「理工基礎 代数系」 問および演習問題の解答 （平成 30 年 4 月 17 日版）

第 1 章　問

問 1.22　$x \in X$ に対して

$$x \in X \setminus (Y \cup Z) \iff x \notin Y \cup Z \iff x \notin Y \text{ かつ } x \notin Z \iff x \in (X \setminus Y) \cap (X \setminus Z),$$
$$x \in X \setminus (Y \cap Z) \iff x \notin Y \cap Z \iff x \notin Y \text{ または } x \notin Z \iff x \in (X \setminus Y) \cup (X \setminus Z)$$

が成り立つことによる．　□

問 1.27　$X = \{ x_1, x_2, \ldots, x_n \}$ $(n = |X|)$ とする．写像 $f : X \to Y$ は $x_1, x_2, \ldots, x_n$ の像により一意的に定まり，$f(x_1)$, $f(x_2)$, …, $f(x_n)$ は Y の任意の元を独立に選ぶことができる（重複があっても構わない）．したがって，写像は全部で $|Y|^n = |Y|^{|X|}$ 個存在する．

なお，本書では暗に考察の対象外としているが，$|X| = 0$ や $|Y| = 0$，すなわち X や Y が空集合の場合についても触れておく．このような場合には，“集合 X の任意の元に対して集合 Y の元をただ一つ対応させる規則” という素朴な方法で写像を定義するのは難しい．実は，“直積集合 $X \times Y$ の部分集合 Γ で条件

(∗)　　任意の $x \in X$ に対し，$(x, y) \in \Gamma$ となるような $y \in Y$ がただ一つ存在する

をみたすもの” というのが “X から Y への写像” の本来の定義である（Γ とは素朴な方法で定義された写像の “グラフ” であると考えれば，この定義の意味が了解されるであろう）．この本来の定義に基づけば，X や Y が空集合であるときの $\mathrm{Map}(X, Y)$ は次のようになることがわかる．

(a)　$X = \emptyset$ の場合．このときには $X \times Y = \emptyset$ となるから，$X \times Y$ の部分集合は空集合に限る．また，$x \in X$ をとることはできないから，$\Gamma = \emptyset$ は条件 (∗) をみたす．よって，Y が空集合であるかどうかに関わらず，$\mathrm{Map}(X, Y) = \{ \emptyset \}$ となる．つまり，X から Y への写像は $\emptyset$ に限る．

(b)　$X \neq \emptyset$ かつ $Y = \emptyset$ の場合．このときにも $X \times Y = \emptyset$ となるから，$X \times Y$ の部分集合は空集合に限る．また，$x \in X$ をとることはできるが，$y \in Y$ をとることはできないから，$\Gamma = \emptyset$ は条件 (∗) をみたさない．よって $\mathrm{Map}(X, Y) = \emptyset$ となる．つまり，X から Y への写像は存在しない．

以上より

$$\text{任意の } Y \text{ に対して } \mathrm{Map}(\emptyset, Y) = \{ \emptyset \}, \text{ したがって } |\mathrm{Map}(\emptyset, Y)| = 1,$$
$$X \neq \emptyset \text{ とするとき } \mathrm{Map}(X, \emptyset) = \emptyset, \text{ したがって } |\mathrm{Map}(X, \emptyset)| = 0$$

となることがわかる．　□

問 1.29　各 $A \in \mathfrak{P}(X)$ に対して $\chi_A \in \mathrm{Map}(X, \{ 0, 1 \})$ を

$$\chi_A(x) = \begin{cases} 1 & (x \in A \text{ の場合}) \\ 0 & (x \notin A \text{ の場合}) \end{cases}$$

により定めると，$A \mapsto \chi_A$ は $\mathfrak{P}(X)$ から $\mathrm{Map}\big(X, \{\,0,1\,\}\big)$ への全単射を与える．実際，

$$\mathrm{Map}\big(X, \{\,0,1\,\}\big) \ni f \longmapsto f^{-1}(\{\,1\,\}) \in \mathfrak{P}(X)$$

が逆写像となっている． □

問 1.31 $f \mapsto \big(f(1), f(2), \ldots, f(n)\big)$ が $\mathrm{Map}(\{\,1,2,\ldots,n\,\}, X)$ から X^n への全単射を与える．実際，

$$X^n \ni (x_1, x_2, \ldots, x_n) \longmapsto \big(k \mapsto x_k\big) \in \mathrm{Map}(\{\,1,2,\ldots,n\,\}, X)$$

