
   $(3,3), (3,3) \in R$ に対して, $(3,3) \in R$.
   以上から, R は推移的である.
   したがって, R は同値関係である.

   $[1]_R = \{1, 2\}$
   $[2]_R = \{1, 2\}$
   $[3]_R = \{3\}$
   $A/R = \{[1]_R, [2]_R, [3]_R\} = \{\{1, 2\}, \{3\}\}$

3. R は対称的かつ推移的だから, R が反射的であることを示せばよい.
   任意の $a \in A$ に対して, ある $b \in A$ が存在して, $(a, b) \in R$ である. このとき, R は対称的だから, $(b, a) \in R$. さらに, $(a, b), (b, a) \in R$ で, R は推移的だから, $(a, a) \in R$. すなわち, R は反射的である.

4. 任意の整数 x に対して, $x - x = 0 \cdot m$ だから, $x \equiv_m x$. すなわち, $\equiv_m$ は反射的である.
   任意の整数 x, y に対して, $x \equiv_m y$ とすると, $x - y = k \cdot m$ (k は整数) とおける. このとき, $y - x = -k \cdot m$ ($-k$ は整数) だから, $y \equiv_m x$. すなわち, $\equiv_m$ は対称的である.
   任意の整数 x, y, z に対して, $x \equiv_m y, y \equiv_m z$ とすると, $x - y = k_1 \cdot m, y - z = k_2 \cdot m$ (k_1, k_2 は整数) とおける. このとき, $x - z = (k_1 + k_2) \cdot m$ ($k_1 + k_2$ は整数) だから, $x \equiv_m z$. すなわち, $\equiv_m$ は推移的である.
   以上から, $\equiv_m$ は同値関係である.

5. $$\begin{aligned} [(2,7)]_\sim &= \{(x, y) \mid y = 5 + x, x, y \in A\} \\ &= \{(1,6), (2,7), (3,8), (4,9), (5,10), (6,11), (7,12), (8,13), (9,14), (10,15)\} \end{aligned}$$

6. 任意の $(a,b) \in \mathbf{N}^2$ に対して, $ab = ba$ だから, $(a,b) \simeq (a,b)$. すなわち, $\simeq$ は反射的である.
任意の $(a,b),(c,d) \in \mathbf{N}^2$ に対して, $(a,b) \simeq (c,d)$ とすると, $ad = bc$. このとき, $cb = da$ だから, $(c,d) \simeq (a,b)$. すなわち, $\simeq$ は対称的である.
任意の $(a,b),(c,d),(e,f) \in \mathbf{N}^2$ に対して, $(a,b) \simeq (c,d),(c,d) \simeq (e,f)$ とすると, $ad = bc, cf = de$. このとき, $adcf = bcde$ だから, $af = be$ であり, $(a,b) \simeq (e,f)$. すなわち, $\simeq$ は推移的である.
以上から, $\simeq$ は同値関係である.

7.
- 直和分割
$\pi_1 = \{\{a\},\{b\},\{c\}\}$
$\pi_2 = \{\{a,b\},\{c\}\}$
$\pi_3 = \{\{a,c\},\{b\}\}$
$\pi_4 = \{\{b,c\},\{a\}\}$
$\pi_5 = \{\{a,b,c\}\}$
- 同値関係
$R_{\pi_1} = (\{a\} \times \{a\}) \cup (\{b\} \times \{b\}) \cup (\{c\} \times \{c\}) = \{(a,a),(b,b),(c,c)\}$
$R_{\pi_2} = (\{a,b\} \times \{a,b\}) \cup (\{c\} \times \{c\}) = \{(a,a),(a,b),(b,a),(b,b),(c,c)\}$
$R_{\pi_3} = (\{a,c\} \times \{a,c\}) \cup (\{b\} \times \{b\}) = \{(a,a),(a,c),(b,b),(c,a),(c,c)\}$
$R_{\pi_4} = (\{a\} \times \{a\}) \cup (\{b,c\} \times \{b,c\}) = \{(a,a),(b,b),(b,c),(c,b),(c,c)\}$
$R_{\pi_5} = \{a,b,c\} \times \{a,b,c\} = \{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\}$
- 任意の R_{π_i} $(i = 1,2,3,4,5)$ に対して, $R_{\pi_1} \subseteq R_{\pi_i}$ だから, 最も細かい分割は π_1 である.
任意の R_{π_i} $(i = 1,2,3,4,5)$ に対して, $R_{\pi_i} \subseteq R_{\pi_5}$ だから, 最も粗い分割は π_5 である.

8. $\{\{1\},\{2,3,4\}\}$
$\{\{1\},\{2\},\{3,4\}\}$
$\{\{1\},\{3\},\{2,4\}\}$
$\{\{1\},\{4\},\{2,3\}\}$
$\{\{1\},\{2\},\{3\},\{4\}\}$

9. (1) $\displaystyle\bigcup_{X \in \pi} X^2 = (\{a,c\} \times \{a,c\}) \cup (\{b\} \times \{b\}) = \{(a,a),(a,c),(c,a),(c,c),(b,b)\}$.

(2) $\displaystyle R = \bigcup_{X \in \pi} X^2$ だから, (1) より, $[a]_R = \{x \mid (a,x) \in R\} = \{a,c\}$.

(3) $\pi_{\max} = \{\{a,b,c\}\}$.
$\pi_{\min} = \{\{a\},\{b\},\{c\}\}$.

(4) $\displaystyle R_{\max} = \bigcup_{X \in \pi_{\max}} X^2 = (\{a,b,c\} \times \{a,b,c\})$
$= \{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\}$.
$\displaystyle R_{\min} = \bigcup_{X \in \pi_{\min}} X^2 = (\{a\} \times \{a\}) \cup (\{b\} \times \{b\}) \cup (\{c\} \times \{c\})$
$= \{(a,a),(b,b),(c,c)\}$.

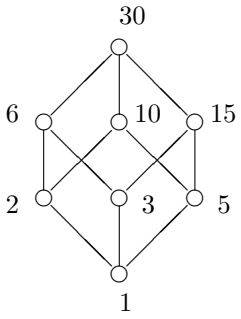
10. $R \circ S$ は同値関係であるとする.
任意の $(x,y) \in R \circ S$ に対して, $R \circ S$ は対称的だから, $(y,x) \in R \circ S$. ゆえに, ある $z \in A$ が存在して, $(y,z) \in S$, $(z,x) \in R$. R,S は対称的だから, $(z,y) \in S$, $(x,z) \in R$. ゆえに, $(x,y) \in S \circ R$.
したがって, $R \circ S \subseteq S \circ R$.
一方, 任意の $(x,y) \in S \circ R$ に対して, ある $z \in A$ が存在して, $(x,z) \in R$, $(z,y) \in S$. R,S は対称的だから, $(z,x) \in R$, $(y,z) \in S$. ゆえに, $(y,x) \in R \circ S$. $R \circ S$ は対称的だから, $(x,y) \in R \circ S$. したがって, $S \circ R \subseteq R \circ S$.
以上から, $R \circ S = S \circ R$.

離散数学演習 5　解答例

1. (1) R は反射的，反対称的，かつ推移的である．
   (2) $(x, y) \in R$ または $(y, x) \in R$.
   (3) R は A 上の半順序であり, かつ, 任意の $x, y \in A$ に対して, x と y は比較可能である．
   (4) $a \leq x$ かつ $a \neq x$ となる $x \in B$ は存在しない．
   (5) $x \leq a$ かつ $a \neq x$ となる $x \in B$ は存在しない．
   (6) 任意の $x \in B$ に対して, $x \leq a$.
   (7) 任意の $x \in B$ に対して, $a \leq x$.
   (8) 任意の $x \in B$ に対して, $x \leq a$.
   (9) a は B の上界であり, かつ, B の任意の上界 x に対して, $a \leq x$.
   (10) 任意の $x \in B$ に対して, $a \leq x$.
   (11) a は B の下界であり, かつ, B の任意の下界 x に対して, $x \leq a$.
2. (1) $R = \{(1,1),(1,2),(1,3),(1,5),(1,6),(1,10),(1,15),(1,30),\ (2,2),(2,6),(2,10),(2,30),$
   $(3,3),(3,6),(3,15),(3,30),\ (5,5),(5,10),(5,15),(5,30),(6,6),(6,30),\ (10,10),(10,30),$
   $(15,15),(15,30),(30,30)\}$
   (2) $(1,1),(2,2),(3,3),(5,5),(6,6),(10,10),(15,15),\ (30,30) \in R$ だから, R は反射的である．
   $(1,2) \in R$ に対して, $(2,1) \notin R$.
   $(1,3) \in R$ に対して, $(3,1) \notin R$.
   $(1,5) \in R$ に対して, $(5,1) \notin R$.
   $(1,6) \in R$ に対して, $(6,1) \notin R$.
   $(1,10) \in R$ に対して, $(10,1) \notin R$.
   $(1,15) \in R$ に対して, $(15,1) \notin R$.
   $(1,30) \in R$ に対して, $(30,1) \notin R$.
   $(2,6) \in R$ に対して, $(6,2) \notin R$.
   $(2,10) \in R$ に対して, $(10,2) \notin R$.
   $(2,30) \in R$ に対して, $(30,2) \notin R$.
   $(3,6) \in R$ に対して, $(6,3) \notin R$.
   $(3,15) \in R$ に対して, $(15,3) \notin R$.
   $(3,30) \in R$ に対して, $(30,3) \notin R$.
   $(5,10) \in R$ に対して, $(10,5) \notin R$.
   $(5,15) \in R$ に対して, $(15,5) \notin R$.
   $(5,30) \in R$ に対して, $(30,5) \notin R$.
   $(6,30) \in R$ に対して, $(30,6) \notin R$.
   $(10,30) \in R$ に対して, $(30,10) \notin R$.
   $(15,30) \in R$ に対して, $(30,15) \notin R$.
   以上から, R は反対称的である．
   $(1,1),(1,1) \in R$ に対して, $(1,1) \in R$.
   $(1,1),(1,2) \in R$ に対して, $(1,2) \in R$.
   $(1,1),(1,3) \in R$ に対して, $(1,3) \in R$.
   $(1,1),(1,5) \in R$ に対して, $(1,5) \in R$.
   $(1,1),(1,6) \in R$ に対して, $(1,6) \in R$.
   $(1,1),(1,10) \in R$ に対して, $(1,10) \in R$.
   $(1,2),(2,2) \in R$ に対して, $(1,2) \in R$.
   $(1,2),(2,6) \in R$ に対して, $(1,6) \in R$.
   $(1,2),(2,10) \in R$ に対して, $(1,10) \in R$.
   $(1,2),(2,30) \in R$ に対して, $(1,30) \in R$.
   $(1,3),(3,3) \in R$ に対して, $(1,3) \in R$.
   $(1,3),(3,6) \in R$ に対して, $(1,6) \in R$.
   $(1,3),(3,15) \in R$ に対して, $(1,15) \in R$.
   $(1,3),(3,30) \in R$ に対して, $(1,30) \in R$.
   $(1,5),(5,5) \in R$ に対して, $(1,5) \in R$.
   $(1,5),(5,10) \in R$ に対して, $(1,10) \in R$.

$(1,5),(5,15) \in R$ に対して, $(1,15) \in R$.
$(1,5),(5,30) \in R$ に対して, $(1,30) \in R$.
$(1,6),(6,6) \in R$ に対して, $(1,6) \in R$.
$(1,6),(6,30) \in R$ に対して, $(1,30) \in R$.
$(1,10),(10,10) \in R$ に対して, $(1,10) \in R$.
$(1,10),(10,30) \in R$ に対して, $(1,30) \in R$.
$(1,15),(15,15) \in R$ に対して, $(1,15) \in R$.
$(1,15),(15,30) \in R$ に対して, $(1,30) \in R$.
$(1,30),(30,30) \in R$ に対して, $(1,30) \in R$.
$(2,2),(2,2) \in R$ に対して, $(2,2) \in R$.
$(2,2),(2,6) \in R$ に対して, $(2,6) \in R$.
$(2,2),(2,10) \in R$ に対して, $(2,10) \in R$.
$(2,2),(2,30) \in R$ に対して, $(2,30) \in R$.
$(2,6),(6,6) \in R$ に対して, $(2,6) \in R$.
$(2,6),(6,30) \in R$ に対して, $(2,30) \in R$.
$(2,10),(10,10) \in R$ に対して, $(2,10) \in R$.
$(2,10),(10,30) \in R$ に対して, $(2,30) \in R$.
$(2,30),(30,30) \in R$ に対して, $(2,30) \in R$.
$(3,3),(3,3) \in R$ に対して, $(3,3) \in R$.
$(3,3),(3,6) \in R$ に対して, $(3,6) \in R$.
$(3,3),(3,15) \in R$ に対して, $(3,15) \in R$.
$(3,3),(3,30) \in R$ に対して, $(3,30) \in R$.
$(3,6),(6,6) \in R$ に対して, $(3,6) \in R$.
$(3,6),(6,30) \in R$ に対して, $(3,30) \in R$.
$(3,10),(10,10) \in R$ に対して, $(3,10) \in R$.
$(3,10),(10,30) \in R$ に対して, $(3,30) \in R$.
$(3,15),(15,15) \in R$ に対して, $(3,15) \in R$.
$(3,15),(15,30) \in R$ に対して, $(3,30) \in R$.
$(3,30),(30,30) \in R$ に対して, $(3,30) \in R$.
$(5,5),(5,5) \in R$ に対して, $(5,5) \in R$.
$(5,5),(5,10) \in R$ に対して, $(5,10) \in R$.
$(5,5),(5,15) \in R$ に対して, $(5,15) \in R$.
$(5,5),(5,30) \in R$ に対して, $(5,30) \in R$.
$(5,10),(10,10) \in R$ に対して, $(5,10) \in R$.
$(5,10),(10,30) \in R$ に対して, $(5,30) \in R$.
$(5,15),(15,15) \in R$ に対して, $(5,15) \in R$.
$(5,15),(15,30) \in R$ に対して, $(5,30) \in R$.
$(5,30),(30,30) \in R$ に対して, $(5,30) \in R$.
$(6,6),(6,6) \in R$ に対して, $(6,6) \in R$.
$(6,6),(6,30) \in R$ に対して, $(6,30) \in R$.
$(6,30),(30,30) \in R$ に対して, $(6,30) \in R$.
$(10,10),(10,10) \in R$ に対して, $(10,10) \in R$.
$(10,30),(30,30) \in R$ に対して, $(10,30) \in R$.
$(15,15),(15,15) \in R$ に対して, $(15,15) \in R$.
$(15,15),(15,30) \in R$ に対して, $(15,30) \in R$.
$(15,30),(30,30) \in R$ に対して, $(15,30) \in R$.
$(30,30),(30,30) \in R$ に対して, $(30,30) \in R$.
以上から, R は推移的である.

(3)



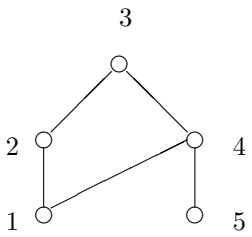
(4) $30Rx, x \neq 30$ となる $x \in A$ は存在しないから, A の極大元は 30 である.
$xR1, x \neq 1$ となる $x \in A$ は存在しないから, A の極小元は 1 である.
$1R30, 2R30, 3R30, 5R30, 6R30, 10R30, 15R30, 30R30$ だから, A の最大元は 30 である.
$1R1, 1R2, 1R3, 1R5, 1R6, 1R10, 1R15, 1R30$ だから, A の最小元は 1 である.

(5) $(2,3) \notin R$, $(3,2) \notin R$ だから, 2 と 3 は比較可能ではない. ゆえに, R は全順序ではない.

3. (1) $R = \{(3,3),(3,2),(3,1),(3,4),(3,5),\ (2,2),(2,1),(1,1),(4,4),(4,1),\ (4,5),(5,5)\}$

(2) $1 \leq x, x \neq 1$ となる $x \in A$ は存在しない.
$5 \leq x, x \neq 5$ となる $x \in A$ は存在しない.
ゆえに, A の極大元は 1, 5 である.
$x \leq 3, x \neq 3$ となる $x \in A$ は存在しない.
ゆえに, A の極小元は 3 である.

(3)



4. (図略)
$\mathcal{P}(A)$=$\{\phi, \{a\}, \{b\}, \{c\}, \{d\}, \{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\}, \{c,d\}, \{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}, \{a,b,c,d\}\ \}$

5. 任意の $x \in Z$ に対して, $x = x^1$ だから, $(x,x) \in R$. すなわち, R は反射的である.
任意の $x, y \in Z$ に対して, $(x,y), (y,x) \in R$ とすると, 正の整数 r_1, r_2 が存在して, $y = x^{r_1}$, $x = y^{r_2}$.
このとき, $x = (x^{r_1})^{r_2} = x^{r_1 r_2}$ だから, $r_1 r_2 = 1$. $r_1 r_2$ は正の整数だから, $r_1 = r_2 = 1$. ゆえに, $x = y$ だから, R は反対称的である.
任意の $x, y, z \in Z$ に対して, $(x,y), (y,z) \in R$ とすると, 正の整数 r_1, r_2 が存在して, $y = x^{r_1}$, $z = y^{r_2}$.
このとき, $z = x^{r_1 r_2}$. $r_1 r_2$ は正の整数だから, $(x,z) \in R$. すなわち, R は推移的である.
以上から, R は半順序である.
(反対称性に関する別証明) 任意の $x, y \in Z (x \neq y)$ に対して, $(x,y) \in R$ とすると, 正の整数 r が存在して, $y = x^r$ $(r \neq 1)$. このとき, $x = y^{\frac{1}{r}}$. $\dfrac{1}{r}$ は正の整数でないので, $(y,x) \notin R$. すなわち, R は反対称的である.

6. B の最大元は唯一でないと仮定する. そこで, 最大元が 2 つあるとして, それらを $b_1, b_2 \in B$ とする.
このとき, b_1 は最大元だから, $(b_2, b_1) \in R$. また, b_2 は最大元だから, $(b_1, b_2) \in R$. R は反対称的だから, $b_1 = b_2$. すなわち, B の最大元は唯一である.
最小元の唯一性も同様に示せる.

7. $a \neq b$ とする.
$\leq$ は全順序だから, $a \leq b$ または $b \leq a$.
$a \leq b$ のとき, b が極小元であることに矛盾する. $b \leq a$ のとき, a が極小元であることに矛盾する.
ゆえに, $a = b$.

8. $2R1, 3R1, 4R1$.
$2R2, 3R2, 4R2$.
ゆえに, B の上界は 1, 2 である.
$5R2, 5R3, 5R4$.
$6R2, 6R3, 6R4$.
ゆえに, B の下界は 5, 6 である.
B の上界 1, 2 に対して, $2R1, 2R2$ だから, B の上限は 2 である.
B の下界 5, 6 に対して, $5Rx, 6Rx$ となる $x \in \{5, 6\}$ は存在しないので, B の下限は存在しない.

9. B: $3R1, 5R1$.
$3R2, 5R2$.
$3R3, 5R3$.
ゆえに, B の上界は 1,2,3 である.
$5R3, 5R5$.
$6R3, 6R5$.
$7R3, 7R5$.
$8R3, 7R5$.
ゆえに, B の下界は 5,6,7,8 である.
B の上界 1,2,3 に対して, $3R1, 3R2, 3R3$ だから, B の上限は 3 である.
B の下界 5,6,7,8 に対して, $5R5, 6R5, 6R5, 8R5$ だから, B の下限は 5 である.

C: $6R1, 8R1$.
$6R2, 8R2$.
$6R3, 8R3$.
$6R4, 8R4$.
$6R5, 8R5$.
$6R6, 8R6$.
ゆえに, C の上界は 1,2,3,4,5,6 である.
$6R8, 8R8$.
ゆえに, C の下界は 8 である.
C の上界 1,2,3,4,5,6 に対して, $6R1, 6R2, 6R3, 6R4, 6R5, 6R6$ だから, C の上限は 6 である.
C の下界 8 に対して, $8R8$ だから, C の下限は 8 である.

D: $2R2, 3R2, 6R2$
ゆえに, D の上界は 2 である.
$6R2, 6R3, 6R6$.
$8R2, 8R3, 8R6$.
ゆえに, D の下界は 6,8 である.
D の上界 2 に対して, $2R2$ だから, D の上限は 2 である.
D の下界 6,8 に対して, $6R6, 8R6$ だから, D の下限は 6 である.

E: $4R1, 5R1, 6R1$.
$4R2, 5R2, 6R2$.
$4R3, 5R3, 6R3$.
ゆえに, E の上界は 1,2,3 である.
$6R4, 6R5, 6R6$.
$8R4, 8R5, 8R6$.
ゆえに, E の下界は 6,8 である.
E の上界 1,2,3 に対して, $3R1, 3R2, 3R3$ だから, E の上限は 3 である.
E の下界 6,8 に対して, $6R6, 8R6$ だから, E の下限は 6 である.

F: $4R1, 5R1, 7R1$.
$4R2, 5R2, 7R2$.
$4R3, 5R3, 7R3$.
ゆえに, F の上界は 1,2,3 である.
$8R4, 8R5, 8R7$

ゆえに, F の下界は 8 である.
F の上界 1,2,3 に対して, $3R1, 3R2, 3R3$ だから, F の上限は 3 である.
F の下界 8 に対して, $8R8$ だから, F の下限は 8 である.

G: $1Rx, 2Rx, 4Rx, 7Rx$ となる $x \in A$ は存在しないから, G の上界は存在しない.
$8R1, 8R2, 8R4, 8R7$.
ゆえに, G の下界は 8 である.
G の上界は存在しないから, G の上限も存在しない.
G の下界 8 に対して, $8R8$ だから, G の下限は 8 である.

10. 任意の $(a,b) \in M^2$ に対して, a で割り切れる $c \in M$ $(a \neq c)$ と b 以上である $d \in M$ $(b \neq d)$ は必ず存在する. ゆえに, $(a,b) \leq (c,d), (a,b) \neq (c,d)$ となる $(c,d) \in M^2$ は必ず存在する. ゆえに, M^2 の極大元は存在しない.
また, $(a,b) \in M^2$ に対して, $(a,b) \leq (p,2)$ (ただし, p は素数) であるとき, $a = p$ かつ $b = 2$. ゆえに, $(a,b) \leq (p,2), (a,b) \neq (p,2)$ となる $(a,b) \in M^2$ は存在しない. ゆえに, $(p,2)$ は M^2 の極小元である.

