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, $ba^{-1} = h \in H$.