が逆写像となっている． □

第 1 章　演習問題

演習 1　全射は f_1 と f_3，単射は f_1 と f_2．

(1) $\mathbb{R} \ni x \mapsto x - 1 \in \mathbb{R}$ が f_1 の逆関数を与える．

(2) f_2 は (狭義) 単調増加なので単射．また，$f_2(x) \leq 0$ となるような $x \in \mathbb{R}$ は存在しないから全射ではない．

(3) f_3 は連続で $\lim_{x\to\infty} f_3(x) = \infty$ と $\lim_{x\to-\infty} f_3(x) = -\infty$ をみたすから全射（中間値の定理を用いた）．また，$f_3(0) = f_3(1) = 0$ なので単射ではない．

(4) $|f_4(x)| > 1$ となるような $x \in \mathbb{R}$ は存在しないから f_4 は全射ではない．また，$f_4(0) = f_4(\pi) = 0$ なので単射でもない． □

演習 2　**【命題 1.8 の証明】**　(1) 任意の $x \in X$ に対し，$\psi = h \circ g,\ y = f(x)$ とおくと

$$\big((h \circ g) \circ f\big)(x) = \big(\psi \circ f\big)(x) = \psi(f(x)) = \psi(y) = (h \circ g)(y) = h(g(y)) = h(g(f(x))).$$

また，$\phi = g \circ f$ とおくと，$\phi(x) = g(f(x))$ より

$$\big(h \circ (g \circ f)\big)(x) = (h \circ \phi)(x) = h(\phi(x)) = h(g(f(x))).$$

つまり

$$\big((h \circ g) \circ f\big)(x) = \big(h \circ (g \circ f)\big)(x) = h(g(f(x)))$$

が成り立つ．したがって，$x \in X$ が任意であることより，$(h \circ g) \circ f = h \circ (g \circ f)$ がわかる．

(2) まず，任意の $x \in X$ に対して $(f \circ \mathrm{id}_X)(x) = f(\mathrm{id}_X(x)) = f(x)$ が成り立つことより，$f \circ \mathrm{id}_X = f$ がわかる．また，任意の $x \in X$ に対して $(\mathrm{id}_Y \circ f)(x) = \mathrm{id}_Y(f(x)) = f(x)$ が成り立つことより，$\mathrm{id}_Y \circ f = f$ がわかる． □

【命題 1.9 の証明】　(1) f と g は共に全射であるとし，$z \in Z$ を任意にとる．このとき g が全射であることより $g(y) = z$ となるような $y \in Y$ が存在する．さらに f が全射であることより

$f(x)=y$ となるような $x\in X$ が存在する．よって $(g\circ f)(x)=g(f(x))=g(y)=z$．したがって $g\circ f$ は全射である．

(2) f と g は共に単射であるとし，$x,x'\in X$ が $(g\circ f)(x)=(g\circ f)(x')$，すなわち $g(f(x))=g(f(x'))$ をみたしたとする．このとき g が単射であることより $f(x)=f(x')$．さらに f が単射であることより $x=x'$．したがって $g\circ f$ は単射である． □

【命題 1.10 の証明】 (1) $g\circ f$ は全射であるとし，$z\in Z$ を任意にとる．このとき，$g\circ f$ が全射であることより，$(g\circ f)(x)=z$ となるような $x\in X$ が存在する．よって $y=f(x)$ とおくと $y\in Y$ は $g(y)=z$ をみたす．したがって g は全射である．

(2) $g\circ f$ は単射であるとし，$x,x'\in X$ が $f(x)=f(x')$ をみたしたとする．このとき，$g(f(x))=g(f(x'))$ となるから，$g\circ f$ が単射であることより $x=x'$．したがって f は単射である． □

演習 3 関数 f の $x<-1$ での最大値は 4 である．また，最小値は存在せず，下限は $-\infty$ である．よって $f(A)=\{\,y\in\mathbb{R}\mid y\le 4\,\}$（中間値の定理を用いた）．また，不等式 $f(x)\ge 4$ の解は $x=-2$ または $x\ge 1$ で与えられるから，$f^{-1}(B)=\{\,-2\,\}\cup\{\,x\in\mathbb{R}\mid x\ge 1\,\}$ となる． □

演習 4 **【命題 1.23 の証明】** (1) 前者の等号は，$y\in Y$ に対して

$$\begin{aligned} y\in f\big(\textstyle\bigcup_{i\in I}A_i\big) &\iff f(x)=y \text{ となるような } x\in\textstyle\bigcup_{i\in I}A_i \text{ が存在する}\\ &\iff f(x)=y \text{ となるような } i\in I \text{ と } x\in A_i \text{ が存在する}\\ &\iff y\in f(A_i) \text{ となるような } i\in I \text{ が存在する}\\ &\iff y\in\textstyle\bigcup_{i\in I}f(A_i)\end{aligned}$$