11. (1) R は反射的だから, 任意の $x \in A$ に対して, xRx. このとき, $x \equiv x$ だから, $\equiv$ は反射的である.
任意の $x, y \in A$ に対して, $x \equiv y$ とする. このとき, xRy かつ yRx だから, yRx かつ xRy. ゆえに, $y \equiv x$. したがって, $\equiv$ は対称的である.
任意の $x, y, z \in A$ に対して, $x \equiv y$, $y \equiv z$ とする. このとき, xRy かつ yRx, yRz かつ zRy. R は推移的だから, xRz かつ zRx. ゆえに, $x \equiv z$. したがって, $\equiv$ は推移的である.
以上から, $\equiv$ は同値関係である.

(2) 任意の $[x]_{\equiv} \in A/\equiv$ に対して, $x \in A$. R は反射的だから, xRx. ゆえに, $[x]_{\equiv} \leq [x]_{\equiv}$ だから, $\leq$ は反射的である.
任意の $[x]_{\equiv}, [y]_{\equiv} \in A/\equiv$ に対して, $[x]_{\equiv} \leq [y]_{\equiv}$ かつ $[y]_{\equiv} \leq [x]_{\equiv}$ とする. このとき, xRy かつ yRx だから, $x \equiv y$. ゆえに, $[x]_{\equiv} = [y]_{\equiv}$ だから, $\leq$ は反対称的である.
任意の $[x]_{\equiv}, [y]_{\equiv}, [z]_{\equiv} \in A/\equiv$ に対して, $[x]_{\equiv} \leq [y]_{\equiv}$ かつ $[y]_{\equiv} \leq [z]_{\equiv}$ とする. このとき, xRy かつ yRz. R は推移的だから, xRz. ゆえに, $[x]_{\equiv} \leq [z]_{\equiv}$ だから, $\leq$ は推移的である.
以上から, $\leq$ は半順序である.

12. (1) S が $\mathcal{A}$ の上界であることと, (2) $\mathcal{A}$ の任意の上界 B に対して, $S \subseteq B$ であること（最小上界であること）を示せばよい.
(1) 任意の $X \in \mathcal{A}$ に対して, 明らかに $X \subseteq \bigcup_{X \in \mathcal{A}} X = S$. ゆえに, S は $\mathcal{A}$ の上界である.
(2) 任意の $x \in A$ に対して, $x \in S = \bigcup_{X \in \mathcal{A}} X$ とする. このとき, ある $X \in \mathcal{A}$ が存在して, $x \in X$. ここで, B を $\mathcal{A}$ の任意の上界とすると, $X \subseteq B$. ゆえに, $x \in B$. すなわち, $S \subseteq B$.

離散数学演習 6　解答例

1. (1) A の任意の部分集合 B に対して, B の上限と下限が存在する.
   (2) L の任意の有限部分集合 B に対して, B の上限と下限が存在する.
   (3) $\{a,b\}$ の上限
   (4) $\{a,b\}$ の下限

2. (1)

$+$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	1	2	1	1	2	1	2
3	1	1	3	1	1	3	3
4	1	1	1	4	4	4	4
5	1	2	1	4	5	4	5
6	1	1	3	4	4	6	6
7	1	2	3	4	5	6	7

$\cdot$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	2	7	5	5	7	7
3	3	7	3	6	7	6	7
4	4	5	6	4	5	6	7
5	5	5	7	5	5	7	7
6	6	7	6	6	7	6	7
7	7	7	7	7	7	7	7

上表から, 任意の 2 つの要素に対して上限と下限が存在するので, 与えられた半順序集合は束である.

   (2)

$+$	1	2	3	4	5	6
1	1	1	1	1	1	1
2	1	2	1	2	2	2
3	1	1	3	1	3	3
4	1	2	1	4	2	4
5	1	2	3	2	5	5
6	1	2	3	4	5	6

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	2	5	4	5	6
3	3	5	3	6	5	6
4	4	4	6	4	6	6
5	5	5	5	6	5	6
6	6	6	6	6	6	6

上表から, 任意の 2 つの要素に対して上限と下限が存在するので, 与えられた半順序集合は束である.

3. (1) $X,Y \in \mathcal{P}(A)$ だから，$X \cup Y \in \mathcal{P}(A)$. また，$X \subseteq X \cup Y$，$Y \subseteq X \cup Y$ だから，$X \cup Y$ は $\{X,Y\}$ の上界である.
   $\{X,Y\}$ の任意の上界を Z とすると，$X \subseteq Z$，$Y \subseteq Z$. このとき，$X \cup Y \subseteq Z$. すなわち，$X \cup Y$ は $\{X,Y\}$ の最小上界，すなわち上限である.
   一方，$X,Y \in \mathcal{P}(A)$ だから，$X \cap Y \in \mathcal{P}(A)$. また，$X \cap Y \subseteq X$，$X \cap Y \subseteq Y$ だから，$X \cap Y$ は $\{X,Y\}$ の下界である.
   $\{X,Y\}$ の任意の下界を Z とすると，$Z \subseteq X$，$Z \subseteq Y$. このとき，$Z \subseteq X \cap Y$. すなわち，$X \cap Y$ は $\{X,Y\}$ の最大下界，すなわち下限である.
   (2) (1) から，任意の $X,Y \in \mathcal{P}(A)$ に対して，$\sup\{X,Y\}$ と $\inf\{X,Y\}$ が存在するので，$(\mathcal{P}(A),\subseteq)$ は束である.

4. (1) $b+c$ は $\{a,c\}$ の上界であることを示す.
   明らかに, $b \le b+c$. $a \le b$ で, $\le$ は推移的であるから, $a \le b+c$.
   一方, 明らかに, $c \le b+c$.
   ゆえに, $b+c$ は $\{a,c\}$ の上界である.
   ところが, $a+c$ は $\{a,c\}$ の上限であるから, $a+c \le b+c$.
   同様に, $a \cdot c \le b \cdot c$ を示すことができる.
   (2) $b+d$ は $\{a,c\}$ の上界であることを示す.
   明らかに, $b \le b+d$, $d \le b+d$. $a \le b$ で, $\le$ は推移的であるから, $a \le b+d$. また, $c \le d$ で, $\le$ は推移的であるから, $c \le b+d$. ゆえに, $b+d$ は $\{a,c\}$ の上界である.
   ところが, $a+c$ は $\{a,c\}$ の上限だから, $a+c \le b+d$.
   同様に, $a \cdot c \le b \cdot d$ を示すことができる.
   (3) $(a \cdot b)+c$ は $\{a,b+c\}$ の下界であることを示す.
   明らかに, $a \cdot b \le a$. また, $c \le a$ だから, a は $\{a \cdot b, c\}$ の上界であり, $(a \cdot b)+c \le a$.
   一方, 明らかに, $c \le b+c$. また, $a \cdot b \le b \le b+c$. ゆえに, $b+c$ は $\{a \cdot b, c\}$ の上界であり, $(a \cdot b)+c \le b+c$.
   以上から, $(a \cdot b)+c$ は $\{a, b+c\}$ の下界である.
   ところが, $a \cdot (b+c)$ は $\{a,b+c\}$ の下限であるから, $(a \cdot b)+c \le a \cdot (b+c)$.

(4) $(a\cdot b)+(a\cdot c)$ は $\{a, b+c\}$ の下界であることを示す.
明らかに, $a\cdot b\le a, a\cdot c\le a$. ゆえに, a は $\{a\cdot b, a\cdot c\}$ の上界であり, $(a\cdot b)+(a\cdot c)\le a$.
一方, $a\cdot b\le b\le b+c$, $a\cdot c\le c\le b+c$. ゆえに, $b+c$ は $\{a\cdot b, a\cdot c\}$ の上界であり, $(a\cdot b)+(a\cdot c)\le b+c$.
以上から, $(a\cdot b)+(a\cdot c)$ は $\{a, b+c\}$ の下界である.
ところが, $a\cdot(b+c)$ は $\{a, b+c\}$ の下限であるから, $(a\cdot b)+(a\cdot c)\le a\cdot(b+c)$.

(5) $a+(b\cdot c)$ は $\{a+b, a+c\}$ の下界であることを示す.
明らかに, $a\le a+b$. また, $b\cdot c\le b\le a+b$. ゆえに, $a+b$ は $\{a, b\cdot c\}$ の上界であり, $a+(b\cdot c)\le a+b$.
一方, 明らかに, $a\le a+c$. また, $b\cdot c\le c\le a+c$. ゆえに, $a+c$ は $\{a, b\cdot c\}$ の上界であり, $a+(b\cdot c)\le a+c$.
以上から, $a+(b\cdot c)$ は $\{a+b, a+c\}$ の下界である.
ところが, $(a+b)\cdot(a+c)$ は $\{a+b, a+c\}$ の下限であるから, $a+(b\cdot c)\le(a+b)\cdot(a+c)$.

5. (1) $a+(b+c)=u$ とおく.
まず, u が $\{a+b, c\}$ の上界であることを示す.
u は $\{a, b+c\}$ の上限だから, $a\le u, b+c\le u$. $b+c\le u$ だから, $b\le u, c\le u$. ゆえに, u は $\{a, b\}$ の上界であり, $a+b\le u$. したがって, u は $\{a+b, c\}$ の上界でもある.
次に, u が $\{a+b, c\}$ の上限であることを示す.
そこで, u' を $\{a+b, c\}$ の任意の上界とする. このとき, $a\le u', b\le u', c\le u'$. ゆえに, u' は $\{b, c\}$ の上界であり, $b+c\le u'$. したがって, u' は $\{a, b+c\}$ の上界でもある. ところが, u は $\{a, b+c\}$ の上限だから, $u\le u'$. ゆえに, u は $\{a+b, c\}$ の最小上界, すなわち, 上限であり, $u=(a+b)+c$. 結局, $a+(b+c)=(a+b)+c$.
同様に, $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ も示すことができる.

(2) 明らかに, $a\cdot b\le a$. このとき, $(a\cdot b)+a=a$. ゆえに, $a+(a\cdot b)=a$.
また, 明らかに, $a\le a+b$. このとき, $a\cdot(a+b)=a$.

(3) $+, \cdot$ の定義から明らか.

6. (2) が成り立つとする. このとき,

$a+a$	$=$	$a+(a\cdot(a+b))$	(吸収則)
	$=$	a	(吸収則)
$a\cdot a$	$=$	$a\cdot(a+(a\cdot b))$	(吸収則)
	$=$	a	(吸収則)

となるから, (3) が成り立つ.

7. (1) が成り立つとする. このとき,

$(a+b)\cdot(a+c)$	$=$	$((a+b)\cdot a)+((a+b)\cdot c))$	((1))
	$=$	$(a\cdot(a+b))+((a+b)\cdot c))$	(交換則)
	$=$	$a+((a+b)\cdot c))$	(吸収則)
	$=$	$a+(c\cdot(a+b))$	(交換則)
	$=$	$a+((c\cdot a)+(c\cdot b))$	((1))
	$=$	$a+((a\cdot c)+(b\cdot c))$	(交換則)
	$=$	$(a+(a\cdot c))+(b\cdot c)$	(結合則)
	$=$	$a+(b\cdot c)$	(吸収則)

となるから, (2) が成り立つ.
同様に, (2) が成り立つならば, (1) が成り立つことを示せる.
ゆえに, (1) と (2) は互いに同値である.

離散数学演習７　解答例

1. (1) $f \subseteq A \times B$, かつ, 任意の $x \in A$ に対して, $y \in B$ が唯一存在して, $(x, y) \in f$.
   (2) $(a, b) \in f$ であるような $b \in B$
   (3) $b = f(a)$ であるような $a \in A$
   (4) $\{f(x) \mid x \in X\}$
   (5) $\{x \mid f(x) \in Y\}$
   (6) $\{x \in A \mid$ ある $y \in B$ に対して, $y = f(x)\}$
   (7) $\{y \in B \mid$ ある $x \in A$ に対して, $y = f(x)\}$
   （別解）$\{f(x) \mid x \in A\}$, $f(A)$
   (8) 任意の $y \in B$ に対して, ある $x \in A$ が存在して, $y = f(x)$.
   (9) 任意の $x_1, x_2 \in A$ に対して, $x_1 \neq x_2$ ならば $f(x_1) \neq f(x_2)$.
   （別解）任意の $x_1, x_2 \in A$ に対して, $f(x_1) = f(x_2)$ ならば $x_1 = x_2$.
   (10) f は全射かつ単射である.
   (11) f は有限集合上の全単射である.
   (12) 任意の $x \in A$ に対して, $I_A(x) = x$.
   (13) 任意の $x \in A$ に対して, $(g \circ f)(x) = g(f(x))$.
   (14) $g \circ f = I_A$ かつ $f \circ g = I_B$.
   (15) $\{f \mid f : A \to B\}$
   (16) $f : A \to \{0, 1\}$

2. $(2, 3), (2, 1) \in R$ であり, $(2, x) \in R$ となる $x \in A$ は唯一でないから, R は関数ではない.
   $(2, y) \in S$ となる $y \in A$ が存在しないので, S は関数ではない.
   任意の $x \in A$ に対して, $(x, y) \in T$ となる $y \in A$ が唯一存在するので, T は関数である.

3. (1) (a) $f \circ g = \{(a, a), (b, d), (c, b), (d, a)\}$ [1]
   (b) $h \circ f = \{(a, c), (b, a), (c, a), (d, c)\}$
   (c) $g \circ g = \{(a, d), (b, c), (c, b), (d, a)\}$
   (2) $a \in A$ に対して, $(a, c), (a, b) \in f^{-1}$ だから, f^{-1} は関数ではない.
   $g^{-1} = \{(b, a), (d, b), (a, c), (c, d)\}$ であり, 任意の $x \in A$ に対して, $(x, y) \in g^{-1}$ となる $y \in A$ は唯一である. ゆえに, g^{-1} は関数である.
   $x \in A$ に対して, $(c, b), (c, d) \in h^{-1}$ だから, h^{-1} は関数ではない.
   (3) $b, c \in A$ に対して, $f(b) = f(c)$ だから, f は単射ではない.
   $A = \{a, b, c, d\}$ であって, $g(a), g(b), g(c), g(d)$ は互いに異なるから, g は単射である.
   $a, c \in A$ に対して, $h(a) = h(c)$ だから, h は単射ではない.
   $(x, c) \in f$ となる $x \in A$ は存在しないから, f は全射ではない.
   任意の $y \in A$ に対して, $(x, y) \in g$ となる $x \in A$ が存在するから, g は全射である.
   $(x, b) \in h$ となる $x \in A$ は存在しないから, h は全射ではない.

4. $B^A = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9\}$. ただし,

$f_1 = \{(a, 1), (b, 1)\}$,	$f_4 = \{(a, 2), (b, 1)\}$,	$f_7 = \{(a, 3), (b, 1)\}$,
$f_2 = \{(a, 1), (b, 2)\}$,	$f_5 = \{(a, 2), (b, 2)\}$,	$f_8 = \{(a, 3), (b, 2)\}$,
$f_3 = \{(a, 1), (b, 3)\}$,	$f_6 = \{(a, 2), (b, 3)\}$,	$f_9 = \{(a, 3), (b, 3)\}$.

5. 任意の $x_1, x_2 \in A$ に対して, $f(x_1) = f(x_2)$ とする. このとき, $g(f(x_1)) = g(f(x_2))$. $g(f(x_1)) = (g \circ f)(x_1) = I_A(x_1) = x_1$, $g(f(x_2)) = (g \circ f)(x_2) = I_A(x_2) = x_2$ だから, $x_1 = x_2$. ゆえに, f は単射である.
   一方, 任意の $x \in A$ に対して, $g(f(x)) = (g \circ f)(y) = I_A(y) = y$. $f(x) = y$ とおくと, $y \in B$ であり, $g(y) = x$. ゆえに, g は全射である.

---

[1] $f \circ g = \begin{bmatrix} a & b & c & d \\ a & d & b & a \end{bmatrix}$ などと書いてもよい.

6. (1) g は全射だから, 任意の $z \in C$ に対して, ある $y \in B$ が存在して, $g(y) = z$. また, f は全射だから, $y \in B$ に対して, ある $x \in A$ が存在して, $f(x) = y$. すなわち, 任意の $z \in C$ に対して, ある $x \in A$ が存在して, $(g \circ f)(x) = g(f(x)) = z$ だから, $g \circ f$ は全射である.

(2) 任意の $x_1, x_2 \in A$ に対して, $(g \circ f)(x_1) = (g \circ f)(x_2)$ とする. このとき, $g(f(x_1)) = g(f(x_2))$. g は単射だから, $f(x_1) = f(x_2)$. さらに, f は単射だから, $x_1 = x_2$. ゆえに, $g \circ f$ は単射である.

(3) $g \circ f : A \to C$ は全射だから, 任意の $z \in C$ に対して, ある $x \in A$ が存在して, $(g \circ f)(x) = z$. このとき, $(g \circ f)(x) = g(f(x))$ だから, $f(x) = y$ $(\in B)$ とおくと, 任意の $z \in C$ に対して, ある $y \in B$ が存在して, $g(y) = z$. すなわち, g は全射である.

(4) 任意の $x_1, x_2 \in A$ に対して, $f(x_1) = f(x_2)$ とする. このとき, $g(f(x_1)) = g(f(x_2))$. ゆえに, $(g \circ f)(x_1) = (g \circ f)(x_2)$. これは $g \circ f$ は単射だから, $x_1 = x_2$. したがって, f は単射である.

7. (1) 任意の $y \in f(A)$ に対して, ある $x_1, x_2 \in A (x_1 \neq x_2)$ が存在して, $(y, x_1), (y, x_2) \in f^{-1}$ と仮定する. このとき, $y = f(x_1) = f(x_2)$. f は単射だから, $x_1 = x_2$. これは矛盾. すなわち, 任意の $y \in f(A)$ に対して, $(y, x) \in f^{-1}$ となる $x \in A$ は唯一存在する. したがって, f^{-1} は $f(A)$ から A への関数である.
一方, 任意の $y_1, y_2 \in f(A)$ に対して, $f^{-1}(y_1) = f^{-1}(y_2)$ とする. $y_1 \in f(A)$ だから, ある $x_1 \in A$ が存在して, $f(x_1) = y_1$. すなわち, $f^{-1}(y_1) = x_1$. また, $y_2 \in f(A)$ だから, ある $x_2 \in A$ が存在して, $f(x_2) = y_2$. すなわち, $f^{-1}(y_2) = x_2$. ゆえに, $x_1 = x_2$. このとき, $f(x_1) = f(x_2)$ だから $y_1 = y_2$. ゆえに, f^{-1} は単射である.

(2) f は全射だから, $f(A) = B$. (1) により, f^{-1} は B から A への単射である.
一方, f は A から B への関数だから, 任意の $x \in A$ に対して, ある $y \in B$ が存在して, $y = f(x)$. すなわち, $f^{-1}(y) = x$. したがって, f^{-1} は全射である.

8. (1) 任意の $x \in X$ に対して, $f(x) \in f(X)$ だから, $x \in f^{-1}(f(X))$. ゆえに, $X_1 \subseteq f^{-1}(f(X))$.
$y \in f(f^{-1}(Y))$ とする. このとき, $x \in f^{-1}(Y)$ が存在して, $y = f(x)$. $x \in f^{-1}(Y)$ だから, $f(x) \in Y_1$. すなわち, $y \in Y$. ゆえに, $f(f^{-1}(Y)) \subseteq Y$.

(2) 任意の $y \in f(X_1)$ に対して, $x \in X_1$ が存在して, $y = f(x)$. $X_1 \subseteq X_2$ だから, $x \in X_2$. ゆえに, $f(x) \in f(X_2)$ であり, $y \in f(X_2)$. すなわち, $f(X_1) \subseteq f(X_2)$.
任意の $x \in f^{-1}(Y_1)$ に対して, $f(x) \in Y_1 \subseteq Y_2$. ゆえに, $x \in f^{-1}(Y_2)$. すなわち, $f^{-1}(Y_1) \subseteq f^{-1}(Y_2)$.

(3) 任意の $y \in f(X_1 \cup X_2)$ に対して, $x \in X_1 \cup X_2$ が存在して, $y = f(x)$. $x \in X_1 \cup X_2$ だから, $x \in X_1$ または $x \in X_2$. ゆえに, $f(x) \in f(X_1)$ または $f(x) \in f(X_2)$ だから, $y = f(x) \in f(X_1) \cup f(X_2)$. すなわち, $f(X_1 \cup X_2) \subseteq f(X_1) \cup f(X_2)$.
一方, 任意の $y \in f(X_1) \cup f(X_2)$ に対して, $y \in f(X_1)$ または $y \in f(X_2)$. $y \in f(X_1)$ のとき, $x_1 \in X_1$ が存在して, $y = f(x_1)$. $X_1 \subseteq X_1 \cup X_2$ だから, $x_1 \in X_1 \cup X_2$. ゆえに, $y = f(x_1) \in f(X_1 \cup X_2)$. $y \in f(X_2)$ のとき, $x_2 \in X_2$ が存在して, $y = f(x_2)$. $X_2 \subseteq X_1 \cup X_2$ だから, $x_2 \in X_1 \cup X_2$. ゆえに, $y = f(x_2) \in f(X_1 \cup X_2)$. いずれの場合も, $x \in X_1 \cup X_2$ が存在して, $y = f(x) \in f(X_1 \cup X_2)$. すなわち, $f(X_1) \cup f(X_2) \subseteq f(X_1 \cup X_2)$.
以上から, $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.
任意の $x \in f^{-1}(Y_1 \cup Y_2)$ に対して, $f(x) \in Y_1 \cup Y_2$ だから, $f(x) \in Y_1$ または $f(x) \in Y_2$. ゆえに, $x \in f^{-1}(Y_1)$ または $x \in f^{-1}(Y_2)$ だから, $x \in f^{-1}(Y_1) \cup f^{-1}(Y_2)$. すなわち, $f^{-1}(Y_1 \cup Y_2) \subseteq f^{-1}(Y_1) \cup f^{-1}(Y_2)$.
一方, 任意の $x \in f^{-1}(Y_1) \cup f^{-1}(Y_2)$ に対して, $x \in f^{-1}(Y_1)$ または $x \in f^{-1}(Y_2)$. ゆえに, $f(x) \in Y_1$ または $f(x) \in Y_2$ だから, $f(x) \in Y_1 \cup Y_2$ であり, $x \in f^{-1}(Y_1 \cup Y_2)$. すなわち, $f^{-1}(Y_1) \cup f^{-1}(Y_2) \subseteq f^{-1}(Y_1 \cup Y_2)$.
以上から, $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.