が成り立つことによる．また，後者の包含関係は，$y\in Y$ に対して

$$\begin{aligned} y\in f\big(\textstyle\bigcap_{i\in I}A_i\big) &\iff f(x)=y \text{ となるような } x\in\textstyle\bigcap_{i\in I}A_i \text{ が存在する}\\ &\implies \text{任意の } i\in I \text{ に対して } y\in f(A_i)\\ &\iff y\in\textstyle\bigcap_{i\in I}f(A_i)\end{aligned}$$

が成り立つことによる．なお，$y\in\bigcap_{i\in I}f(A_i)$ とすると，任意の $i\in I$ に対して $y=f(x_i)$ となるような $x_i\in A_i$ が存在するが，x_i は i に依存するため $y\in f\big(\bigcap_{i\in I}A_i\big)$ であるとは限らない．しかし，f が単射ならば，x_i は i に依らずに一意的に定まるから，それを x で表すことにすると $x\in\bigcap_{i\in I}A_i$ となり，$y\in f\big(\bigcap_{i\in I}A_i\big)$ が従う．

(2) 前者の等号は，$x\in X$ に対して

$$\begin{aligned} x\in f^{-1}\big(\textstyle\bigcup_{j\in J}B_j\big) &\iff f(x)\in\textstyle\bigcup_{j\in J}B_j\\ &\iff f(x)\in B_j \text{ となるような } j\in J \text{ が存在する}\\ &\iff x\in f^{-1}(B_j) \text{ となるような } j\in J \text{ が存在する}\\ &\iff x\in\textstyle\bigcup_{j\in J}f^{-1}(B_j)\end{aligned}$$

が成り立つことによる．また，後者の等号は，$x\in X$ に対して

$$
\begin{aligned}
x \in f^{-1}\big(\textstyle\bigcap_{j\in J} B_j\big) &\iff f(x) \in \textstyle\bigcap_{j\in J} B_j \\
&\iff \text{任意の } j \in J \text{ に対して } f(x) \in B_j \\
&\iff \text{任意の } j \in J \text{ に対して } x \in f^{-1}(B_j) \\
&\iff x \in \textstyle\bigcap_{j\in J} f^{-1}(B_j)
\end{aligned}
$$

が成り立つことによる．□

【命題 1.24 の証明】 まず $x \in A$ とすると，$f(x) \in f(A)$ より $x \in f^{-1}(f(A))$．これより前者の包含関係を得る．f が単射ならば，$f(x) \in f(A)$ から $x \in A$ が従うから，逆向きの包含関係も成り立つ．次に $f(f^{-1}(B)) \subset B$ と $f(f^{-1}(B)) \subset f(X)$ は明らかに成り立つから，$f(f^{-1}(B)) \subset B \cap f(X)$．逆に $y \in B \cap f(X)$ とすると，$f(x) = y$ となるような $x \in f^{-1}(B)$ が存在するから，$y \in f(f^{-1}(B))$．これより $f(f^{-1}(B)) \supset B \cap f(X)$ を得る．□

演習 5 写像 $f : X \to Y$ に対して

$$
\begin{aligned}
f \text{ は全射} &\iff \text{任意の } y \in Y \text{ に対して } \big|f^{-1}(\{\, y \,\})\big| > 0, \\
f \text{ は単射} &\iff \text{任意の } y \in Y \text{ に対して } \big|f^{-1}(\{\, y \,\})\big| \leq 1.
\end{aligned}
$$

□

第 2 章　演習問題

演習 1　たとえば $\sim_1, \sim_2, \sim_3$ を

$$\begin{aligned} x \sim_1 y &\iff xy \geq 0, \\ x \sim_2 y &\iff x \leq y, \\ x \sim_3 y &\iff xy \neq 0 \end{aligned}$$

により定義すれば，それぞれ (1), (2), (3) の性質をもつ．　□

演習 2　$x, x', x'' \in X$ とするとき

(1)　$\sim_Y$ は反射律をみたすから，$f(x) \sim_Y f(x)$．したがって $x \sim_X x$ が成り立つ．

(2)　$\sim_Y$ は対称律をみたすから，$f(x) \sim_Y f(x')$ ならば $f(x') \sim_Y f(x)$．したがって $x \sim_X x'$ ならば $x' \sim_X x$ が成り立つ．