(4) 任意の $y \in f(X_1 \cap X_2)$ に対して, $x \in X_1 \cap X_2$ が存在して, $y = f(x)$. $x \in X_1 \cap X_2$ だから, $x \in X_1$ かつ $x \in X_2$. ゆえに, $f(x) \in f(X_1)$ かつ $f(x) \in f(X_2)$ だから, $y = f(x) \in f(X_1) \cap f(X_2)$. すなわち, $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$.
任意の $x \in f^{-1}(Y_1 \cap Y_2)$ に対して, $f(x) \in Y_1 \cap Y_2$ だから, $f(x) \in Y_1$ かつ $f(x) \in Y_2$. ゆえに, $x \in f^{-1}(Y_1)$ かつ $x \in f^{-1}(Y_2)$ だから, $x \in f^{-1}(Y_1) \cap f^{-1}(Y_2)$. すなわち, $f^{-1}(Y_1 \cap Y_2) \subseteq f^{-1}(Y_1) \cap f^{-1}(Y_2)$.
一方, 任意の $x \in f^{-1}(Y_1) \cap f^{-1}(Y_2)$ に対して, $x \in f^{-1}(Y_1)$ かつ $x \in f^{-1}(Y_2)$. ゆえに, $f(x) \in Y_1$ かつ $f(x) \in Y_2$ だから, $f(x) \in Y_1 \cap Y_2$ であり, $x \in f^{-1}(Y_1 \cap Y_2)$. すなわち, $f^{-1}(Y_1) \cap f^{-1}(Y_2) \subseteq f^{-1}(Y_1 \cap Y_2)$.
以上から, $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

(5) 任意の $y \in f(X_1) - f(X_2)$ に対して, $y \in f(X_1)$ かつ $y \notin f(X_2)$. $y \in f(X_1)$ だから, $x_1 \in X_1$ が存在して, $y = f(x_1)$. また, $y \notin f(X_2)$ だから, 任意の $x_2 \in X_2$ に対して, $y = f(x_2)$ とならない. ゆえに, $x_1 \in X_1 - X_2$ だから, $y = f(x_1) \in f(X_1 - X_2)$. すなわち, $f(X_1) - f(X_2) \subseteq f(X_1 - X_2)$.
任意の $x \in f^{-1}(Y_1 - Y_2)$ に対して, $f(x) \in Y_1 - Y_2$ だから, $f(x) \in Y_1$ かつ $f(x) \notin Y_2$. ゆえに, $x \in f^{-1}(Y_1)$ かつ $x \notin f^{-1}(Y_2)$ だから, $x \in f^{-1}(Y_1) - f^{-1}(Y_2)$. すなわち, $f^{-1}(Y_1 - Y_2) \subseteq f^{-1}(Y_1) - f^{-1}(Y_2)$.
一方, 任意の $x \in f^{-1}(Y_1) - f^{-1}(Y_2)$ に対して, $x \in f^{-1}(Y_1)$ かつ $x \notin f^{-1}(Y_2)$. ゆえに, $f(x) \in Y_1$ かつ $f(x) \notin Y_2$ だから, $f(x) \in Y_1 - Y_2$ であり, $x \in f^{-1}(Y_1 - Y_2)$. すなわち, $f^{-1}(Y_1) - f^{-1}(Y_2) \subseteq f^{-1}(Y_1 - Y_2)$.
以上から, $f^{-1}(Y_1 - Y_2) = f^{-1}(Y_1) - f^{-1}(Y_2)$.

離散数学演習８　解答例

1. 除法定理から, n, d に対して, 自然数の組 (q, r) が唯一に存在して, $n = qd + r$ $(0 \leq r < d)$ となる. そこで, $a_0 = r$ とおく.
   $q < n$ だから, 帰納法の仮定から, q に対して, 自然数の列 $a_1, \cdots, a_k$ （$0 \leq a_i < d$ $(i = 1, \cdots, k)$, $a_k \neq 0$）が唯一に存在して, $q = a_k d^{k-1} + a_{k-1} d^{k-2} + \cdots + a_2 d + a_1$.
   ゆえに, $n = qd + r = a_k d^k + a_{k-1} d^{k-1} + \cdots + a_2 d^2 + a_1 d + a_0$.

2. $m \mid n$ から、整数 q が存在して, $n = qm$. また, $k \mid l$ から, 整数 q' が存在して, $l = q'k$. ゆえに, $nl = qq'mk$. qq' は整数であるから, $mk \mid nl$.

3. (1)
$$\begin{aligned}
& \gcd(6188, 4709) \\
= \ & \gcd(4709, 1479) && 1479 = \mathrm{mod}\ (6188, 4709) \\
= \ & \gcd(1479, 272) && 272 = \mathrm{mod}\ (4709, 1479) \\
= \ & \gcd(272, 119) && 119 = \mathrm{mod}\ (1479, 272) \\
= \ & \gcd(119, 34) && 34 = \mathrm{mod}\ (272, 119) \\
= \ & \gcd(34, 17) && 17 = \mathrm{mod}\ (119, 34) \\
= \ & \gcd(17, 0) && 0 = \mathrm{mod}\ (34, 17) \\
= \ & 17
\end{aligned}$$

   (2)
$$\begin{aligned}
& \gcd(23843, 29041) \\
= \ & \gcd(29041, 23843) && 23843 = \mathrm{mod}\ (23843, 29041) \\
= \ & \gcd(23843, 5198) && 5198 = \mathrm{mod}\ (29041, 23843) \\
= \ & \gcd(5198, 3051) && 3051 = \mathrm{mod}\ (23843, 5198) \\
= \ & \gcd(3051, 2147) && 2147 = \mathrm{mod}\ (5198, 3051) \\
= \ & \gcd(2147, 904) && 904 = \mathrm{mod}\ (3051, 2147) \\
= \ & \gcd(904, 339) && 339 = \mathrm{mod}\ (2147, 904) \\
= \ & \gcd(339, 226) && 226 = \mathrm{mod}\ (904, 339) \\
= \ & \gcd(226, 113) && 113 = \mathrm{mod}\ (339, 226) \\
= \ & \gcd(113, 0) && 0 = \mathrm{mod}\ (226, 113) \\
= \ & 113
\end{aligned}$$

   (3)
$$\begin{aligned}
& \gcd(6825, -1485) \\
= \ & \gcd(-1485, 885) && 885 = \mathrm{mod}\ (6825, -1485) \\
= \ & \gcd(885, 285) && 285 = \mathrm{mod}\ (-1485, 885) \\
= \ & \gcd(285, 30) && 30 = \mathrm{mod}\ (885, 285) \\
= \ & \gcd(30, 15) && 15 = \mathrm{mod}\ (285, 30) \\
= \ & \gcd(15, 0) && 0 = \mathrm{mod}\ (30, 15) \\
= \ & 15
\end{aligned}$$

4. a', b' に正の公約数 $d' > 1$ が存在すると仮定する.
   このとき, 整数 q, r が存在して, $a' = d'q$, $b' = d'r$. ゆえに, $a = (d'q)d = (d'd)q$, $b = (d'r)d = (d'd)r$. したがって, $d'd$ は a, b の公約数である. $d \mid d'd$ だから, これは d が a, b の最大公約数であることに矛盾する.
   ゆえに, a', b' の正の公約数は 1 である. すなわち, a', b' は互いに素である.

5. (1) 整数 $m, km + n$ に対して, 整数 x, y が存在して, $\gcd(m, km + n) = mx + (km + n)y = (x + ky)m + yn$.
   また, $\gcd(m, n) \mid m$. $\gcd(m, n) \mid n$ だから, 任意の整数 a, b に対して, $\gcd(m, n) \mid am + bn$. 特に, 整数 $x + ky, y$ に対して, $\gcd(m, n) \mid (x + ky)m + yn$.
   ゆえに, $\gcd(m, n) \mid \gcd(m, km + n)$.
   一方, 整数 m, n に対して, 整数 x', y' が存在して,
   $\gcd(m, n) = mx' + ny' = (x' - y'k)m + y'(km + n)$.
   また, $\gcd(m, km + n) \mid m$, $\gcd(m, km + n) \mid km + n$ だから, 任意の整数 a, b に対して,
   $\gcd(m, km + n) \mid am + b(km + n)$.
   特に, 整数 $x' - y'k$, y' に対して, $\gcd(m, km + n) \mid (x' - y'k)m + y'(km + n)$.
   ゆえに, $\gcd(m, km + n) \mid \gcd(m, n)$.
   $\gcd(m, n) \mid \gcd(m, km + n)$, $\gcd(m, km + n) \mid \gcd(m, n)$ だから,
   $|\gcd(m, n)| = |\gcd(m, km + n)|$. $\gcd(m, n) \geq 0$, $\gcd(m, km + n) \geq 0$ だから,
   $\gcd(m, n) = \gcd(m, km + n)$.

（別解）
$m, km+n$ のすべての非負公約数からなる集合を $D_{m,km+n}$ とし, m, n のすべての非負公約数からなる集合を $D_{m,n}$ とする.
このとき, 任意の $d \in D_{m,km+n}$ に対して, $d \mid m$, $d \mid km+n$ だから, $d \mid (km+n) - k \cdot m$. $(km+n) - k \cdot m = n$ だから, $d \mid n$. ゆえに, $d \in D_{m,n}$. すなわち, $D_{m,km+n} \subseteq D_{m,n}$.
一方, 任意の $d \in D_{m,n}$ に対して, $d \mid m$, $d \mid n$ だから, $d \mid k \cdot m + n$. ゆえに, $d \in D_{m,km+n}$. すなわち, $D_{m,n} \subseteq D_{m,km+n}$.
したがって, $D_{m,km+n} = D_{m,n}$.
最大公約数は, それらの集合上の整除関係に関する最大元であるから, $\gcd(m, km+n) = \gcd(m, n)$ [1] .

(2) $\dfrac{m}{d} = m', \dfrac{n}{d} = n'$ とおく. このとき, m', n' は整数だから, 整数 x, y が存在して, $\gcd(m', n') = m'x + n'y = \dfrac{1}{d}(xm + yn)$. ゆえに, $d \cdot \gcd(m', n') = xm + yn$.
また, $\gcd(m, n) \mid m$, $\gcd(m, n) \mid n$ だから, 任意の整数 a, b に対して, $\gcd(m, n) \mid am + bn$. 特に, 整数 x, y に対して, $\gcd(m, n) \mid xm + yn$. ゆえに, $\gcd(m, n) \mid d \cdot \gcd(m', n')$.
一方, 整数 m, n に対して, 整数 x', y' が存在して, $\gcd(m, n) = mx' + ny'$.
また, $\gcd(m', n') \mid m'$, $\gcd(m', n') \mid n'$ だから, 任意の整数 a, b に対して, $\gcd(m', n') \mid am' + bn'$. 特に, 整数 x', y' に対して, $\gcd(m', n') \mid x'm' + y'n'$. ゆえに, $\gcd(m', n') \mid \dfrac{1}{d}(x'm + y'n)$. このとき, $d \cdot \gcd(m', n') \mid mx' + ny'$ であり, $d \cdot \gcd(m', n') \mid \gcd(m, n)$.
$\gcd(m, n) \mid d \cdot \gcd(m', n')$, $d \cdot \gcd(m', n') \mid \gcd(m, n)$ だから, $|\gcd(m, n)| = |d \cdot \gcd(m', n')|$.
$\gcd(m, n) > 0$, $d > 0$, $\gcd(m', n') > 0$ だから, $\gcd(m, n) = d \cdot \gcd(m', n')$. すなわち, $\gcd\left(\dfrac{m}{d}, \dfrac{n}{d}\right) = \dfrac{\gcd(m, n)}{d}$.
（別解）
$\dfrac{m}{d} = m', \dfrac{n}{d} = n'$ とおく. m', n' のすべての非負公約数からなる集合を $D_{m',n'}$ とし, m, n のすべての非負公約数からなる集合を $D_{m,n}$ とする. また, $D'_{m,n} = \{\dfrac{x}{d} \mid x \in D_{m,n}, \dfrac{x}{d}$は整数.$\}$ とする.
このとき, 任意の $d' \in D_{m',n'}$ に対して, $d' \mid m'$, $d' \mid n'$. ゆえに, 整数 q, q' が存在して, $m' = qd'$, $n' = q'd'$. したがって, $m = qdd'$, $n = q'dd'$ であり, $dd' \mid m$, $dd' \mid n$. $dd' \in D_{m,n}$ だから, $d' \in D'_{m,n}$. すなわち, $D_{m',n'} \subseteq D'_{m,n}$.
一方, 任意の $\dfrac{d'}{d} \in D'_{m,n}$ $(d' \in D_{m,n})$ に対して, $d' \mid m$, $d' \mid n$. ゆえに, 整数 q, q' が存在して, $m = qd'$, $n = q'd'$. $d \neq 0$ だから, $m' = q\dfrac{d'}{d}$, $n' = q'\dfrac{d'}{d}$. $\dfrac{d'}{d}$ は整数だから, $\dfrac{d'}{d} \mid m'$, $\dfrac{d'}{d} \mid n'$ であり, $\dfrac{d'}{d} \in D_{m',n'}$. すなわち, $D'_{m,n} \subseteq D_{m',n'}$.
したがって, $D_{m',n'} = D'_{m,n}$.
このとき, $\gcd(m', n')$ は, $D_{m',n'}$ 上での整除関係に関する最大元であるから, $D'_{m,n}$ 上の整除関係に関する最大元 $\dfrac{u}{d}$ に等しい. 一方, u は $D_{m,n}$ 上の整除関係に関する最大元である $\gcd(m, n)$ に等しい. ゆえに, $\gcd(m', n') = \gcd\left(\dfrac{m}{d}, \dfrac{n}{d}\right) = \dfrac{\gcd(m, n)}{d}$.

(3) $m, n \neq 0$ だから, $\gcd(m, n) > 0$. そこで, (2) から,
$\gcd\left(\dfrac{m}{\gcd(m, n)}, \dfrac{n}{\gcd(m, n)}\right) = \dfrac{\gcd(m, n)}{\gcd(m, n)} = 1$.
（別解）$\gcd(m, n) = d$ とおく. $m, n \neq 0$ だから, $d \neq 0$.
$\dfrac{m}{d} = m', \dfrac{n}{d} = n'$ とおき, さらに, $\gcd(m', n') = d'$ とおく. このとき, $d' = 1$ を示せばよい.
$\gcd(m', n') = d'$ だから, $d' \mid m'$, $d' \mid n'$, ゆえに, 整数 q, q' が存在して, $m' = qd'$, $n' = q'd'$.
したがって, $m = m'd = qd'd$, $n = n'd = q'd'd$ だから, $d'd \mid m$, $d'd \mid n$. すなわち, $d'd$ は m, n の公約数である.
ところで, d は m, n の最大公約数だから, $d'd \mid d$. ゆえに, 整数 q'' が存在して, $d = q''d'd$. $d \neq 0$ だから, $1 = q''d'$. q'' は整数で, d' は非負整数だから, $d' = 1$.

(4) i) $k > 0$ のとき.

[1] 厳密には, $D_{m,km+n}$ と $D_{m,n}$ が整除関係に関して同型であることを示す.

k は km, kn の正の公約数だから, (2) から, $\gcd\left(\frac{km}{k}, \frac{kn}{k}\right) = \frac{\gcd(km, kn)}{k}$.
ゆえに, $k \cdot \gcd(m, n) = \gcd(km, kn)$.
ii) $k = 0$ のとき.
左辺=$\gcd(0 \cdot m, 0 \cdot n) = \gcd(0, 0) = 0$. 一方, 右辺=$0 \cdot \gcd(m, n) = 0$. ゆえに, 左辺=右辺.
i), ii) から, $k \cdot \gcd(m, n) = \gcd(km, kn)$.
（別解）
整数 m, n に対して, 整数 x, y が存在して, $\gcd(m, n) = mx + ny$.
このとき, $k \cdot \gcd(m, n) = k \cdot (mx + ny) = x(km) + y(kn)$.
また, $\gcd(km, kn) \mid km$, $\gcd(km, kn) \mid kn$ だから, 任意の整数 a, b に対して,
$\gcd(km, kn) \mid a(km) + b(kn)$. 特に, 整数 x, y に対して, $\gcd(km, kn) \mid x(km) + y(kn)$.
ゆえに, $\gcd(km, kn) \mid k \cdot \gcd(m, n)$.
一方, 整数 km, kn に対して, 整数 x', y' が存在して,
$\gcd(km, kn) = (km)x' + (kn)y' = k \cdot (x'm + y'n)$.
また, $\gcd(m, n) \mid m$, $\gcd(m, n) \mid n$ だから, 任意の整数 a, b に対して, $\gcd(m, n) \mid am + bn$. 特に, 整数 x', y' に対して, $\gcd(m, n) \mid x'm + y'n$. ゆえに, $k \cdot \gcd(m, n) \mid k \cdot (x'm + y'n)$.
したがって, $k \cdot \gcd(m, n) \mid \gcd(km, kn)$.
$\gcd(km, kn) \mid k \cdot \gcd(m, n)$, $k \cdot \gcd(m, n) \mid \gcd(km, kn)$ だから, $|\gcd(km, kn)| = |k \cdot \gcd(m, n)|$.
$\gcd(km, kn) \geq 0$, $k \cdot \gcd(m, n) \geq 0$ だから, $\gcd(km, kn) = k \cdot \gcd(m, n)$.

6. (1) m_1, m_2, n のすべての非負公約数からなる集合を $D_{m_1,m_2,n}$ とし, n, r_1, r_2 のすべての非負公約数からなる集合を D_{n,r_1,r_2} とする.
このとき, 任意の $d \in D_{m_1,m_2,n}$ に対して, $d \mid m_1$, $d \mid m_2$, かつ $d \mid n$ だから, $d \mid m_1 - q_1 n$ であり, $d \mid r_1$. 同様に, $d \mid (m_2 - q_2 n)$ であり, $d \mid r_2$. ゆえに, $d \in D_{n,r_1,r_2}$. すなわち, $D_{m_1,m_2,n} \subseteq D_{n,r_1,r_2}$.
一方, 任意の $d' \in D_{n,r_1,r_2}$ に対して, $d' \mid n$, $d' \mid r_1$, かつ $d' \mid r_2$ だから, $d' \mid q_1 n + r_1$ であり, $d \mid m_1$. 同様に, $d' \mid q_2 n + r_2$ であり, $d \mid m_2$. ゆえに, $d \in D_{m_1,m_2,n}$. すなわち, $D_{n,r_1,r_2} \subseteq D_{m_1,m_2,n}$.
したがって, $D_{m_1,m_2,n} = D_{n,r_1,r_2}$.
最大公約数は, それらの集合上の整除関係に関する最大元であるから, $\gcd(m_1, m_2, n) = \gcd(n, r_1, r_2)$.

(2)
$$
\begin{aligned}
& \gcd(126, 336, 91) \\
= \ & \gcd(336, 126, 91) \\
= \ & \gcd(63, 35, 91) && 63 = \mathrm{mod}\ (336, 91), 35 = \mathrm{mod}\ (126, 91) \\
= \ & \gcd(91, 63, 35) \\
= \ & \gcd(21, 28, 35) && 21 = \mathrm{mod}\ (91, 35),\ 28 = \mathrm{mod}\ (63, 35) \\
= \ & \gcd(35, 28, 21) \\
= \ & \gcd(14, 7, 21) && 14 = \mathrm{mod}\ (35, 21),\ 7 = \mathrm{mod}\ (28, 21) \\
= \ & \gcd(21, 14, 7) \\
= \ & \gcd(0, 0, 7) && 0 = \mathrm{mod}\ (21, 7),\ 0 = \mathrm{mod}\ (14, 7) \\
= \ & 7
\end{aligned}
$$

7.
```
int gcd(int m, int n)
{
    if(n==0){
        return(abs(m));
    }
    else{
        return(gcd(n, m%n));
    }
}
```

または

```
int gcd(int m, int n)
{
    int x, y, z;

    if(n==0){
        return(abs(m));
    }
    x=m;
    y=n;
    while(y!=0){
        z=x;
        x=y;
        y=z%y;
    };
    return(x);
}
```

離散数学演習９　解答例

1.

	○ 2	○ 3	× 4	○ 5	× 6
○ 7	× 8	× 9	× 10	11	× 12
13	× 14	× 15	× 16	17	× 18
19	× 20	× 21	× 22	23	× 24
× 25	× 26	× 27	× 28	29	× 30
31	× 32	× 33	× 34	× 35	× 36
37	× 38	× 39	× 40	41	× 42
43	× 44	× 45	× 46	47	× 48
× 49	× 50	× 51	× 52	53	× 54
× 55	× 56	× 57	× 58	59	× 60
61	× 62	× 63	× 64	× 65	× 66
67	× 68	× 69	× 70	71	× 72
73	× 74	× 75	× 76	× 77	× 78
79	× 80	× 81	× 82	83	× 84
× 85	× 86	× 87	× 88	89	× 90
× 91	× 92	× 93	× 94	× 95	× 96
97	× 98	× 99	× 100		

注意：$\sqrt{100} = 10$ より小さい素数について, その倍数に×を付ければよい.

100 以下の素数は, $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$ だから, $\pi(100) = 25$.

一方, $\dfrac{100}{\log_e 100} = \dfrac{100}{2\log_e 10} = \dfrac{100}{4.606} = 21.711.$

ゆえに, $\pi(100) \Big/ \dfrac{100}{\log_e 100} = 1.151.$

2. (1) $mn = \mathrm{lcm}(m,n)\gcd(m,n) = \mathrm{lcm}(m,n)\cdot 1 = \mathrm{lcm}(m,n)$. $n \mid nk$ であり, また, $m|nk$ だから nk は m と n の公倍数である. ゆえに, $\mathrm{lcm}(m,n) \mid nk$. すなわち, 整数 q が存在して, $nk = q\cdot\mathrm{lcm}(m,n) = qmn$. したがって, $k = qm$ だから, $m \mid k$.

   (2) $p|mn$ であるが, $p \mid m$ でも $p \mid n$ でもないと仮定する. このとき, $\gcd(p,m) = 1$ だから, (1) により, $p \mid n$. これは矛盾. ゆえに, $p \mid m$ または $p \mid n$.

3. n に関する帰納法により示す.

   （基底段階）$n = 0$ のとき.
   $F_{n+1} = F_1 = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5.$
   $F_0F_1\cdots F_n + 2 = F_0 + 2 = 2^{2^0} + 1 + 2 = 2^1 + 1 + 2 = 2 + 1 + 2 = 5.$
   ゆえに, $F_{n+1} = F_0F_1\cdots F_n + 2$.

   （帰納段階）$F_{n+1} = F_0F_1\cdots F_n + 2$ と仮定する.
   このとき, $F_{n+2} = 2^{2^{n+2}} + 1 = 2^{2^{n+1}2^1} + 1 = (2^{2^{n+1}})^2 + 1 = (F_{n+1}-1)^2 + 1 = F_{n+1}^2 - 2F_{n+1} + 2$
   $= (F_{n+1} - 2)F_{n+1} + 2.$
   ここで, 帰納法の仮定から, $F_{n+2} = (F_0F_1\cdots F_n)F_{n+1} + 2 = F_0F_1\cdots F_nF_{n+1} + 2.$

   以上から, 任意の n に対して, $F_n = F_0F_1\cdots F_{n-1} + 2$.

4. (1) n の正の約数は, $p_1^{h_1}p_2^{h_2}\cdots p_r^{h_r}$ $(0 \le h_i \le e_i, 1 \le i \le r)$ という形である. そのような h_i の選び方は $e_i + 1$ 通りあるから, 組 $(h_1, h_2, \cdots, h_r)$ の選び方は $(e_1+1)(e_2+1)\cdots(e_r+1)$ 通りである. 組 $(h_1, h_2, \cdots, h_r)$ が n の正の約数と 1 対 1 に対応するから, n の異なる正の約数の個数は $(e_1+1)(e_2+1)\cdots(e_r+1)$ である.

   (2) $p_1, p_2, \cdots, p_r$ は互いに異なる素数であるから, $\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2})\cdots\sigma(p_r^{e_r})$. ここで, $\sigma(p_i^{e_i}) = 1 + p_i^1 + p_i^2 + \cdots + p_i^{e_i}$. [1]
   $\sigma(p_i^{e_i}) = \dfrac{p_i^{e_i+1} - 1}{p_i - 1}$ だから, $\sigma(n) = \dfrac{p_1^{e_1+1} - 1}{p_1 - 1}\cdot\dfrac{p_2^{e_2+1} - 1}{p_2 - 1}\cdot\cdots\cdot\dfrac{p_r^{e_r+1} - 1}{p_r - 1}.$

[1] $\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2})\cdots\sigma(p_r^{e_r}) = (1 + p_1^1 + p_1^2 + \cdots + p_1^{e_1})(1 + p_2^1 + p_2^2 + \cdots + p_2^{e_2})\cdots(1 + p_r^1 + p_r^2 + \cdots + p_r^{e_r})$ を展開したときに得られる各項 $p_1^{h_1}p_2^{h_2}\cdots p_r^{h_r}$ $(0 \le h_i \le e_i, 1 \le i \le r)$ により, n の正の約数が重複なくすべて与えられることに注意せよ.

5. 2^p-1 は素数だから,

$$\begin{aligned}\sigma(2^{p-1}(2^p-1)) &= \sigma(2^{p-1})\sigma(2^p-1)\\ &= (1+2+2^2+\cdots+2^{p-1})(1+(2^p-1))\\ &= (2^p-1)2^p\\ &= 2\cdot 2^{p-1}(2^p-1)\end{aligned}$$

ゆえに, $2^{p-1}(2^p-1)$ は完全数である.

6. (1) $\begin{aligned}7x+5y &= 5(x+y)+2x\\ &= 5z+2x \qquad (z=x+y)\\ &= 2(2z+x)+z\\ &= 2u+z \qquad (u=2z+x)\end{aligned}$

ゆえに, $2u+z=100$ だから, $z=100-2u$.
したがって, $x=u-2z=u-2(100-2u)=-200+5u$.
$y=z-x=(100-2u)-(-200+5u)=300-7u$.
$u=0$ とおくと, 特殊解は $x=-200$, $y=300$.

(2) $\begin{aligned}385x+364y &= 364(x+y)+21x\\ &= 364z+21x \qquad (z=x+y)\\ &= 21(17z+x)+7z\\ &= 21u+7z \qquad (u=17z+x)\\ &= 7(3u+z)\end{aligned}$

ゆえに, $7(3u+z)=42$ だから, $z=6-3u$.
したがって, $x=u-17z=u-17(6-3u)=-102+52u$.
$y=z-x=(6-3u)-(-102+52u)=108-55u$.
$u=0$ とおくと, 特殊解は $x=-102$, $y=108$.

(3) $\begin{aligned}57x-87y &= 57(x-y)-30y\\ &= 57z-30y \qquad (z=x-y)\\ &= -30(-z+y)+27z\\ &= -30u+27z \qquad (u=-z+y)\\ &= 27(-2u+z)+24u\\ &= 27v+24u \qquad (v=-2u+z)\\ &= 24(v+u)+3v\\ &= 24w+3v \qquad (w=v+u)\\ &= 3(8w+v)\end{aligned}$

ゆえに, $3(8w+v)=342$ だから, $v=114-8w$.
$u=w-v=w-(114-8w)=-114+9w$.
$z=v+2u=(114-8w)+2(-114+9w)=-114+10w$.
したがって, $y=u+z=(-114+9w)+(-114+10w)=-228+19w$.
$x=z+y=(-114+10w)+(-228+19w)=-342+29w$.
$w=0$ とおくと, 特殊解は $x=-342$, $y=-228$.

7. (1) $\begin{aligned}x+2y+3z &= (x+y+z)+y+2z\\ &= u+y+2z \qquad (u=x+y+z)\\ &= (u+y+z)+z\\ &= v+z \qquad (v=u+y+z)\end{aligned}$

ゆえに, $v+z=4$ だから, $z=4-v$.
したがって, $y=v-u-z=v-u-(4-v)=2v-u-4$.
$x=u-y-z=u-(2v-u-4)-(4-v)=-v+2u$.
(別解) $\begin{aligned}x+2y+3z &= u\\ y &= v\\ z &= w\end{aligned}$
ゆえに, $u=4$ だから, $x=4-2y+3z=4-2v+3w$.
$u=v=w=0$ とおくと, 特殊解は $x=4$, $y=0$, $z=0$.

(2) $\begin{aligned}18x-24y+13z &= 13(x-2y+z)+5x+2y\\ &= 13u+5x+2y \qquad (u=x-2y+z)\\ &= 2(6u+2x+y)+u+x\\ &= 2v+u+x \qquad (v=6u+2x+y)\end{aligned}$

ゆえに, $2v+u+x=50$ だから, $x=50-2v-u$.
$y=v-6u-2x=v-6u-2(50-2v-u)=5v-4u-100$.
$z=u-x+2y=u-(50-2v-u)+2(5v-4u-100)=-6u+12v-250$.
$u=v=w=0$ とおくと, 特殊解は $x=50$, $y=-100$, $z=-250$.

（別解） $\begin{aligned} 18x-24y+13z &= 18(x-2y)+12y+13z \\ &= 18u+12(y+z)+z \qquad (u=x-2y) \\ &= 18u+12v+z \qquad (v=y+z) \end{aligned}$

ゆえに, $18u+12v+z=50$ だから, $z=50-18u-12v$.
$y=v-z=-50+18u+13v$.
$x=u+2y=-100+37u+26v$.
$u=v=w=0$ とおくと, 特殊解は $x=-100$, $y=-50$, $z=50$.

(3) $\begin{aligned} 105x-273y-195z &= 105(x-3y-2z)+42y+15z \\ &= 105u+42y+15z \qquad (u=x-3y-2z) \\ &= 15(7u+2y+z)+12y \\ &= 15v+12y \qquad (v=7u+2y+z) \\ &= 12(v+y)+3v \\ &= 12w+3v \qquad (w=v+y) \\ &= 3(4w+v) \end{aligned}$

ゆえに, $3(4w+v)=1365$ だから, $v=455-4w$.
したがって, $y=w-v=w-(455-4w)=-455+5w$.
$z=v-7u-2y=(455-4w)-7u-2(-455+5w)=3\cdot 455-14w-7u$.
$x=u+3y+2z=u+3(-455+5w)+2(3\cdot 455-14w-7u)=1365-13w-13u$.
$u=w=0$ とおくと, 特殊解は $x=1365$, $y=-455$, $z=1365$.

8. x,y が一般解であるとする. このとき, $ax+by=c$.
x_0,y_0 は特殊解だから, $ax_0+by_0=c$. ゆえに, $a(x-x_0)=-b(y-y_0)$.
ところで, $\gcd(a,b)=d$ だから, ある整数 a',b' が存在して, $a=a'd, b=b'd$. ゆえに, $a'd(x-x_0)=-b'd(y-y_0)$. したがって, $b'|a'(x-x_0)$.
$\gcd(a',b')=1$ だから, $b'|(x-x_0)$. このとき, ある整数 k が存在して, $x-x_0=kb'$. ゆえに, $x=x_0+\dfrac{b}{d}k$.
また, $a'dkb'=-b'd(y-y_0)$ だから, $y-y_0=-a'k$. ゆえに, $y=y_0-\dfrac{a}{d}k$.

9. $\begin{aligned} 2x+3y+5z &= 2(x+y+2z)+y+z \\ &= 2u+y+z \qquad (u=x+y+2z) \end{aligned}$

$2u+y+z=1$ だから, $y=1-z-2u$.
$x=u-y-2z=u-(1-z-2u)-2z=-1-z+3u$.
これを $3x+5y+7z=1$ に代入すると, $3(-1-z+3u)+5(1-z-2u)+7z=1$ だから, $1-z-u=0$.
ゆえに, $u=1-z$.
したがって, $x=-1-z+3(1-z)=2-4z$.
$y=1-z-2(1-z)=-1+z$.

（別解）与えられた連立 1 次方程式の係数行列を A, 拡大係数行列を $\tilde{A}$ とする. $\tilde{A}$ に基本行変形を施すと,

$\tilde{A}=\left[\begin{array}{ccc|c} 2 & 3 & 5 & 1 \\ 3 & 5 & 7 & 1 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & \frac{3}{2} & \frac{5}{2} & \frac{1}{2} \\ 3 & 5 & 7 & 1 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & \frac{3}{2} & \frac{5}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & \frac{3}{2} & \frac{5}{2} & \frac{1}{2} \\ 0 & 1 & -1 & -1 \end{array}\right]$
$\to \left[\begin{array}{ccc|c} 1 & 0 & 4 & 2 \\ 0 & 1 & -1 & -1 \end{array}\right]$.

A は 3 列で, $r(A)=r(\tilde{A})=2$ だから, $3-2=1$ 個のパラメータで表される無限個の解が存在する.
このとき, $\left[\begin{array}{ccc} 1 & 0 & 4 \\ 0 & 1 & -1 \end{array}\right]\left[\begin{array}{c} x \\ y \\ z \end{array}\right]=\left[\begin{array}{c} 2 \\ -1 \end{array}\right]$ だから, z をパラメータとして, 解は, $\left\{\begin{array}{rcl} x+4z &=& 2 \\ y+z &=& -1 \end{array}\right.$.
すなわち. $\left\{\begin{array}{rcl} x &=& 2-4z \\ y &=& -1+z \end{array}\right.$.

離散数学演習 10　解答例

1. $a \equiv b \pmod{p}$ だから, ある整数 k が存在して, $a - b = kp$. また, $d \mid p$ だから, ある整数 k' が存在して, $p = k'd$. ゆえに, $a - b = kk'd$. kk' は整数だから, $a \equiv b \pmod{d}$.

2. $2 \mid n$ であるとき. 整数 q が存在して, $n = q \cdot 2$. ゆえに, $n^2 = 4q^2 \equiv 0 \pmod{4}$.
一方, $2 \mid n$ でないとき. 除法定理から, 整数 q, r が存在して, $n = q \cdot 2 + r$ $(0 \leq |r| < 2)$. このとき, $r = \pm 1$ だから, $n = q \cdot 2 \pm 1$. ゆえに, $n^2 = 4q^2 \pm 4q + 1 \equiv 1 \pmod{4}$.

3. (1) $3x \equiv 13 \equiv 30 \pmod{17}$
$\gcd(3, 17) = 1$ だから, $x \equiv 10 \pmod{17}$

   (2) $7x \equiv 1 \pmod{13}$
一方, $13x \equiv 13 \pmod{13}$
ゆえに, $6x \equiv 12 \pmod{13}$
$\gcd(6, 13) = 1$ だから, $x \equiv 2 \pmod{13}$

   (3) $6x \equiv 22 \pmod{40}$
$\gcd(6, 22, 40) = 2$ だから, $3x \equiv 11 \pmod{20}$
ゆえに, $3x \equiv -9 \pmod{20}$
$\gcd(3, 20) = 1$ だから, $x \equiv -3 \equiv 17 \pmod{20}$

4. $\mathrm{lcm}(3, 5, 7) = 105$ である.
$x \equiv 2 \pmod{3}$ から, $35x \equiv 70 \pmod{105}$.
$x \equiv 3 \pmod{5}$ から, $21x \equiv 63 \pmod{105}$.
$x \equiv 4 \pmod{7}$ から, $15x \equiv 60 \pmod{105}$.
ゆえに, $21x + 15x - 35x \equiv 63 + 60 - 70 \pmod{105}$. すなわち, $x \equiv 53 \pmod{105}$.

（別解）次の連立 1 次不定方程式の一般解を求めればよい.

$$\begin{cases} x - 2 &= 3y \quad (1) \\ x - 3 &= 5z \quad (2) \\ x - 4 &= 7u \quad (3) \end{cases}$$

(1), (2) から, $3y + 2 = 5z + 3$. すなわち, $3y - 5z = 1$.
このとき, $3y - 5z = 3(y - 2z) + z = 3p + z$ $(p = y - 2z)$ だから, $3p + z = 1$. すなわち, $z = 1 - 3p$.
一方, (2), (3) から, $5z + 3 = 7u + 4$. すなわち, $5z - 7u = 1$.
これに $z = 1 - 3p$ を代入すると, $5(1 - 3p) - 7u = 5 - 15p - 7u = 1$. すなわち, $15p + 7u = 4$.
$15p + 7u = 7(u + 2p) + p = 7q + p$ $(q = u + 2p)$ だから, $7q + p = 4$.
このとき, $p = 4 - 7q$.
また, $u = q - 2p = q - 2(4 - 7q) = 15q - 8$.
ゆえに, $x = 7u + 4 = 7(15q - 8) + 4 = 105q - 52$.
したがって, $x \equiv -52 \equiv 53 \pmod{105}$.

（別解）
$M_1 = p_2p_3 = 5 \cdot 7 = 35$, $M_2 = p_1p_3 = 3 \cdot 7 = 21$, $M_3 = p_1p_2 = 3 \cdot 5 = 15$.
不定方程式 $35u_1 + 21u_2 + 15u_3 = 1$ を解く.

$$\begin{aligned} 35u_1 + 21u_2 + 15u_3 &= 15(2u_1 + u_2 + u_3) + 5u_1 + 6u_2 \\ &= 15p + 5u_1 + 6u_2 && (p = 2u_1 + u_2 + u_3) \\ &= 5(3p + u_1 + u_2) + u_2 \\ &= 5q + u_2 && (q = 3p + u_1 + u_2) \end{aligned}$$

ゆえに, $5q + u_2 = 1$ だから, $u_2 = 1 - 5q$.
$u_1 = q - 3p - u_2 = q - 3p - (1 - 5q) = 6q - 3p - 1$.
したがって, $u_3 = p - 2u_1 - u_2 = p - 2(6q - 3p - 1) - (1 - 5q) = 7p - 7q + 1$.
$p = q = 0$ とおくと, 特殊解は $u_1 = -1, u_2 = 1, u_3 = 1$.
連立方程式の一般解は,

$$\begin{aligned} x &\equiv M_1u_1x_1 + M_2u_2x_2 + M_3u_3x_3 \pmod{M} \\ &\equiv 35 \cdot (-1) \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 4 \pmod{105} \\ &\equiv -70 + 63 + 60 \pmod{105} \\ &\equiv 53 \pmod{105} \end{aligned}$$

5. $3x^2 - x - 2 \equiv 0 \pmod{7}$ だから, $(3x + 2)(x - 1) \equiv 0 \pmod{7}$.
7 は素数だから, $3x + 2 \equiv 0 \pmod{7}$ または $x - 1 \equiv 0 \pmod{7}$.

ゆえに, $3x \equiv -2 \pmod 7$ $(*)$ または $x \equiv 1 \pmod 7$.
$(*)$ から, $6x \equiv -4 \pmod 7$ $(**)$.
ここで, $7x \equiv 0 \pmod 7$ $(***)$.
$(***) - (**)$ から, $x \equiv 4 \pmod 7$.
ゆえに, $x \equiv 4 \pmod 7$ または $x \equiv 1 \pmod 7$.
（別解）
法は 7 であるから, 解は $x = 0, 1, \cdots, 6$ のうちにある.
そこで, 与えられた合同方程式の左辺に $x = 0, 1, \cdots, 6$ をそれぞれ代入すると,
$x = 1$ のとき, $3 \cdot x^2 - x = 3 \cdot 1^2 - 1 = 2 \equiv 2 \pmod 7$.
$x = 4$ のとき, $3 \cdot x^2 - x = 3 \cdot 4^2 - 4 = 44 \equiv 2 \pmod 7$.
ゆえに, これらは与えられた合同方程式の解である. したがって, $x \equiv 1 \pmod 7$ または $x \equiv 4 \pmod 7$.

6. (1) (a) $a \equiv b \pmod p$ とする.
$x \in [a]_p$ とすると, $x \equiv a \pmod p$. $a \equiv b \pmod p$ だから, $x \equiv b \pmod p$. ゆえに, $x \in [b]_p$. したがって, $[a]_p \subseteq [b]_p$.
同様に, $[b]_p \subseteq [a]_p$.
ゆえに, $[a]_p = [b]_p$.
一方, $[a]_p = [b]_p$ とする. 明らかに, $a \in [a]_p$ だから, $a \in [b]_p$. ゆえに, $a \equiv b \pmod p$.

(b) $a \not\equiv b \pmod p$ とする.
ここで, $[a]_p \cap [b]_p \neq \phi$ と仮定すると, $x \in [a]_p \cap [b]_p$ が存在する. ゆえに, $x \equiv a \pmod p$ かつ $x \equiv b \pmod p$ だから, $a \equiv b \pmod p$. これは矛盾.
したがって, $[a]_p \cap [b]_p = \phi$.
一方, $[a]_p \cap [b]_p = \phi$ とする.
ここで, $a \equiv b \pmod p$ と仮定すると, $a \in [b]_p$. また, 明らかに, $a \in [a]_p$. ゆえに, $a \in [a]_p \cap [b]_p$ だから, $[a]_p \cap [b]_p \neq \phi$. これは矛盾.
したがって, $a \not\equiv b \pmod p$.

(2) (a) 任意の $n \in \mathbf{Z}$ に対して, $q, r \in \mathbf{Z}$ が存在して, $n = qp + r$ $(0 \leq r < p)$ である. このとき, $n \equiv r \pmod p$. ゆえに, 任意の $[n]_p \in \mathbf{Z}/\equiv_p$ に対して, $r + 1 \in \mathbf{N}_p$ を考えると, $f(r+1) = [r]_p = [n]_p$. したがって, f は全射である.
$n_1, n_2 \in \mathbf{N}_p$ $(n_1 \neq n_2)$ に対して, $f(n_1) = f(n_2)$ とする. このとき, $[n_1 - 1]_p = [n_2 - 1]_p$. ゆえに, $n_1 - 1 \equiv n_2 - 1 \pmod p$ だから, $n_1 \equiv n_2 \pmod p$. ところが, $1 \leq n_1, n_2 \leq p$, $n_1 \neq n_2$ だから, $n_1 = n_2$. したがって, f は単射である.
以上から, f は全単射である.

(b) (a) から f は全単射だから, $\mathbf{Z}/\equiv_p = \{f(1), f(2), \cdots, f(p)\} = \{[0]_p, [1]_p, \cdots, [p-1]_p\}$.

7. (1)
$X_1 = \{1\}$
$X_2 = \{1\}$
$X_3 = \{1, 2\}$
$X_4 = \{1, 3\}$
$X_5 = \{1, 2, 3, 4\}$
$X_6 = \{1, 5\}$
$X_7 = \{1, 2, 3, 4, 5, 6\}$
$X_8 = \{1, 3, 5, 7\}$
$X_9 = \{1, 2, 4, 5, 7, 8\}$
$X_{10} = \{1, 3, 7, 9\}$

(2)
$\varphi(1) = |X_1| = 1$
$\varphi(2) = |X_2| = 1$
$\varphi(3) = |X_3| = 2$
$\varphi(4) = |X_4| = 2$
$\varphi(5) = |X_5| = 4$
$\varphi(6) = |X_6| = 2$
$\varphi(7) = |X_7| = 6$
$\varphi(8) = |X_8| = 4$
$\varphi(9) = |X_9| = 6$
$\varphi(10) = |X_{10}| = 4$

8. (1) (a) 自然数 n $(1 \leq n \leq p^2)$ に対して, $p \mid n$ であるとすると, $n \in \{1 \cdot p, 2 \cdot p, \cdots, p \cdot p\}$. すなわち, $p \mid n$ となる n は p 個である. ゆえに, $\varphi(p^2) = p^2 - p$.

(b) 自然数 n $(1 \leq n \leq p^e)$ に対して, $p \mid n$ であるとすると, $n \in \{1 \cdot p, 2 \cdot p, \cdots, p^{e-1} \cdot p\}$. すなわち, $p \mid n$ となる n は p^{e-1} 個である. ゆえに, $\varphi(p^e) = p^e - p^{e-1}$.

(c) $\gcd(p_1, p_2, \cdots, p_r) = 1$ だから, $\gcd(p_1^{e_1}, p_2^{e_2}, \cdots, p_r^{e_r}) = 1$. $\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r})$.
(b) から, $\varphi(p_i^{e_i}) = p_i^{e_i} - p_i^{e_i - 1} = p_i^{e_i}\left(1 - \dfrac{1}{p_i}\right)$.

$$\begin{aligned} \text{ゆえに,} \quad \varphi(n) &= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_1^{e_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{e_r}\left(1 - \frac{1}{p_r}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right). \end{aligned}$$

(2) $24 = 2^3 \cdot 3$ だから，$\varphi(24) = 24\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 24 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8.$

9. (1) $\gcd(p,m) = 1$ かつ $\gcd(p,n) = 1$ とする．
$\gcd(p,m) = 1$ だから，整数 x, y が存在して，$px + my = 1$.
また，$\gcd(p,n) = 1$ だから，整数 u, v が存在して，$pu + nv = 1$.
ゆえに，$(px+my)(pu+nv) = p \cdot (pxu + xnv + myu) + mn \cdot yv = 1$.
$\gcd(p, mn)$ は p, mn の約数だから，$p \cdot (pxu + xnv + myu) + mn \cdot yv$ の約数である．ゆえに，$\gcd(p, mn)$ は 1 の約数でもあるから，$\gcd(p, mn) = 1$.
一方，$\gcd(p, mn) = 1$ とする．
$\gcd(p, m)$ は p, m の公約数だから，p, mn の公約数でもある．$\gcd(p, mn) = 1$ だから，p, mn の公約数は 1 または -1．ゆえに，p, m の公約数も 1 または -1 であり，$\gcd(p, m) = 1$.
同様に，$\gcd(p, n) = 1$.

(2) $x \equiv b_1 \pmod{m}$ だから，ある整数 q_1 が存在して，$x = q_1 \cdot m + b_1$.
$\gcd(q_1 \cdot m + b_1, m) = \gcd(m, b_1)$ だから，$\gcd(x, m) = \gcd(m, b_1)$.
同様に，$\gcd(x, n) = \gcd(n, b_2)$.
ゆえに，(1) より，$\gcd(m, b_1) = 1$ かつ $\gcd(n, b_2) = 1$ であるとき，かつそのときに限り，$\gcd(mn, x) = 1$.

10. (1) $(a+b)^p = \sum_{k=0}^{p} {}_pC_k a^p b^{p-k} = a^p + {}_pC_1 a^{p-1}b + {}_pC_1 a^{p-1}b + {}_pC_2 a^{p-2}b^2 + \cdots + {}_pC_{p-1} ab^{p-1} + b^p.$
ここで，${}_pC_k = \frac{p!}{k!(p-k)!}$ は整数であり，$k \neq 0, p$ のとき，${}_pC_k$ は p で割り切れる．ゆえに，${}_pC_1 \equiv 0 \pmod{p}$, ${}_pC_2 \equiv 0 \pmod{p}$, $\cdots$, ${}_pC_{p-1} \equiv 0 \pmod{p}$.
すなわち，$(a+b)^p \equiv a^p + 0 + 0 + \cdots + 0 + b^p = a^p + b^p \pmod{p}$.

(2) n に関する数学的帰納法を用いる．
（基底段階）
$n = 1$ のとき．明らか．
$n = 2$ のとき[1]．(1) から明らか．
（帰納段階）$n = k$ $(k \geq 2)$ のときに命題は成り立つと仮定する．
$n = k + 1$ のとき．

$$\begin{aligned}
(a_1 + a_2 + \cdots + a_n)^p &= (a_1 + a_2 + \cdots + a_{k+1})^p \\
&= ((a_1 + a_2 + \cdots + a_k) + a_{k+1})^p \\
&\equiv (a_1 + a_2 + \cdots + a_k)^p + a_{k+1}^p \pmod{p} && \text{((1) から)} \\
&\equiv (a_1^p + a_2^p + \cdots + a_k^p) + a_{k+1}^p \pmod{p} && \text{(帰納法の仮定)} \\
&= a_1^p + a_2^p + \cdots + a_k^p + a_{k+1}^p \\
&= a_1^p + a_2^p + \cdots + a_n^p
\end{aligned}$$

(3) （基底段階）$a = 1$ のとき．$a^p = 1^p = 1 \equiv 1 = a \pmod{p}$.
（帰納段階）$a = k$ のときに命題が成り立つと仮定する．
$a = k + 1$ のとき，(1) から，$a^p = (k+1)^p \equiv k^p + 1^p = k^p + 1 \pmod{p}$.
帰納法の仮定から，$k^p + 1 \equiv k + 1 = a \pmod{p}$．ゆえに，$a^p \equiv a \pmod{p}$.

(4) $b = -a$ とおくと，b は自然数だから，(3) から，$b^p \equiv b \pmod{p}$．ゆえに，$(-a)^p \equiv -a \pmod{p}$.
すなわち，$(-1)^p a^p \equiv (-1)a \pmod{p}$.
$p = 2$ のとき．$(-1)^p = (-1)^2 = 1$, $-1 \equiv 1 \pmod{2}$ だから，$a^p \equiv a \pmod{p}$.
p が奇素数のとき．$(-1)^p = -1$ だから，$-a^p \equiv -a \pmod{p}$．ゆえに，$a^p \equiv a \pmod{p}$.
以上から，$a^p \equiv a \pmod{p}$.

(5) a が自然数のとき，(3) から明らか．
a が負の整数のとき，(4) から明らか．
$a = 0$ のとき，$a^p = 0^p = 0 \equiv 0 = a \pmod{p}$.
以上から，a が整数のとき，$a^p \equiv a \pmod{p}$.

(6) (5) において，p は素数で，$a \not\equiv 0 \pmod{p}$ だから，明らか．

[1] 基底段階は $n = 1$ のときだけでなく，$n = 2$ のときも証明する必要があることに注意せよ．なぜならば，帰納段階の証明は，$n \geq 3$ のときにのみ正しいからである．すなわち，$n = 2$ のときに命題が成り立つことは，$n = 1$ のときに命題が成り立つことを仮定しても導かれない．

11. 17 は素数, $2 \not\equiv 0 \pmod{17}$ だから, Fermat の小定理により, $2^{16} \equiv 1 \pmod{17}$. $1000000 = 16 \cdot 62500$ だから, $2^{1000000} = (2^{16})^{62500} \equiv 1^{62500} \equiv 1 \pmod{17}$. ゆえに, 剰余は 1 である.

12. (1) $d \mid n$ とする. このとき, d は自然数だから, 自然数 q が存在して, $n = qd$. ゆえに, $a^n = a^{qd} = (a^d)^q$. $a^d \equiv 1 \pmod{p}$ だから, $a^n \equiv 1^q \pmod{p}$. したがって, $a^n \equiv 1 \pmod{p}$.
一方, $a^n \equiv 1 \pmod{p}$ とする. $d \mid n$ でないと仮定すると, 自然数 q, r が存在して, $n = qd + r$ $(0 < r < d)$. ゆえに, $a^n = a^{qd+r} = a^{qd}a^r = (a^d)^q a^r$. $a^d \equiv 1 \pmod{p}$ だから, $a^n \equiv 1^q a^r \pmod{p}$. ゆえに, $a^n \equiv a^r \pmod{p}$ だから, $a^r \equiv 1 \pmod{p}$. $r < d$ だから, $r = 0$. これは矛盾. ゆえに, $d|n$.

(2) Fermat の小定理から, $a^{p-1} \equiv 1 \pmod{p}$. (1) から, $d|p-1$, すなわち, d は $p-1$ の約数である.

(3) $a^i \equiv a^j \pmod{p}$ であるとき, かつそのときに限り, $a^{i-j} \equiv 1 \pmod{p}$. (1) から, このとき, かつそのときに限り, $d|i-j$. ゆえに, $a^i \equiv a^j \pmod{p}$ であるならば, かつそのときに限り, $i \equiv j \pmod{d}$.

離散数学演習 11　解答例

1. $\gcd(x^4+10x^3+35x^2+50x+24, x^3+12x^2+41x+30)$
   $= \gcd(x^3+12x^2+41x+30, 6(3x^2+17x+14))$
   $(x^4+10x^3+35x^2+50x+24 = (x-2)(x^3+12x^2+41x+30)+6(3x^2+17x+14))$
   $= \gcd(x^3+12x^2+41x+30, 3x^2+17x+14)$
   $= \gcd(3x^2+17x+14, \frac{4}{9}(x+1))$
   $(x^3+12x^2+41x+30 = \frac{1}{3}(x+\frac{19}{3})(3x^2+17x+14)+\frac{4}{9}(x+1))$
   $= \gcd(3x^2+17x+14, x+1)$
   $= \gcd(x+1, 0)$
   $(3x^2+17x+14 = (3x+14)(x+1))$
   $= x+1$

2. $(x^2+2x)u(x)+(x^3+5x^2+7x+2)v(x)$
   $= (x^2+2x)(u(x)+(x+3)v(x))+(x+2)v(x)$
   $= (x^2+2x)w(x)+(x+2)v(x)$ $\quad (w(x)=u(x)+(x+3)v(x))$
   $= (x+2)(xw(x)+v(x))$
   ゆえに, $(x+2)(xw(x)+v(x))=x+2$.
   $x=-2$ のとき. $w(x), v(x)$ は任意の多項式であるから, $u(x), v(x)$ は任意の多項式である.
   $x\neq -2$ のとき. $xw(x)+v(x)=1$ だから, $v(x)=1-xw(x)$.
   したがって, $u(x)=w(x)-(x+3)v(x)=w(x)-(x+3)(1-xw(x))=-(x+3)+(x^2+3x+1)w(x)$.

3. (1) 加算表は次の通り. 乗算表は次の通り.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

   (2) $0\in\mathbf{Z}_4$ を考えると, $0+_4 0=0$, $1+_4 0=0+_4 1=1$, $2+_4 0=0+_4 2=2$, $3+_4 0=0+_4 3=3$. ゆえに, 任意の $n\in\mathbf{Z}_4$ に対して, $n+_4 0=0+_4 n=n$. すなわち, 0 は加法の単位元である.

   (3) $0+_4 0=0$ だから, 0 に対する加法の逆元 $-0=0$.
   $1+_4 3=3+_4 1=0$ だから, 1 に対する加法の逆元 $-1=3$, 3 に対する加法の逆元 $-3=1$.
   $2+_4 2=0$ だから, 2 に対する加法の逆元 $-2=2$.

   (4) $1\in\mathbf{Z}_4$ を考えると, $0\cdot_4 1=1\cdot_4 0=0$, $1\cdot_4 1=1$, $2\cdot_4 1=1\cdot_4 2=2$, $3\cdot_4 1=1\cdot_4 3=3$. ゆえに, 任意の $n\in\mathbf{Z}_4$ に対して, $n\cdot_4 1=1\cdot_4 n=n$. すなわち, 1 は乗法の単位元である.

   (5) $0\cdot_4 n=n\cdot_4 0=1$ となる $n\in\mathbf{Z}_4$ は存在しないから, 0 に対する乗法の逆元 0^{-1} は存在しない.
   $1\cdot_4 1=1$ だから, 1 に対する乗法の逆元 $1^{-1}=1$.
   $2\cdot_4 n=n\cdot_4 2=1$ となる $n\in\mathbf{Z}_4$ は存在しないから, 2 に対する乗法の逆元 2^{-1} は存在しない.
   $3\cdot_4 3=1$ だから, 3 に対する乗法の逆元 $3^{-1}=3$.

   (6) (1)〜(5) から, 以下のことは明らかである.
   - 任意の $m,n,k\in\mathbf{Z}_4$ に対して, $m+_4(n+_4 k)=(m+_4 n)+_4 k$. すなわち, 加法の結合則が成り立つ.
   - 加法の単位元が存在する.
   - 任意の $n\in\mathbf{Z}_4$ に対して, 加法の逆元 $-n$ が存在する.
   - 任意の $m,n\in\mathbf{Z}_4$ に対して, $m+_4 n=n+_4 m$. すなわち, 加法の交換則が成り立つ.
   - 任意の $m,n,k\in\mathbf{Z}_4$ に対して, $m\cdot_4(n\cdot_4 k)=(m\cdot_4 n)\cdot_4 k$. すなわち, 乗法の結合則が成り立つ.
   - 乗法の単位元が存在する.
   - 任意の $m,n,k\in\mathbf{Z}_4$ に対して, $m\cdot_4(n+_4 k)=(m\cdot_4 n)+_4(m\cdot_4 k)$. また, $(m+_4 n)\cdot_4 k=(m\cdot_4 k)+_4(n\cdot_4 k)$. すなわち, 分配則が成り立つ.

   以上から, $(\mathbf{Z}_4,+_4,\cdot_4)$ は環である.

   (7) (1) から, 任意の $m,n\in\mathbf{Z}_4$ に対して, $m\cdot_4 n=n\cdot_4 m$. すなわち, 乗法の交換則が成り立つ. ゆえに, $(\mathbf{Z}_4,+_4,\cdot_4)$ は可換環である.

4. (1) $0 \notin \mathbf{Z}^+$ だから, 加法の単位元は $\mathbf{Z}^+$ に存在しない. ゆえに, $(\mathbf{Z}^+, +, \cdot)$ は環でない.

(2) $n = 1$ のとき, $n\mathbf{Z} = \mathbf{Z}$ だから, $(n\mathbf{Z}, +, \cdot)$ は環である.
$n > 1$ のとき, $1 \notin n\mathbf{Z}$ だから, 乗法の単位元は $n\mathbf{Z}$ に存在しない. ゆえに, $(n\mathbf{Z}, +, \cdot)$ は環でない.

(3) i) 任意の $(a,b), (c,d), (e,f) \in \mathbf{Z}^2$ に対して,

$$\begin{aligned}((a,b)+(c,d))+(e,f) &= (a+c, b+d)+(e,f)\\ &= ((a+c)+e, (b+d)+f)\\ &= (a+(c+e), b+(d+f))\\ &= (a,b)+(c+e, d+f)\\ &= (a,b)+((c,d)+(e,f))\end{aligned}$$

となるから, 加法の結合則が成り立つ.

ii) $(0,0) \in \mathbf{Z}$ を考えると, 任意の $(a,b) \in \mathbf{Z}^2$ に対して,
$(0,0)+(a,b) = (0+a, 0+b) = (a,b)$,
$(a,b)+(0,0) = (a+0, b+0) = (a,b)$.
ゆえに, $(0,0)+(a,b) = (a,b)+(0,0) = (a,b)$. すなわち, 加法の単位元は $(0,0)$ である.

iii) 任意の $(a,b) \in \mathbf{Z}^2$ に対して, $(-a,-b) \in \mathbf{Z}^2$ を考えると,
$(a,b)+(-a,-b) = (a-a, b-b) = (0,0)$,
$(-a,-b)+(a,b) = (a-a, b-b) = (0,0)$.
ゆえに, $(a,b)+(-a,-b) = (-a,-b)+(a,b) = (0,0)$. すなわち, $(a,b) \in \mathbf{Z}^2$ に対して, 加法の逆元は $(-a,-b)$ である.

iv) 任意の $(a,b), (c,d) \in \mathbf{Z}^2$ に対して,

$$\begin{aligned}(a,b)+(c,d) &= (a+c, b+d)\\ &= (c+a, d+b)\\ &= (c,d), (a,b)\end{aligned}$$

となるから, 加法の交換則が成り立つ.

v) 任意の $(a,b), (c,d), (e,f) \in \mathbf{Z}^2$ に対して,

$$\begin{aligned}((a,b)\cdot(c,d))\cdot(e,f) &= (ac, bd)\cdot(e,f)\\ &= ((ac)e, (bd)f)\\ &= (a(ce), b(df))\\ &= (a,b)\cdot(ce, df)\\ &= (a,b)\cdot((c,d)\cdot(e,f))\end{aligned}$$

となるから, 乗法の結合則が成り立つ.

vi) $(1,1) \in \mathbf{Z}$ を考えると, 任意の $(a,b) \in \mathbf{Z}^2$ に対して,
$(1,1)\cdot(a,b) = (1a, 1b) = (a,b)$,
$(a,b)\cdot(1,1) = (a1, b1) = (a,b)$.
ゆえに, $(1,1)\cdot(a,b) = (a,b)\cdot(1,1) = (a,b)$. すなわち, 乗法の単位元は $(1,1)$ である.

vii) 任意の $(a,b), (c,d), (e,f) \in \mathbf{Z}^2$ に対して,

$$\begin{aligned}(a,b)\cdot((c,d)+(e,f)) &= (a,b)\cdot(c+e, d+f)\\ &= (a(c+e), b(d+f))\\ &= (ac+ae, bd+bf)\\ &= (ac, bd)+(ae, bf)\\ &= ((a,b)\cdot(c,d))+((a,b)\cdot(e,f))\\ ((a,b)+(c,d))\cdot(e,f)) &= ((a+c, b+d)\cdot(e,f)\\ &= ((a+c)e, (b+d)f)\\ &= (ae+ce, bf+df)\\ &= (ae, bf)+(ce, df)\\ &= ((a,b)\cdot(e,f))+((c,d)\cdot(e,f))\end{aligned}$$

ゆえに, 分配則が成り立つ.

i)〜vii) から, $(\mathbf{Z}^2, +, \cdot)$ は環である.

(4) i) 加法の結合則が成り立つこと, 加法の単位元と逆元が存在すること, 加法の交換則が成り立つことは (3) と同様に示せる.

ii) 任意の $(a,b), (c,d) \in \mathbf{Z}^2$ に対して, $ac, ad+bc \in \mathbf{Z}$ だから, $(a,b)\cdot(c,d) \in \mathbf{Z}$. ゆえに, $\mathbf{Z}^2$ は乗法 $\cdot$ に関して閉じている.

iii) 任意の $(a,b), (c,d), (e,f) \in \mathbf{Z}^2$ に対して,

$$\begin{aligned}((a,b)\cdot(c,d))\cdot(e,f) &= (ac,ad+bc)\cdot(e,f)\\ &= ((ac)e,(ac)f+(ad+bc)e)\\ &= (a(ce),a(cf+de)+b(ce))\\ &= (a,b)\cdot(ce,cf+de)\\ &= (a,b)\cdot((c,d)\cdot(e,f))\end{aligned}$$

となるから, 乗法の結合則が成り立つ.

iv) $(1,0)\in\mathbf{Z}$ を考えると, 任意の $(a,b)\in\mathbf{Z}^2$ に対して,
$(1,0)\cdot(a,b)=(1a,1b+0a)=(a,b)$,
$(a,b)\cdot(1,0)=(a1,a0+b1)=(a,b)$.
ゆえに, $(1,0)\cdot(a,b)=(a,b)\cdot(1,0)=(a,b)$. すなわち, 乗法の単位元は $(1,1)$ である.

v) 任意の $(a,b),(c,d),(e,f)\in\mathbf{Z}^2$ に対して,

$$\begin{aligned}(a,b)\cdot((c,d)+(e,f)) &= (a,b)\cdot(c+e,d+f)\\ &= (a(c+e),a(d+f)+b(c+e))\\ &= (ac+ae,(ad+bc)+(af+be))\\ &= (ac,ad+bc)+(ae,af+be)\\ &= ((a,b)\cdot(c,d))+((a,b)\cdot(e,f))\end{aligned}$$

$$\begin{aligned}((a,b)+(c,d))\cdot(e,f)) &= (a+c,b+d)\cdot(e,f)\\ &= ((a+c)e,(a+c)f+(b+d)e)\\ &= (ae+ce,(af+be)+(cf+de))\\ &= (ae,af+be)+(ce,cf+de)\\ &= ((a,b)\cdot(e,f))+((c,d)\cdot(e,f))\end{aligned}$$

ゆえに, 分配則が成り立つ.

i)〜v) から, $(\mathbf{Z}^2,+,\cdot)$ は環である.

(5) i) $A+B=(A\cup B)-(A\cap B)=(A\cap B^c)\cup(A^c\cap B)$.
ゆえに,

$$\begin{aligned}(A+B)^c &= ((A\cap B^c)\cup(A^c\cap B))^c\\ &= (A\cap B^c)^c\cap(A^c\cap B)^c\\ &= (A^c\cup(B^c)^c)\cap((A^c)^c\cup B^c)\\ &= (A^c\cup B)\cap(A\cup B^c)\\ &= ((A^c\cup B)\cap A)\cup((A^c\cup B)\cap B^c)\\ &= ((A^c\cap A)\cup(B\cap A))\cup((A^c\cap B^c)\cup(B\cap B^c))\\ &= (\phi\cup(B\cap A))\cup((A^c\cap B^c)\cup\phi)\\ &= (B\cap A)\cup(A^c\cap B^c)\\ &= (A\cap B)\cup(A^c\cap B^c)\end{aligned}$$

任意の $A,B,C\in\mathcal{P}(X)$ に対して,

$$\begin{aligned}(A+B)+C &= ((A+B)\cap C^c)\cup((A+B)^c\cap C)\\ &= (((A\cap B^c)\cup(A^c\cap B))\cap C^c)\cup(((A\cap B)\cup(A^c\cap B^c))\cap C)\\ &= ((A\cap B^c\cap C^c)\cup(A^c\cap B\cap C^c))\cup((A\cap B\cap C)\cup(A^c\cap B^c\cap C))\\ &= (A\cap B^c\cap C^c)\cup(A^c\cap B\cap C^c)\cup(A\cap B\cap C)\cup(A^c\cap B^c\cap C)\end{aligned}$$

$$\begin{aligned}A+(B+C) &= (A\cap(B+C)^c)\cup(A^c\cap(B+C))\\ &= (A\cap((B\cap C)\cup(B^c\cap C^c))\cup(A^c\cap((B\cap C^c)\cup(B^c\cap C)))\\ &= (A\cap B\cap C)\cup(A\cap B^c\cap C^c)\cup(A^c\cap B\cap C^c)\cup(A^c\cap B^c\cap C)\end{aligned}$$

ゆえに, $(A+B)+C=A+(B+C)$ となるから, 加法の結合則が成り立つ.

ii) $\phi\in\mathcal{P}(X)$ を考えると, 任意の $A\in\mathcal{P}(X)$ に対して,
$\phi+A=(\phi\cup A)-(\phi\cap A)=A-\phi=A$,
$A+\phi=(A\cup\phi)-(A\cap\phi)=A-\phi=A$,
ゆえに, $\phi+A=A+\phi=A$. すなわち, 加法の単位元は ϕ である.

iii) 任意の $A\in\mathcal{P}(X)$ に対して, $A+A=(A\cup A)-(A\cap A)=A-A=\phi$ だから, 加法の逆元は A 自身である.

iv) 任意の $A,B\in\mathcal{P}(X)$ に対して,

$$\begin{aligned}A+B &= (A\cup B)-(A\cap B)\\ &= (B\cup A)-(B\cap A)\\ &= B+A\end{aligned}$$

ゆえに, 加法の交換則が成り立つ.

v) 任意の $A,B,C\in\mathcal{P}(X)$ に対して,

$$\begin{aligned}(A\cdot B)\cdot C &= (A\cap B)\cap C\\ &= A\cap(B\cap C)\\ &= A\cdot(B\cdot C)\end{aligned}$$

ゆえに, 乗法の結合則が成り立つ.

vi) $X\in\mathcal{P}(X)$ を考えると, 任意の $A\in\mathcal{P}(X)$ に対して,
$X\cdot A = X\cap A = A$,
$A\cdot X = A\cap X = A$.
ゆえに, $X\cdot A = A\cdot X = A$. すなわち, 乗法の単位元は X である.

vii) 任意の $A,B,C\in\mathcal{P}(X)$ に対して,

$$\begin{aligned}A\cdot(B+C) &= A\cap(B+C)\\ &= A\cap((B\cap C^c)\cup(B^c\cap C))\\ &= (A\cap B\cap C^c)\cup(A\cap B^c\cap C)\end{aligned}$$

$$\begin{aligned}(A\cdot B)+(A\cdot C) &= ((A\cdot B)\cap(A\cdot C)^c)\cup((A\cdot B)^c\cap(A\cdot C))\\ &= ((A\cap B)\cap(A\cap C)^c)\cup((A\cap B)^c\cap(A\cap C))\\ &= ((A\cap B)\cap(A^c\cup C^c))\cup((A^c\cup B^c)\cap(A\cap C))\\ &= ((A\cap B\cap A^c)\cup(A\cap B\cap C^c))\cup((A^c\cap A\cap C)\cup(B^c\cap A\cap C))\\ &= ((\phi\cap B)\cup(A\cap B\cap C^c))\cup((\phi\cap C)\cup(B^c\cap A\cap C))\\ &= (\phi\cup(A\cap B\cap C^c))\cup(\phi\cup(B^c\cap A\cap C))\\ &= (A\cap B\cap C^c)\cup(B^c\cap A\cap C)\\ &= (A\cap B\cap C^c)\cup(A\cap B^c\cap C)\end{aligned}$$

ゆえに, $A\cdot(B+C) = (A\cdot B)+(A\cdot C)$ となる.
同様に, $(A+B)\cdot C = (A\cdot C)+(B\cdot C)$ を示せる.
したがって, 分配則が成り立つ.

i)〜vii) から, $(\mathcal{P}(X),+,\cdot)$ は環である.

5. (1)
$$\begin{aligned}x\cdot y+(-x)\cdot y &= (x+(-x))\cdot y && \text{(分配則)}\\ &= 0\cdot y && \text{(加法の逆元の性質)}\\ &= 0 && \text{(零元の性質)}\end{aligned}$$

ゆえに, $(-x)\cdot y = -(x\cdot y)$.
同様に, $x\cdot(-y) = -(x\cdot y)$.

(2)
$$\begin{aligned}(-x)\cdot(-y) &= -(x\cdot(-y)) && \text{((1) から)}\\ &= -(-(x\cdot y)) && \text{((1) から)}\\ &= x\cdot y && \text{(定理)}\end{aligned}$$

6. (1) $x,y\in R$ とする.
$$\begin{aligned}(x+y)^2 &= (x+y)\cdot(x+y)\\ &= x^2+x\cdot y+y\cdot x+y^2\\ &= x+x\cdot y+y\cdot x+y\end{aligned}$$
一方, $(x+y)^2 = x+y$.
ゆえに, $x\cdot y+y\cdot x = 0$.
ここで, $y=x$ とおくと, $x^2+x^2=0$ となるから, $x+x=0$. ゆえに, $2x=0$.

(2) (1) から, $x+x=0$ だから, $x=-x$.
また, (1) から, $x\cdot y+y\cdot x=0$ だから, $x\cdot y=-y\cdot x=y\cdot(-x)=y\cdot x$. ゆえに, 乗法の交換則が成り立つ.

7. $1=0$ とする. このとき, 任意の $x\in R$ に対して, $x=1\cdot x=0\cdot x=0$. ゆえに, $R=\{0\}$.
逆に, $R=\{0\}$ とする. 0 は R の唯一の元で, $0\cdot 0=0$ だから, 0 は乗法の単位元である. ゆえに, $1=0$.

離散数学演習 12　解答例

1. $(F,+,\cdot,c,e)$ を体とし, 任意の $x,y\in F$ に対して, $xy=c$, $x\neq c$ とする. F は可換環でもあるから, $y=c$ を示せばよい. ところで, F は体だから, $x^{-1}\in F$ が存在する. $xy=c$ だから, $x^{-1}xy=x^{-1}c$. $x^{-1}xy=ey=y$, $x^{-1}c=c$ だから, $y=c$.

2. R は環だから, $R[x]$ 上の演算を自然に定義すれば, 明らかに $R[x]$ は可換環である.
$f(x),g(x)\in R[x]$ とする. このとき, $f(x)=\sum_{i=0}^{n}a_ix^i$ $(a_n\neq 0,a_1,\cdots,a_n\in R)$, $g(x)=\sum_{i=0}^{m}b_ix^i$ $(b_m\neq 0,b_1,\cdots,b_m\in R)$ とおける.
さらに, $f(x)\neq 0, g(x)\neq 0$ とする. R は整域であり, $a_n\neq 0, b_m\neq 0$ だから, $a_nb_m\neq 0$.
$f(x)g(x)$ は $m+n$ 次の多項式で, $f(x)g(x)\in R[x]$. a_nb_m は $f(x)g(x)$ の最高次の係数だから, $f(x)g(x)\neq 0$.
ゆえに, $R[x]$ は整域である.

3. $(\mathbf{Z}^2,+,\cdot)$ は可換環であり, 加法の単位元は $(0,0)$ である. 任意の $a,b\in\mathbf{Z}$ $(a,b\neq 0)$ に対して, $(0,a),(b,0)\in\mathbf{Z}^2$ を考えると, $(0,a),(b,0)\neq(0,0)$. ところが, $(0,a)\cdot(b,0)=(0b,a0)=(0,0)$ だから, $(0,a),(b,0)$ は零因子である. ゆえに, $(\mathbf{Z}^2,+,\cdot)$ は整域ではない.

4. (1) $I^2=\begin{bmatrix} i & 0\\ 0 & -i\end{bmatrix}\begin{bmatrix} i & 0\\ 0 & -i\end{bmatrix}=\begin{bmatrix} i^2 & 0\\ 0 & (-i)^2\end{bmatrix}=\begin{bmatrix} -1 & 0\\ 0 & -1\end{bmatrix}=E,$

$J^2=\begin{bmatrix} 0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix} 0 & 1\\ -1 & 0\end{bmatrix}=\begin{bmatrix} -1 & 0\\ 0 & -1\end{bmatrix}=-E,$

$K^2=\begin{bmatrix} 0 & i\\ i & 0\end{bmatrix}\begin{bmatrix} 0 & i\\ i & 0\end{bmatrix}=\begin{bmatrix} i^2 & 0\\ 0 & i^2\end{bmatrix}=\begin{bmatrix} -1 & 0\\ 0 & -1\end{bmatrix}=-E$

(2) $IJ=\begin{bmatrix} i & 0\\ 0 & -i\end{bmatrix}\begin{bmatrix} 0 & 1\\ -1 & 0\end{bmatrix}=\begin{bmatrix} 0 & i\\ i & 0\end{bmatrix}=K,$

$JK=\begin{bmatrix} 0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix} 0 & i\\ i & 0\end{bmatrix}=\begin{bmatrix} i & 0\\ 0 & -i\end{bmatrix}=I,$

$KI=\begin{bmatrix} 0 & i\\ i & 0\end{bmatrix}\begin{bmatrix} i & 0\\ 0 & -i\end{bmatrix}=\begin{bmatrix} 0 & 1\\ -1 & 0\end{bmatrix}=J.$

$IJ=K$ から, $I^2J=IK$. $I^2=-E$ だから, $-J=IK$. ゆえに, $J=-IK$.
$JK=I$ から, $J^2K=JI$. $J^2=-E$ だから, $-K=JI$. ゆえに, $K=-JI$.
$KI=J$ から, $K^2I=KJ$. $K^2=-E$ だから, $-I=KJ$. ゆえに, $I=-KJ$.

(3) i) 任意の $A_1=a_1E+b_1I+c_1J+d_1K, A_2=a_2E+b_2I+c_2J+d_2K\in H$ に対して,

$$\begin{aligned}A_1+A_2 &= (a_1E+b_1I+c_1J+d_1K)+(a_2E+b_2I+c_2J+d_2K)\\ &= (a_1+a_2)E+(b_1+b_2)I+(c_1+c_2)J+(d_1+d_2)K\end{aligned}.$$

$a_1+a_2,b_1+b_2,c_1+c_2,d_1+d_2\in\mathbf{R}$ だから, $A_1+A_2\in H$.

$$\begin{aligned}\text{一方, } A_1A_2 &= (a_1E+b_1I+c_1J+d_1K)\cdot(a_2E+b_2I+c_2J+d_2K)\\ &= (a_1a_2E^2+a_1b_2EI+a_1c_2EJ+a_1d_2EK)\\ &\quad +(b_1a_2IE+b_1b_2I^2+b_1c_2IJ+b_1d_2IK)\\ &\quad +(c_1a_2JE+c_1b_2JI+c_1c_2J^2+c_1d_2JK)\\ &\quad +(d_1a_2KE+d_1b_2KI+d_1c_2KJ+d_1d_2K^2)\\ &= (a_1a_2E+a_1b_2I+a_1c_2J+a_1d_2K)\\ &\quad +(b_1a_2I-b_1b_2E+b_1c_2K-b_1d_2J)\\ &\quad +(c_1a_2J-c_1b_2K-c_1c_2E+c_1d_2I)\\ &\quad +(d_1a_2K+d_1b_2J-d_1c_2I-d_1d_2E)\\ &= (a_1a_2-b_1b_2-c_1c_2-d_1d_2)E+(a_1b_2+b_1a_2+c_1d_2-d_1c_2)I\\ &\quad +(a_1c_2-b_1d_2+c_1a_2+d_1b_2)J+(a_1d_2+b_1c_2-c_1b_2+d_1a_2)K\end{aligned}.$$

$a_1a_2-b_1b_2-c_1c_2-d_1d_2, a_1b_2+b_1a_2+c_1d_2-d_1c_2, a_1c_2-b_1d_2+c_1a_2+d_1b_2, a_1d_2+b_1c_2-c_1b_2+d_1a_2\in\mathbf{R}$ だから, $A_1A_2\in H$.
ゆえに, H は加法 $+$ と乗法 $\cdot$ に関して閉じているので, $(H,+,\cdot)$ は代数系である.

ii) 任意の $A_1=a_1E+b_1I+c_1J+d_1K, A_2=a_2E+b_2I+c_2J+d_2K, A_3=a_3E+b_3I+c_3J+d_3K\in H$ に対して,

$$\begin{aligned}(A_1+A_2)+A_3 &= ((a_1+a_2)+a_3)E+((b_1+b_2)+b_3)I+((c_1+c_2)+c_3)J\\ &\quad +((d_1+d_2)+d_3)K\\ &= (a_1+(a_2+a_3))E+(b_1+(b_2+b_3))I+(c_1+(c_2+c_3))J\\ &\quad +(d_1+(d_2+d_3)K\\ &= A_1+(A_2+A_3)\end{aligned}$$

となるから, 加法の結合則が成り立つ.

iii) $O=0E+0I+0J+0K\in H$ を考えると, 任意の $A=aE+bI+cJ+dK\in H$ に対して,
$O+A=(0+a)E+(0+b)I+(0+c)J+(0+d)K=aE+bI+cJ+dK=A$,
$A+O=(a+0)E+(b+0)I+(c+0)J+(d+0)K=aE+bI+cJ+dK=A$.
ゆえに, O は加法の単位元である.

iv) 任意の $A=aE+bI+cJ+dK\in H$ に対して, $-A=(-a)E+(-b)I+(-c)J+(-d)K\in H$ を考えると, $A+(-A)=(a+(-a))E+(b+(-b))I+(c+(-c))J+(d+(-d))K=0E+0I+0J+0K=O$,
$(-A)+A=((-a)+a)E+((-b)+b)I+((-c)+c)J+((-d)+d)K=0E+0I+0J+0K=O$
ゆえに, A に対して, 加法の逆元は $-A$ である.

v) 任意の $A_1=a_1E+b_1I+c_1J+d_1K, A_2=a_2E+b_2I+c_2J+d_2K\in H$ に対して,

$$\begin{aligned}A_1+A_2 &= (a_1+a_2)E+(b_1+b_2)I+(c_1+c_2)J+(d_1+d_2)K\\ &= (a_2+a_1)E+(b_1+b_1)I+(c_2+c_1)J+(d_2+d_1)K\\ &= A_2+A_1\end{aligned}$$

となるから, 加法の交換則が成り立つ.

vi) 任意の $A_1 = a_1E + b_1I + c_1J + d_1K, A_2 = a_2E + b_2I + c_2J + d_2K, A_3 = a_3E + b_3I + c_3J + d_3K \in H$ に対して,

$$
\begin{aligned}
(A_1A_2)A_3 &= ((a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)E + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)I \\
&\quad +(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)J + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)K) \\
&\quad \cdot(a_3E + b_3I + c_3J + d_3K) \\
&= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)a_3E^2 + (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)b_3EI \\
&\quad +(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)c_3EJ + (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)d_3EK \\
&\quad +(a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)a_3IE + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)b_3I^2 \\
&\quad +(a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)c_3IJ + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)d_3IK \\
&\quad +(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)a_3JE + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)b_3JI \\
&\quad +(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)c_3J^2 + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)d_3JK \\
&\quad +(a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)a_3KE + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)b_3KI \\
&\quad +(a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)c_3KJ + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)d_3K^2 \\
&= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)a_3E + (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)b_3I \\
&\quad +(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)c_3J + (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)d_3K \\
&\quad +(a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)a_3I - (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)b_3E \\
&\quad +(a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)c_3K - (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)d_3J \\
&\quad +(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)a_3J - (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)b_3K \\
&\quad -(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)c_3E + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)d_3I \\
&\quad +(a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)a_3K + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)b_3J \\
&\quad -(a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)c_3I - (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)d_3E \\
&= ((a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)a_3 - (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)b_3 \\
&\quad -(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)c_3 - (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)d_3))E \\
&\quad +((a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)b_3 + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)a_3 \\
&\quad +(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)d_3 - (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)c_3))I \\
&\quad +((a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)c_3 - (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)d_3 \\
&\quad +(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)a_3 + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)b_3))J \\
&\quad +((a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)d_3 + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)c_3 \\
&\quad -(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)b_3 + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)a_3)K) \\
&= (a_1a_2a_3 - a_1b_2b_3 - a_1c_2c_3 - a_1d_2d_3 - a_2b_1b_3 - a_2c_1c_3 - a_2d_1d_3 - a_3b_1b_2 \\
&\quad -a_3c_1c_2 - a_3d_1d_2 - b_1c_2d_3 + b_1c_3d_2 + b_2c_1d_3 - b_2c_3d_1 - b_3c_1d_2 + b_3c_2d_1)E \\
&\quad +(a_1a_2b_3 + a_1a_3b_2 + a_1c_2d_3 - a_1c_3d_2 + a_2a_3b_1 + a_2c_1d_3 - a_2c_3d_1 + a_3c_1d_2 \\
&\quad -a_3c_2d_1 - b_1b_2b_3 - b_1c_2c_3 - b_1d_2d_3 + b_2c_1c_3 + b_2d_1d_3 - b_3c_1c_2 - b_3d_1d_2)I \\
&\quad +(a_1a_2c_3 + a_1a_3c_2 - a_1b_2d_3 + a_1b_3d_2 + a_2a_3c_1 - a_2b_1d_3 + a_2b_3d_1 - a_3b_1d_2 \\
&\quad +a_3b_2d_1 - b_1b_2c_3 + b_1b_3c_2 - b_2b_3c_1 - c_1c_2c_3 - c_1d_2d_3 + c_2d_3d_1 - c_3d_1d_2)J \\
&\quad +(a_1a_2d_3 + a_1a_3d_2 + a_1b_2c_3 - a_1b_3c_2 + a_2a_3d_1 + a_2b_1c_3 - a_2b_3c_1 + a_3b_1c_2 \\
&\quad -a_3b_2c_1 - b_1b_2d_3 + b_1b_3d_2 - b_2b_3d_1 - c_1c_2d_3 + c_1c_3d_2 - c_2c_3d_1 - d_1d_2d_3)K
\end{aligned}
$$

$$
\begin{aligned}
A_1(A_2A_3) &= (a_1E + b_1I + c_1J + d_1K) \\
&\quad \cdot((a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3)E + (a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)I \\
&\quad +(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)J + (a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)K) \\
&= a_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3)E^2 + a_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)EI \\
&\quad +a_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)EJ + a_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)EK \\
&\quad +b_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3)IE + b_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)I^2 \\
&\quad +b_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)IJ + b_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)IK \\
&\quad +c_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3)JE + c_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)JI \\
&\quad +c_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)J^2 + c_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)JK \\
&\quad +d_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3)KE + d_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)KI \\
&\quad +d_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)KJ + d_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)K^2 \\
&= a_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3)E + a_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)I \\
&\quad +a_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)J + a_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)K \\
&\quad +b_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3)I - b_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)E \\
&\quad +b_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)K - b_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)J \\
&\quad +c_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3)J - c_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)K \\
&\quad -c_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)E + c_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)I \\
&\quad +d_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3)K + d_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3)J \\
&\quad -d_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3)I - d_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3)E \\
&= (a_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3) - b_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3) \\
&\quad -c_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3) - d_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3))E \\
&\quad +(a_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3) + b_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3) \\
&\quad +c_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3) - d_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3))I \\
&\quad +(a_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3) - b_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3) \\
&\quad +c_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3) + d_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3))J \\
&\quad +(a_1(a_2d_3 + b_2c_3 - c_2b_3 + d_2a_3) + b_1(a_2c_3 - b_2d_3 + c_2a_3 + d_2b_3) \\
&\quad -c_1(a_2b_3 + b_2a_3 + c_2d_3 - d_2c_3) + d_1(a_2a_3 - b_2b_3 - c_2c_3 - d_2d_3))K \\
&= (a_1a_2a_3 - a_1b_2b_3 - a_1c_2c_3 - a_1d_2d_3 - a_2b_1b_3 - a_2c_1c_3 - a_2d_1d_3 - a_3b_1b_2 \\
&\quad -a_3c_1c_2 - a_3d_1d_2 - b_1c_2d_3 + b_1c_3d_2 + b_2c_1d_3 - b_2c_3d_1 - b_3c_1d_2 + b_3c_2d_1)E \\
&\quad +(a_1a_2b_3 + a_1a_3b_2 + a_1c_2d_3 - a_1c_3d_2 + a_2a_3b_1 + a_2c_1d_3 - a_2c_3d_1 + a_3c_1d_2 \\
&\quad -a_3c_2d_1 - b_1b_2b_3 - b_1c_2c_3 - b_1d_2d_3 + b_2c_1c_3 + b_2d_1d_3 - b_3c_1c_2 - b_3d_1d_2)I \\
&\quad +(a_1a_2c_3 + a_1a_3c_2 - a_1b_2d_3 + a_1b_3d_2 + a_2a_3c_1 - a_2b_1d_3 + a_2b_3d_1 - a_3b_1d_2 \\
&\quad +a_3b_2d_1 - b_1b_2c_3 + b_1b_3c_2 - b_2b_3c_1 - c_1c_2c_3 - c_1d_2d_3 + c_2d_1d_3 - c_3d_1d_2)J \\
&\quad +(a_1a_2d_3 + a_1a_3d_2 + a_1b_2c_3 - a_1b_3c_2 + a_2a_3d_1 + a_2b_1c_3 - a_2b_3c_1 + a_3b_1c_2 \\
&\quad -a_3b_2c_1 - b_1b_2d_3 + b_1b_3d_2 - b_2b_3d_1 - c_1c_2d_3 + c_1c_3d_2 - c_2c_3d_1 - d_1d_2d_3)K
\end{aligned}
$$

となるから, $(A_1A_2)A_3 = A_1(A_2A_3)$. ゆえに, 乗法の結合則が成り立つ.

vii) $E = 1E + 0I + 0J + 0K \in H$ を考えると, 任意の $A = aE + bI + cJ + dK \in H$ に対して,
$EA = E(aE + bI + cJ + dK) = aE^2 + bEI + cEJ + dEK = aE + bI + cJ + dK = A$,
$AE = (aE + bI + cJ + dK)E = aE^2 + bIE + cJE + dKE = aE + bI + cJ + dK = A$.
ゆえに, E は乗法の単位元である.

viii) 任意の $A_1 = a_1E + b_1I + c_1J + d_1K, A_2 = a_2E + b_2I + c_2J + d_2K, A_3 = a_3E + b_3I + c_3J + d_3K \in H$ に対して,

$$\begin{aligned}
A_1(A_2 + A_3) &= (a_1E + b_1I + c_1J + d_1K) \\
&\quad \cdot((a_2E + b_2I + c_2J + d_2K) + (a_3E + b_3I + c_3J + d_3K)) \\
&= (a_1E + b_1I + c_1J + d_1K) \\
&\quad \cdot((a_2 + a_3)E + (b_2 + b_3)I + (c_2 + c_3)J + (d_2 + d_3)K) \\
&= (a_1(a_2 + a_3))E^2 + (a_1(b_2 + b_3))EI + (a_1(c_2 + c_3))EJ + (a_1(d_2 + d_3))EK \\
&\quad +(b_1(a_2 + a_3))IE + (b_1(b_2 + b_3))I^2 + (b_1(c_2 + c_3))IJ + (b_1(d_2 + d_3))IK \\
&\quad +(c_1(a_2 + a_3))JE + (c_1(b_2 + b_3))JI + (c_1(c_2 + c_3))J^2 + (c_1(d_2 + d_3))JK \\
&\quad +(d_1(a_2 + a_3))KE + (d_1(b_2 + b_3))KI + (d_1(c_2 + c_3))KJ + (d_1(d_2 + d_3))K^2 \\
&= (a_1(a_2 + a_3))E + (a_1(b_2 + b_3))I + (a_1(c_2 + c_3))J + (a_1(d_2 + d_3))K \\
&\quad +(b_1(a_2 + a_3))I - (b_1(b_2 + b_3))E + (b_1(c_2 + c_3))K - (b_1(d_2 + d_3))J \\
&\quad +(c_1(a_2 + a_3))J - (c_1(b_2 + b_3))K - (c_1(c_2 + c_3))E + (c_1(d_2 + d_3))I \\
&\quad +(d_1(a_2 + a_3))K + (d_1(b_2 + b_3))J - (d_1(c_2 + c_3))I - (d_1(d_2 + d_3))E \\
&= (a_1(a_2 + a_3) - b_1(b_2 + b_3) - c_1(c_2 + c_3) - d_1(d_2 + d_3))E \\
&\quad +(a_1(b_2 + b_3) + b_1(a_2 + a_3) + c_1(d_2 + d_3) - d_1(c_2 + c_3))I \\
&\quad +a_1(d_2 + d_3) - (b_1(d_2 + d_3) + (c_1(a_2 + a_3) + d_1(b_2 + b_3)J \\
&\quad +(a_1(c_2 + c_3) + b_1(c_2 + c_3) - c_1(b_2 + b_3) + d_1(a_2 + a_3)K \\
&= ((a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1a_3 - b_1b_3 - c_1c_3 - d_1d_3))E \\
&\quad +((a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2) + (a_1b_3 + b_1a_3 + c_1d_3 - d_1c_3))I \\
&\quad +((a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2) + (a_1c_3 - b_1d_3 + c_1a_3 + d_1b_3))J \\
&\quad +((a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2) + (a_1d_3 + b_1c_3 - c_1b_3 + d_1a_3))K.
\end{aligned}$$

一方,

$$\begin{aligned}
A_1A_2 &= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)E + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)I \\
&\quad +(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)J + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)K, \\
A_1A_3 &= (a_1a_3 - b_1b_3 - c_1c_3 - d_1d_3)E + (a_1b_3 + b_1a_3 + c_1d_3 - d_1c_3)I \\
&\quad +(a_1c_3 - b_1d_3 + c_1a_3 + d_1b_3)J + (a_1d_3 + b_1c_3 - c_1b_3 + d_1a_3)K, \\
A_1A_2 + A_1A_3 &= ((a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1a_3 - b_1b_3 - c_1c_3 - d_1d_3))E \\
&\quad +((a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2) + (a_1b_3 + b_1a_3 + c_1d_3 - d_1c_3))I \\
&\quad +((a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2) + (a_1c_3 - b_1d_3 + c_1a_3 + d_1b_3))J \\
&\quad +((a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2) + (a_1d_3 + b_1c_3 - c_1b_3 + d_1a_3))K \\
&= ((a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1a_3 - b_1b_3 - c_1c_3 - d_1d_3))E \\
&\quad +((a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2) + (a_1b_3 + b_1a_3 + c_1d_3 - d_1c_3))I \\
&\quad +((a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2) + (a_1c_3 - b_1d_3 + c_1a_3 + d_1b_3))J \\
&\quad +((a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2) + (a_1d_3 + b_1c_3 - c_1b_3 + d_1a_3))K
\end{aligned}$$

となるから, $A_1(A_2 + A_3) = A_1A_2 + A_1A_3$.

同様に, $(A_1 + A_2)A_3 = A_1A_3 + A_2A_3$ を示せる.

したがって, 分配則が成り立つ.

i)〜viii) から, $(H, +, \cdot)$ は環である.

(4) $k = a^2 + b^2 + c^2 + d^2$ とおく.

$$\begin{aligned}
kAB &= (aE + bI + cJ + dK)(aE - bI - cJ - dK) \\
&= (a^2E^2 - abEI - acEJ - adEK) + (abIE - b^2I^2 - bcIJ - bdIK) \\
&\quad +(acJE - bcJI - c^2J^2 - cdJK) + (adKE - bdKI - cdKJ - d^2K^2) \\
&= (a^2E - abI - acJ - adK) + (abI + b^2E - bcK + bdJ) \\
&\quad +(acJ + bcK + c^2E - cdI) + (adK - bdJ + cdI + d^2E) \\
&= (a^2 + b^2 + c^2 + d^2)E + (-ab + ab - cd + cd)I \\
&\quad +(-ac + bd + ac - bd)J + (-ad - bc + bc + ad)K \\
&= (a^2 + b^2 + c^2 + d^2)E \\
&= kE
\end{aligned}$$

となるから, $AB = E$

同様に, $BA = E$ を示せる.

5. (1) 2 項演算 · は, 2 引数であり, 各引数の選び方にそれぞれ 0, 1 の 2 通りがあるので, 引数のすべての組は 2^2 通りである. その各組に対して, 2 項演算の値の選び方はそれぞれ 0, 1 の 2 通りがあるので, 結局, 2 項演算 · は次の a)〜p) の $2^{2^2} = 16$ 通りが考えられる.

a)

·	0	1
0	0	0
1	0	0

b)

·	0	1
0	0	0
1	0	1

c)

·	0	1
0	0	0
1	1	0

d)

·	0	1
0	0	0
1	1	1

e)

·	0	1
0	0	1
1	0	0

f)

·	0	1
0	0	1
1	0	1

g)

·	0	1
0	0	1
1	1	0

h)

·	0	1
0	0	1
1	1	1

i)

·	0	1
0	1	0
1	0	0

j)

·	0	1
0	1	0
1	0	1

k)

·	0	1
0	1	0
1	1	0

l)

·	0	1
0	1	0
1	1	1

m)

·	0	1
0	1	1
1	0	0

n)

·	0	1
0	1	1
1	0	1

o)

·	0	1
0	1	1
1	1	0

p)

·	0	1
0	1	1
1	1	1

(2) 単位元が存在するものは, b), g), h), j).
b) の単位元 1, g) の単位元 0, h) の単位元 0, j) の単位元 1.

(3) 交換則が成り立つものは, 乗積表が対角線に関して対称になっているから,
a), b), g), h), i), j), o), p) である.

6. (1)

·	E	A	B	C
E	E	A	B	C
A	A	E	C	B
B	B	C	E	A
C	C	B	A	E

(2) $E \in G$ を考えると, $EE = E$, $AE = EA = A$, $BE = EB = B$, $CE = EC = C$. ゆえに, 任意の $X \in G$ に対して, $XE = EX = X$. すなわち, E は単位元である.

(3) $EE = E$ だから, E の逆元 $E^{-1} = E$.
$AA = E$ だから, A の逆元 $A^{-1} = A$.
$BB = E$ だから, B の逆元 $B^{-1} = B$.
$CC = E$ だから, C の逆元 $C^{-1} = C$.

(4) (1)〜(3) から, 以下のことは明らかである.

- 任意の $X, Y, Z \in G$ に対して, $X(YZ) = (XY)Z$. すなわち, 結合則が成り立つ.
- 単位元が存在する.
- 任意の $X \in G$ に対して, 逆元 X^{-1} が存在する
- 任意の $X, Y \in G$ に対して, $XY = YX$. すなわち, 交換則が成り立つ.

以上から, G は可換群である.

7. (1)

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

(2) $f_1 \in H$ を考えると, $f_1 \circ f_1 = f_1$, $f_2 \circ f_1 = f_1 \circ f_2 = f_2$, $f_3 \circ f_1 = f_1 \circ f_3 = f_3$, $f_4 \circ f_1 = f_1 \circ f_4 = f_4$.
ゆえに, 任意の $f_i \in H$ に対して, $f_i \circ f_1 = f_1 \circ f_i = f_1$. すなわち, f_1 は単位元である.

(3) $f_1 \circ f_1 = f_1$ だから, f_1 の逆元 $f_1^{-1} = f_1$.
$f_2 \circ f_2 = f_1$ だから, f_2 の逆元 $f_2^{-1} = f_2$.
$f_3 \circ f_3 = f_1$ だから, f_3 の逆元 $f_3^{-1} = f_3$.
$f_4 \circ f_4 = f_1$ だから, f_4 の逆元 $f_4^{-1} = f_4$.

(4) (1)〜(3) から, 以下のことは明らかである.

- 任意の $f_i, f_j, f_k \in H$ に対して, $f_i \circ (f_j \circ f_k) = (f_i \circ f_j) \circ f_k$. すなわち, 結合則が成り立つ.
- 単位元が存在する.
- 任意の $f_i \in H$ に対して, 逆元 f_i^{-1} が存在する
- 任意の $f_i, f_j \in H$ に対して, $f_i \circ f_j = f_j \circ f_i$. すなわち, 交換則が成り立つ.

以上から, H は可換群である.

8. i) 任意の $(a,b),(c,d),(e,f) \in G$ に対して,
$(a,b) \star ((c,d) \star (e,f)) = (a,b) \star (ce, de+f) = (ace, bce+de+f)$,
$((a,b) \star (c,d)) \star (e,f) = (ac, bc+d) \star (e,f) = (ace, (bc+d)e+f) = (ace, bce+de+f)$.
ゆえに, $(a,b) \star ((c,d) \star (e,f)) = ((a,b) \star (c,d)) \star (e,f)$. したがって, 結合則が成り立つ.

ii) 任意の $(a,b) \in G$ に対して, $(1,0) \in G$ を考えると,
$(a,b) \star (1,0) = (a \cdot 1, b \cdot 1 + 0) = (a,b)$,
$(1,0) \star (a,b) = (1 \cdot a, 0 \cdot a + b) = (a,b)$.
ゆえに, $(1,0)$ は単位元である.

iii) 任意の $(a,b) \in G$ に対して, $\dfrac{1}{a}, -\dfrac{b}{a} \in \mathbf{R}$, $\dfrac{1}{a} \neq 0$ だから, $\left(\dfrac{1}{a}, -\dfrac{b}{a}\right) \in G$.
ここで, $(a,b) \star \left(\dfrac{1}{a}, -\dfrac{b}{a}\right) = \left(a \cdot \dfrac{1}{a}, b \cdot \dfrac{1}{a} - \dfrac{b}{a}\right) = (1,0)$,
$\left(\dfrac{1}{a}, -\dfrac{b}{a}\right) \star (a,b) = \left(\dfrac{1}{a} \cdot a, -\dfrac{b}{a} \cdot a + b\right) = (1,0)$.
ゆえに, (a,b) の逆元は $\left(\dfrac{1}{a}, -\dfrac{b}{a}\right)$ である.

i)〜iii) から, $(G, \star)$ は群である.

9. (1) $ax = ay$ とする.

$$\begin{array}{rcll} x & = & ex & (\text{単位元の存在}) \\ & = & (a^{-1}a)x & (\text{逆元の存在}) \\ & = & a^{-1}(ax) & (\text{結合則}) \\ & = & a^{-1}(ay) & (ax = ay) \\ & = & (a^{-1}a)y & (\text{結合則}) \\ & = & ey & (\text{逆元の存在}) \\ & = & y & (\text{単位元の存在}) \end{array}$$

(2) $(ab)^2 = a^2b^2$ とする.

$$\begin{array}{rcll} ab & = & e(ab)e & (\text{単位元の存在}) \\ & = & (a^{-1}a)(ab)(bb^{-1}) & (\text{逆元の存在}) \\ & = & a^{-1}(a(ab))(bb^{-1}) & (\text{結合則}) \\ & = & a^{-1}((aa)b)(bb^{-1}) & (\text{結合則}) \\ & = & a^{-1}(aa)(b(bb^{-1})) & (\text{結合則}) \\ & = & a^{-1}(aa)(bb)b^{-1} & (\text{結合則}) \\ & = & a^{-1}a^2b^2b^{-1} & \\ & = & a^{-1}(ab)^2b^{-1} & ((ab)^2 = a^2b^2) \\ & = & a^{-1}(ab)(ab)b^{-1} & \\ & = & ((a^{-1}a)b)(a(bb^{-1})) & (\text{結合則}) \\ & = & (eb)(ae) & (\text{逆元の存在}) \\ & = & ba & (\text{単位元の存在}) \end{array}$$

10. G は性質 (1)〜(3) を満たすとする.
性質 (3) から, 任意の $x \in G$ に対して, $y \in G$ が存在して, $yx = e$.
さらに, 性質 (3) から, この $y \in G$ に対して, $z \in G$ が存在して, $zy = e$.

ここで, $xy = (ex)y$ (2)
$= e(xy)$ (1)
$= (zy)(xy)$
$= z(y(xy))$ (1)
$= z((yx)y)$ (1)
$= z(ey)$
$= zy$ (2)
$= e$

ゆえに, $xy = yx = e$. すなわち, y は x の逆元である.

一方, $xe = x(yx)$
$= (xy)x$ (1)
$= ex$
$= x$

ゆえに, $xe = ex = x$. すなわち, e は単位元である.

性質 (1) から, G は結合則が成り立つ.

以上から, G は群である.

逆に, G が群であるならば, 明らかに, 性質 (1)〜(3) を満たす.

離散数学演習 13　解答例

1. $H_1 \subseteq G$, $H_2 \subseteq G$ だから, $H_1 \cap H_2 \subseteq G$.

   任意の $x, y \in H_1 \cap H_2$ に対して, $x, y \in H_1$ かつ $x, y \in H_2$.
   H_1, H_2 は群だから, $xy \in H_1$ かつ $xy \in H_2$. ゆえに, $xy \in H_1 \cap H_2$.

   $e \in H_1$ かつ $e \in H_2$ だから, $e \in H_1 \cap H_2$.

   任意の $x \in H_1 \cap H_2$ に対して, $x \in H_1$ かつ $x \in H_2$.
   H_1, H_2 は群だから, $x^{-1} \in H_1$ かつ $x^{-1} \in H_2$. ゆえに, $x^{-1} \in H_1 \cap H_2$.

   以上から, $(H_1 \cap H_2, \cdot)$ は G の部分群である.

2. 任意の $x, y \in X$ に対して,
   $$\begin{aligned}(\psi \circ \varphi)(xy) &= \psi(\varphi(xy)) \\ &= \psi(\varphi(x)\varphi(y)) \\ &= \psi(\varphi(x))\psi(\varphi(y)) \\ &= (\psi \circ \varphi)(x)(\psi \circ \varphi)(y)\end{aligned}$$
   となるから, $\psi \circ \varphi$ は準同型である.

3. (1)
   - 任意の $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in G^2$ に対して,
     $$\begin{aligned}((x_1, y_1) \circ (x_2, y_2)) \circ (x_3, y_3) &= (x_1 \cdot x_2, y_1 \cdot y_2) \circ (x_3, y_3) \\ &= ((x_1 \cdot x_2) \cdot x_3, (y_1 \cdot y_2) \cdot y_3) \\ &= (x_1 \cdot (x_2 \cdot x_3), y_1 \cdot (y_2 \cdot y_3)) \\ &= (x_1, y_1) \circ (x_2 \cdot x_3, y_2 \cdot y_3) \\ &= (x_1, y_1) \circ ((x_2, y_2) \circ (x_3, y_3))\end{aligned}$$
     ゆえに, 結合則が成り立つ.
   - $(e, e) \in G^2$ を考えると, 任意の $(x, y) \in G^2$ に対して, $(x, y) \circ (e, e) = (x \cdot e, y \cdot e) = (x, y)$.
     一方, $(e, e) \circ (x, y) = (e \cdot x, e \cdot y) = (x, y)$.
     ゆえに, $(x, y) \circ (e, e) = (e, e) \circ (x, y) = (x, y)$ だから, (e, e) は単位元である.
   - G は群だから, $x, y \in G$ に対して, それぞれ逆元 x^{-1}, y^{-1} が存在する. 任意の $(x, y) \in G^2$ に対して, $(x^{-1}, y^{-1}) \in G^2$ を考えると, $(x, y) \circ (x^{-1}, y^{-1}) = (x \cdot x^{-1}, y \cdot y^{-1}) = (e, e)$,
     $(x^{-1}, y^{-1}) \circ (x, y) = (x^{-1} \cdot x, y^{-1} \cdot y) = (e, e)$.
     ゆえに, $(x, y) \circ (x^{-1}, y^{-1}) = (x^{-1}, y^{-1}) \circ (x, y) = (e, e)$ だから, (x, y) の逆元は (x^{-1}, y^{-1}) である.
   - 以上から, $(G^2, \circ)$ は群である.

   (2) $\mathrm{kernel}(\varphi) = \{(x, y) \mid \varphi((x, y)) = e,\ x, y \in G\}$ である. ここで, $\varphi((x, y)) = x$ だから, $x = e$. ゆえに, $\mathrm{kernel}(\varphi) = \{(e, y) \mid y \in G\}$.

   (3) $\mathrm{image}(\varphi) = \varphi(G^2) = \{\varphi((x, y)) \mid (x, y) \in G^2\} = \{x \mid x, y \in G\} = G$

   (4) 任意の $(x_1, y_1), (x_2, y_2) \in G^2$ に対して, $\varphi((x_1, y_1) \circ (x_2, y_2)) = \varphi(x_1 \cdot x_2, y_1 \cdot y_2) = x_1 \cdot x_2$.
   一方, $\varphi((x_1, y_1)) \cdot \varphi((x_2, y_2)) = x_1 \cdot x_2$.
   ゆえに, $\varphi((x_1, y_1) \circ (x_2, y_2)) = \varphi((x_1, y_1)) \cdot \varphi((x_2, y_2))$ だから, φ は準同型である.

4. $\varphi : G \to H$ を次のように定める: $\varphi(E) = f_1$, $\varphi(A) = f_2$, $\varphi(B) = f_3$, $\varphi(C) = f_4$
   このとき,

   $$\varphi(EE) = \varphi(E) = f_1 = f_1 \circ f_1 = \varphi(E) \circ \varphi(E)$$
   $$\varphi(EA) = \varphi(A) = f_2 = f_1 \circ f_2 = \varphi(E) \circ \varphi(A)$$
   $$\varphi(EB) = \varphi(B) = f_3 = f_1 \circ f_3 = \varphi(E) \circ \varphi(B)$$
   $$\varphi(EC) = \varphi(C) = f_4 = f_1 \circ f_4 = \varphi(E) \circ \varphi(C)$$
   $$\varphi(AE) = \varphi(A) = f_2 = f_2 \circ f_1 = \varphi(A) \circ \varphi(E)$$
   $$\varphi(AA) = \varphi(E) = f_1 = f_2 \circ f_2 = \varphi(A) \circ \varphi(A)$$
   $$\varphi(AB) = \varphi(C) = f_4 = f_2 \circ f_3 = \varphi(A) \circ \varphi(B)$$
   $$\varphi(AC) = \varphi(B) = f_3 = f_2 \circ f_4 = \varphi(A) \circ \varphi(C)$$
   $$\varphi(BE) = \varphi(B) = f_3 = f_3 \circ f_1 = \varphi(B) \circ \varphi(E)$$
   $$\varphi(BA) = \varphi(C) = f_4 = f_3 \circ f_2 = \varphi(B) \circ \varphi(A)$$

$$\varphi(BB) = \varphi(E) = f_1 = f_3 \circ f_3 = \varphi(B) \circ \varphi(B)$$
$$\varphi(BC) = \varphi(A) = f_2 = f_3 \circ f_4 = \varphi(B) \circ \varphi(C)$$
$$\varphi(CE) = \varphi(C) = f_4 = f_4 \circ f_1 = \varphi(C) \circ \varphi(E)$$
$$\varphi(CA) = \varphi(B) = f_3 = f_4 \circ f_2 = \varphi(C) \circ \varphi(A)$$
$$\varphi(CB) = \varphi(A) = f_2 = f_4 \circ f_3 = \varphi(C) \circ \varphi(B)$$
$$\varphi(CC) = \varphi(E) = f_1 = f_4 \circ f_4 = \varphi(C) \circ \varphi(C)$$

ゆえに, 任意の $X, Y \in G$ に対して, $\varphi(XY) = \varphi(X) \circ \varphi(Y)$.
また, φ は明らかに全単射である.
したがって, φ は同型写像であり, $G \simeq H$.

5. (1) 任意の $x, y \in \mathbf{R}$ に対して, $\varphi(x) = \varphi(y)$ とする. このとき, $\exp(x) = \exp(y)$ だから, $x = y$. ゆえに, φ は単射である.
任意の $x, y \in \mathbf{R}$ に対して, $\varphi(x + y) = \exp(x + y) = \exp(x)\exp(y) = \varphi(x)\varphi(y)$. ゆえに, φ は準同型である.

   (2) $\mathrm{image}(\varphi) = \{\varphi(x) \mid x \in \mathbf{R}\} = \{\exp(x) \mid x \in \mathbf{R}\}$.
$(\mathbf{R} - \{0\}, \cdot)$ の単位元は 1 だから, $\mathrm{kernel}(\varphi) = \{x \mid \varphi(x) = 1\}$. $\varphi(x) = \exp(x) = 1$ のとき, $x = 0$ だから, $\mathrm{kernel}(\varphi) = \{0\}$.

   (3) (1) と同様に, $\varphi' : \mathbf{R} \to \mathbf{R}^+$ として $\varphi'(x) = \exp(x)$ を考えると, φ' は単射かつ準同型である. 任意の $y \in \mathbf{R}^+$ に対して, $x = \log y$ とおくと, $y = \varphi'(x)$ かつ $x \in \mathbf{R}$. ゆえに, φ' は全射である.
φ' は全単射かつ準同型だから, $(\mathbf{R}, +) \simeq (\mathbf{R}^+, \cdot)$.

6. φ は単射であるとする.
任意の $x \in \mathrm{kernel}(\varphi)$ に対して, $\varphi(x) = e'$. また, 群準同型は単位元を保存するから, $\varphi(e) = e'$.
ゆえに, $\varphi(x) = \varphi(e)$. φ は単射であるから, $x = e$.
したがって, $\mathrm{kernel}(\varphi) \subseteq \{e\}$.
また, $\varphi(e) = e'$ から, $e \in \mathrm{kernel}(\varphi)$. ゆえに, $\{e\} \subseteq \mathrm{kernel}(\varphi)$.
以上から, $\mathrm{kernel}(\varphi) = \{e\}$.

   逆に, $\mathrm{kernel}(\varphi) = \{e\}$ とする.
また, 任意の $x_1, x_2 \in G$ に対して, $\varphi(x_1) = \varphi(x_2)$ とする.
このとき, $e' = \varphi(x_1) * \varphi(x_2)^{-1}$.
群準同型は逆元を保存するから, $\varphi(x_2)^{-1} = \varphi(x_2^{-1})$. ゆえに, $e' = \varphi(x_1) * \varphi(x_2^{-1})$.
さらに, φ は準同型だから, $e' = \varphi(x_1 x_2^{-1})$. ゆえに, $x_1 x_2^{-1} \in \mathrm{kernel}(\varphi) = \{e\}$.
したがって, $x_1 x_2^{-1} = e$ だから, $x_1 = x_2$. すなわち, φ は単射である.

7. (1) i)

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

   ii) $0 \in \mathbf{Z}_6$ を考えると, $0 +_6 0 = 0$, $1 +_6 0 = 0 +_6 1 = 1$, $2 +_6 0 = 0 +_6 2 = 2$, $3 +_6 0 = 0 +_6 3 = 3$, $4 +_6 0 = 0 +_6 4 = 4$, $5 +_6 0 = 0 +_6 5 = 5$. ゆえに, 任意の $n \in \mathbf{Z}_6$ に対して, $n +_6 0 = 0 +_6 n = n$.
すなわち, 0 は単位元である.

   iii) $0 +_6 0 = 0$ だから, 0 の逆元 $-0 = 0$.
$1 +_6 5 = 5 +_6 1 = 0$ だから, 1 の逆元 $-1 = 5$, 5 の逆元 $-5 = 1$.
$2 +_6 4 = 4 +_6 2 = 0$ だから, 2 の逆元 $-2 = 4$, 4 の逆元 $-4 = 2$.
$3 +_6 3 = 0$ だから, 3 の逆元 $-3 = 3$.

   iv) i)〜iii) から, 以下のことは明らかである.
   - 任意の $m, n, k \in \mathbf{Z}_6$ に対して, $m +_6 (n +_6 k) = (m +_6 n) +_6 k$. すなわち, 結合則が成り立つ.
   - 単位元が存在する.
   - 任意の $n \in \mathbf{Z}_6$ に対して, 逆元 $-n$ が存在する.

   以上から, $(\mathbf{Z}_6, +_6)$ は群である.

(2) i) $\varphi(0) = \mod(2\cdot 0, 6) = \mod(0,6) = 0$,
$\varphi(1) = \mod(2\cdot 1, 6) = \mod(2,6) = 2$,
$\varphi(2) = \mod(2\cdot 2, 6) = \mod(4,6) = 4$,
$\varphi(3) = \mod(2\cdot 3, 6) = \mod(6,6) = 0$,
$\varphi(4) = \mod(2\cdot 4, 6) = \mod(8,6) = 2$,
$\varphi(5) = \mod(2\cdot 5, 6) = \mod(10,6) = 4$.
ゆえに, $\varphi = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 2 & 4 & 0 & 2 & 4 \end{bmatrix}$.

ii) 任意の $m, n \in \mathbf{Z}_6$ に対して, $\varphi(m +_6 n) = \mod(2(m +_6 n), 6) \equiv 2(m +_6 n) \pmod 6$ [1].
$2(m +_6 n) \equiv 2(m+n) = 2m + 2n \pmod 6$ だから, $\varphi(m +_6 n) \equiv 2m + 2n \pmod 6$.
一方, $\varphi(m) +_6 \varphi(n) = \mod(2m, 6) +_6 \mod(2n, 6) \equiv \mod(2m, 6) + \mod(2n, 6) \pmod 6$.
$\mod(2m, 6) \equiv 2m \pmod 6$, $\mod(2n, 6) \equiv 2n \pmod 6$ だから, $\varphi(m) +_6 \varphi(n) \equiv 2m + 2n \pmod 6$.
ゆえに, $\varphi(m +_6 n) \equiv \varphi(m) +_6 \varphi(n) \pmod 6$.
$\varphi(m +_6 n), \varphi(m) +_6 \varphi(n) \in \mathbf{Z}_6$ だから, $\varphi(m +_6 n) = \varphi(m) +_6 \varphi(n)$.
ゆえに, φ は準同型である.

(3) i) (2) i) から, $\mathrm{image}(\varphi) = \{0, 2, 4\}$.

ii)

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

iii) $0 \in \mathrm{image}(\varphi)$ を考えると, $0 +_6 0 = 0$, $2 +_6 0 = 0 +_6 2 = 2$, $4 +_6 0 = 0 +_6 4 = 4$. ゆえに, 任意の $n \in \mathrm{image}(\varphi)$ に対して, $n +_6 0 = 0 +_6 n = n$. すなわち, 0 は単位元である.

iv) $0 +_6 0 = 0$ だから, 0 の逆元 $-0 = 0$.
$2 +_6 4 = 4 +_6 2 = 0$ だから, 2 の逆元 $-2 = 4$, 4 の逆元 $-4 = 2$.

v) ii)〜iv) から, 以下のことは明らかである.
- 任意の $m, n, k \in \mathrm{image}(\varphi)$ に対して, $m +_6 (n +_6 k) = (m +_6 n) +_6 k$. すなわち, 結合則が成り立つ.
- 単位元が存在する.
- 任意の $n \in \mathbf{Z}_6$ に対して, 逆元 $-n$ が存在する

以上から, $(\mathrm{image}(\varphi), +_6)$ は群である.

(4) i) $\mathbf{Z}_6$ の単位元は 0 だから, (1) i) から, $\mathrm{kernel}(\varphi) = \{0, 3\}$.

ii)

$+_6$	0	3
0	0	3
3	3	0

iii) $0 \in \mathrm{kernel}(\varphi)$ を考えると, $0 +_6 0 = 0$, $3 +_6 0 = 0 +_6 3 = 3$. ゆえに, 任意の $n \in \mathrm{kernel}(\varphi)$ に対して, $n +_6 0 = 0 +_6 n = n$. すなわち, 0 は単位元である.

iv) $0 +_6 0 = 0$ だから, 0 の逆元 $-0 = 0$.
$3 +_6 3 = 0$ だから, 3 の逆元 $-3 = 3$.

v) ii)〜iv) から, 以下のことは明らかである.
- 任意の $m, n, k \in \mathrm{kernel}(\varphi)$ に対して, $m +_6 (n +_6 k) = (m +_6 n) +_6 k$. すなわち, 結合則が成り立つ.
- 単位元が存在する.
- 任意の $n \in \mathbf{Z}_6$ に対して, 逆元 $-n$ が存在する.

以上から, $(\mathrm{kernel}(\varphi), +_6)$ は群である.

8. 明らかに, $\mathrm{image}(\varphi) \subseteq H$.
任意の $x', y' \in \mathrm{image}(\varphi)$ に対して, $x, y \in G$ が存在して, $x' = \varphi(x), y' = \varphi(y)$.
$xy \in G$ で, φ は準同型だから, $x'y' = \varphi(x) * \varphi(y) = \varphi(xy) \in \mathrm{image}(\varphi)$.

[1] 整数 n, p に対して, $\mod(n, p) \equiv n \pmod p$ であることに注意せよ. 実際, ある整数 q に対して, $n = qp + \mod(n, p)$ だから, このことが成り立つ.

群準同型は単位元を保存するから, $\varphi(e) = e'$. ゆえに, $e' \in \mathrm{image}(\varphi)$.

任意の $x' \in \mathrm{image}(\varphi)$ に対して, $x \in G$ が存在して, $x' = \varphi(x)$. すなわち, $(x')^{-1} = \varphi(x)^{-1}$. 群準同型は逆元を保存するから, $\varphi(x)^{-1} = \varphi(x^{-1})$. $x^{-1} \in G$ から, $\varphi(x^{-1}) \in \mathrm{image}(\varphi)$. ゆえに, $(x')^{-1} \in \mathrm{image}(\varphi)$.

以上から, $(\mathrm{image}(\varphi), \cdot)$ は H の部分群である.

9. (1) 任意の $x, y \in G$ に対して,

$$\begin{array}{rcll} (f+g)(x+y) & = & f(x+y)+g(x+y) & (f+g \text{ の定義から}) \\ & = & (f(x)+f(y))+(g(x)+g(y)) & (f, g \text{ は準同型だから}) \\ & = & (f(x)+g(x))+(f(y)+g(y)) & (H \text{ は可換群だから}) \\ & = & (f+g)(x)+(f+g)(y) & (f+g \text{ の定義から}) \end{array}$$

ゆえに, $f+g$ は準同型である. すなわち, $f+g \in \mathrm{Hom}\,(G, H)$.

(2) 関数 $f_c : G \to H$ を

任意の $x \in G$ に対して, $f_c(x) = c$ (c は H の単位元)

と定義する. このとき, 任意の $x, y \in G$ に対して, $f_c(x+y) = c$. 一方, $f_c(x)+f_c(y) = c+c = c$. ゆえに, $f_c(x+y) = f_c(x)+f_c(y)$ だから, $f_c \in \mathrm{Hom}\,(G, H)$.
さらに, 任意の $f \in \mathrm{Hom}\,(G, H)$ と任意の $x \in G$ に対して, $(f+f_c)(x) = f(x)+f_c(x) = f(x)+c = f(x)$. 一方, $(f_c+f)(x) = f_c(x)+f(x) = c+f(x) = f(x)$.
ゆえに, $f+f_c = f_c+f = f$ だから, f_c は単位元である.

(3) 任意の $f \in \mathrm{Hom}\,(G, H)$ に対して, 関数 $f^- : G \to H$ を

任意の $x \in G$ に対して, $f^-(x) = -f(x)$ ($-f(x)$ は H における $f(x)$ の逆元)

と定義する. このとき, 任意の $x, y \in G$ に対して, $f^-(x+y) = -f(x+y) = -(f(x)+f(y)) = (-f(x))+(-f(y))) = f^-(x)+f^-(y)$ だから, $f^- \in \mathrm{Hom}\,(G, H)$.
さらに, 任意の $f \in \mathrm{Hom}\,(G, H)$ と任意の $x \in G$ に対して, $(f+f^-)(x) = f(x)+f^-(x) = f(x)+(-f(x)) = c = f_c(x)$ (c は H の単位元). 一方, $(f^-+f)(x) = f^-(x)+f(x) = (-f(x))+f(x) = c = f_c(x)$.
ゆえに, $f+f^- = f^-+f = f_c$ だから, f^- は f の逆元である.

(4) (1)〜(3) より, $(\mathrm{Hom}\,(G, H), +)$ において, 結合則と交換則が成り立つことを示せばよい.
任意の $f, g, h \in \mathrm{Hom}\,(G, H)$ と任意の $x \in G$ に対して,

$$\begin{array}{rcll} ((f+g)+h)(x) & = & (f+g)(x)+h(x) & (\text{定義から}) \\ & = & (f(x)+g(x))+h(x) & (\text{定義から}) \\ & = & f(x)+(g(x)+h(x)) & (H \text{ は可換群だから}) \\ & = & f(x)+(g+h)(x) & (\text{定義から}) \\ & = & (f+(g+h))(x) & (\text{定義から}) \end{array}$$

だから, $(f+g)+h = f+(g+h)$. すなわち, 結合則が成り立つ.
任意の $f, g \in \mathrm{Hom}\,(G, H)$ と任意の $x \in G$ に対して,

$$\begin{array}{rcll} (f+g)(x) & = & f(x)+g(x) & (\text{定義から}) \\ & = & g(x)+f(x) & (H \text{ は可換群だから}) \\ & = & (g+f)(x) & (\text{定義から}) \end{array}$$

だから, $f+g = g+f$. すなわち, 交換則が成り立つ.
以上から, $(\mathrm{Hom}\,(G, H), +)$ は可換群である.

10. $ba^{-1} \in H$ とする.
任意の $x \in Hb$ に対して, ある $h \in H$ が存在して, $x = hb$.
また, $x = hb = (hb)e = (hb)(a^{-1}a) = ((hb)a^{-1})a = (h(ba^{-1}))a$. H は群であり, $ba^{-1}, h \in H$ だから, $h(ba^{-1}) \in H$. ゆえに, $x \in Ha$. したがって, $Hb \subseteq Ha$.
同様に, $Ha \subseteq Hb$.
以上から, $Ha = Hb$.

逆に, $Ha = Hb$ とする. このとき, $b = eb \in Hb = Ha$ だから, ある $h \in H$ が存在して, $b = ha$.
ゆえに, $ba^{-1} = h \in H$.

離散数学演習 14　解答例

1. (1) i) 加算表は次の通り.　　乗算表は次の通り.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

ii) $[0] \in \mathbf{Z}/\equiv_5$ を考えると, $[0]+[0]=[0]$, $[1]+[0]=[0]+[1]=[1]$, $[2]+[0]=[0]+[2]=[2]$, $[3]+[0]=[0]+[3]=[3]$, $[4]+[0]=[0]+[4]=[4]$. ゆえに, 任意の $[m] \in \mathbf{Z}/\equiv_5$ に対して, $[m]+[0]=[0]+[m]=[m]$. すなわち, $[0]$ は加法の単位元である.
$[1] \in \mathbf{Z}/\equiv_5$ を考えると, $[0]\cdot[1]=[1]\cdot[0]=[0]$, $[1]\cdot[1]=[1]$, $[2]\cdot[1]=[1]\cdot[2]=[2]$, $[3]\cdot[1]=[1]\cdot[3]=[3]$, $[4]\cdot[1]=[1]\cdot[4]=[4]$. ゆえに, 任意の $[m] \in \mathbf{Z}/\equiv_5$ に対して, $[m]\cdot[1]=[1]\cdot[m]=[m]$. すなわち, $[1]$ は乗法の単位元である.

iii) $[0]+[0]=[0]$ だから, $-[0]=[0]$.
$[1]+[4]=[4]+[1]=[0]$ だから, $-[1]=[4]$.
$[2]+[3]=[3]+[2]=[0]$ だから, $-[2]=[3]$.
$[3]+[2]=[2]+[3]=[0]$ だから, $-[3]=[2]$.
$[4]+[1]=[1]+[4]=[0]$ だから, $-[4]=[1]$.
$[0]\cdot[m]=[m]\cdot[0]=[1]$ となる $m \in \mathbf{Z}/\equiv_5$ は存在しない. ゆえに, $[0]^{-1}$ は存在しない.
$[1]\cdot[1]=[1]$ だから, $[1]^{-1}=[1]$.
$[2]\cdot[3]=[3]\cdot[2]=[1]$ だから, $[2]^{-1}=[3]$.
$[3]\cdot[2]=[2]\cdot[3]=[1]$ だから, $[3]^{-1}=[2]$.
$[4]\cdot[4]=[4]\cdot[4]=[1]$ だから, $[4]^{-1}=[4]$.

(2) 任意の $[m],[n],[k] \in \mathbf{Z}/\equiv_p$ に対して,

i) 任意の $[m],[n],[k] \in \mathbf{Z}/\equiv_p$ に対して,

$$\begin{aligned}([m]+[n])+[k] &= [m+n]+[k]\\ &= [(m+n)+k]\\ &= [m+(n+k)]\\ &= [m]+[n+k]\\ &= [m]+([n]+[k])\end{aligned}$$

となるから, 加法の結合則が成り立つ.

ii) $[0] \in \mathbf{Z}/\equiv_p$ を考えると, 任意の $[m] \in \mathbf{Z}/\equiv_p$ に対して, $[m]+[0]=[m+0]=[m]$, $[0]+[m]=[0+m]=[m]$.
ゆえに, $[m]+[0]=[0]+[m]=[m]$. すなわち, $[0]$ は加法の単位元である.

iii) 任意の $[m] \in \mathbf{Z}/\equiv_p$ に対して, $[-m] \in \mathbf{Z}/\equiv_p$ を考えると,
$[m]+[-m]=[m+(-m)]=[0]$,
$[-m]+[m]=[(-m)+m]=[0]$.
ゆえに, $[m]+[-m]=[-m]+[m]=[0]$. すなわち, $[m]$ に対して, $[-m]$ は加法の逆元である.

iv) 任意の $[m],[n] \in \mathbf{Z}/\equiv_p$ に対して,

$$\begin{aligned}[m]+[n] &= [m+n]\\ &= [n+m]\\ &= [m]+[n]\end{aligned}$$

となるから, 加法の交換則が成り立つ.

v) 任意の $[m],[n],[k] \in \mathbf{Z}/\equiv_p$ に対して,

$$\begin{aligned}([m]\cdot[n])\cdot[k] &= [m\cdot n]\cdot[k]\\ &= [(m\cdot n)\cdot k]\\ &= [m\cdot(n\cdot k)]\\ &= [m]\cdot[n\cdot k]\\ &= [m]\cdot([n]\cdot[k])\end{aligned}$$

となるから, 乗法の結合則が成り立つ.

vi) $[1] \in \mathbf{Z}/\equiv_p$ を考えると, 任意の $[m] \in \mathbf{Z}/\equiv_p$ に対して,
$[m]\cdot[1]=[m\cdot 1]=[m]$,

$[1]\cdot[m]=[1\cdot m]=[m]$.
ゆえに, $[m]\cdot[1]=[1]\cdot[m]=[m]$. すなわち, $[1]$ は乗法の単位元である.

vii) 任意の $[m],[n],[k]\in\mathbf{Z}/\equiv_p$ に対して,

$$\begin{aligned}
[m]\cdot([n]+[k]) &= [m]\cdot[n+k]\\
&= [m\cdot(n+k)]\\
&= [(m\cdot n)+(m\cdot k)] \qquad ,\\
&= [m\cdot n]+[m\cdot k]\\
&= ([m]\cdot[n])+([m]\cdot[k])\\
([m]+[n])\cdot[k] &= [m+n]\cdot[k]\\
&= [(m+n)\cdot k]\\
&= [(m\cdot k)+(n\cdot k)] \qquad ,\\
&= [m\cdot k]+[n\cdot k]\\
&= ([m]\cdot[k])+([n]\cdot[k])
\end{aligned}$$

となるから, 分配則が成り立つ.

viii) 任意の $[m],[n]\in\mathbf{Z}/\equiv_p$ に対して,

$$\begin{aligned}
[m]\cdot[n] &= [m\cdot n]\\
&= [n\cdot m]\\
&= [m]\cdot[n]
\end{aligned}$$

となるから, 乗法の交換則が成り立つ.

i)〜viii) から, $(\mathbf{Z}/\equiv_p,+,\cdot)$ は可換環である.

(3) 関数 $\varphi:\mathbf{Z}\to\mathbf{Z}/\equiv_p$ を
任意の $n\in\mathbf{Z}$ に対して, $\varphi(n)=[n]$.
と定義する. このとき, 任意の $m,n\in\mathbf{Z}$ に対して,
$\varphi(m+n)=[m+n]=[m]+[n]=\varphi(m)+\varphi(n)$,
$\varphi(m\cdot n)=[m\cdot n]=[m]\cdot[n]=\varphi(m)\cdot\varphi(n)$,
ゆえに, φ は準同型である. すなわち, $(\mathbf{Z}/\equiv_p,+,\cdot)$ は $(\mathbf{Z},+,\cdot)$ に準同型である.

(4) 関数 $\varphi:\mathbf{Z}\to\mathbf{Z}_p$ を
任意の $n\in\mathbf{Z}$ に対して, $\varphi(n)=\mathrm{mod}\ (n,p)$.
と定義する. このとき, 任意の $m,n\in\mathbf{Z}$ に対して,
$\varphi(m+n)=\mathrm{mod}\ (m+n,p)\equiv m+n\ (\mathrm{mod}\ p)$.
一方, $\varphi(m)+_p\varphi(n)=\mathrm{mod}\ (m,p)+_p\mathrm{mod}\ (n,p)\equiv\mathrm{mod}\ (m,p)+\mathrm{mod}\ (n,p)\ (\mathrm{mod}\ p)$.
$\mathrm{mod}\ (m,p)\equiv m\ (\mathrm{mod}\ p)$, $\mathrm{mod}\ (n,p)\equiv n\ (\mathrm{mod}\ p)$ だから, $\varphi(m)+_p\varphi(n)\equiv m+n\ (\mathrm{mod}\ p)$.
ゆえに, $\varphi(m+n)\equiv\varphi(m)+_p\varphi(n)\ (\mathrm{mod}\ p)$.
$\varphi(m+n),\varphi(m)+_p\varphi(n)\in\mathbf{Z}_p$ だから, $\varphi(m+n)=\varphi(m)+_p\varphi(n)$.
同様に, $\varphi(m\cdot n)=\varphi(m)\cdot_p\varphi(n)$.
ゆえに, φ は準同型である. すなわち, $(\mathbf{Z}_p,+_p,\cdot_p)$ は $(\mathbf{Z},+,\cdot)$ に準同型である.

2. (1) 任意の $[m],[n]\in\mathbf{Z}/\equiv_p$ に対して,
$\varphi([m]+[n])=\varphi([m+n])=[2(m+n)]=[2m+2n]=[2m]+[2n]=\varphi([m])+\varphi([n])$.
ゆえに, φ は準同型である.

(2) i) $\varphi([0])=[2\cdot0]=[0]$,
$\varphi([1])=[2\cdot1]=[2]$,
$\varphi([2])=[2\cdot2]=[4]$,
$\varphi([3])=[2\cdot3]=[6]=[0]$,
$\varphi([4])=[2\cdot4]=[8]=[2]$,
$\varphi([5])=[2\cdot5]=[10]=[4]$.

$$\varphi=\begin{bmatrix}[0] & [1] & [2] & [3] & [4] & [5]\\ [0] & [2] & [4] & [0] & [2] & [4]\end{bmatrix}.$$

ii) i) から, $\mathrm{image}(\varphi)=\{[0],[2],[4]\}$.

iii) $\mathbf{Z}/\equiv_6$ の単位元は $[0]$ だから, i) から, $\mathrm{kernel}(\varphi)=\{[0],[3]\}$.