(3)　$\sim_Y$ は推移律をみたすから，$f(x) \sim_Y f(x')$ かつ $f(x') \sim_Y f(x'')$ ならば $f(x) \sim_Y f(x'')$．したがって $x \sim_X x'$ かつ $x' \sim_X x''$ ならば $x \sim_X x''$ が成り立つ．　□

演習 3　(1)　まず，$\boldsymbol{x} = 1 \cdot \boldsymbol{x}$ より $\boldsymbol{x} \sim \boldsymbol{x}$．次に，$\boldsymbol{y} = t\boldsymbol{x}$ $(t \neq 0)$ ならば $\boldsymbol{x} = t^{-1}\boldsymbol{y}$ となるから，$\boldsymbol{x} \sim \boldsymbol{y}$ ならば $\boldsymbol{x} \sim \boldsymbol{y}$．また，$\boldsymbol{y} = t\boldsymbol{x}$, $\boldsymbol{z} = u\boldsymbol{y}$ $(t, u \neq 0)$ ならば $\boldsymbol{z} = (tu)\boldsymbol{x}$ となるから，$\boldsymbol{x} \sim \boldsymbol{y}$ かつ $\boldsymbol{y} \sim \boldsymbol{z}$ ならば $\boldsymbol{x} \sim \boldsymbol{z}$．以上より，$\sim$ は $\mathbb{R}^2 \setminus \{\boldsymbol{0}\}$ の同値関係である．

(2)　$\boldsymbol{x} \in \mathbb{R}^2 \setminus \{\boldsymbol{0}\}$ を代表元とする同値類は $\{t\boldsymbol{x} \mid t \in \mathbb{R} \setminus \{0\}\}$ となる．よって，$\sim$ に関する同値類は原点を通る直線から原点を除いたものになる．

(3)　$(x, y), (x', y') \in \mathbb{R}^2 \setminus \{\boldsymbol{0}\}$ が $\sim$ に関して同値であるとし，$(x', y') = t(x, y)$ $(t \neq 0)$ とする．このとき，$y \neq 0$ であれば $y' = ty \neq 0$ で，$f(x, y) = x/y = (tx)/(ty) = x'/y' = f(x', y')$．また $y = 0$ であれば $y' = ty = 0$ で，$f(x, y) = \infty = f(x', y')$．つまり，いずれの場合にも $f(x, y) = f(x', y')$ となる．

逆に，$(x, y), (x', y') \in \mathbb{R}^2 \setminus \{\boldsymbol{0}\}$ が $f(x, y) = f(x', y')$ をみたしたとする．このとき，$y \neq 0$ であれば $y' \neq 0$ で，$x/y = f(x, y) = f(x', y') = x'/y'$．したがって y'/y を t と置けば $(x', y') = t(x, y)$ が成り立つ．また $y = 0$ であれば $x \neq 0$ で，$f(x', y') = f(x, y) = \infty$ より $y' = 0$ がわかる．したがって x'/x を t と置けば $(x', y') = t(x, y)$ が成り立つ．つまり，いずれの場合にも $(x, y) \sim (x', y')$ となる．　□

演習 4　(1)　まず，単位行列 E に対して $A = EAE^{-1}$ が成り立つから $A \sim A$．次に $B = PAP^{-1}$ ならば $A = P^{-1}B\,(P^{-1})^{-1}$ となるから，$A \sim B$ ならば $B \sim A$．また，$B = PAP^{-1}$, $C = QBQ^{-1}$ ならば $C = (QP)A\,(QP)^{-1}$ となるから，$A \sim B$ かつ $B \sim C$ ならば $A \sim C$．以上より，$\sim$ は $\mathrm{M}_2(\mathbb{R})$ の同値関係である．

(2)　$B = PAP^{-1}$ ならば $\det(B) = \det(PAP^{-1}) = \det(P)\det(A)\det(P)^{-1} = \det(A)$ となる．つまり $A \sim B$ ならば $\det(A) = \det(B)$．よって，関数 $\mathrm{M}_2(\mathbb{R}) \ni A \mapsto \det(A) \in \mathbb{R}$ は商集合 $\mathrm{M}_2(\mathbb{R})/\sim$ 上の関数を引き起こす．　□

演習 5　商集合 $(\mathbb{Z}\times\mathbb{N})/\sim$ 上の関数を引き起こすものは f_1, f_5.

(1)　$y>0$ より，$f_1(x,y)=\varepsilon(x)=\varepsilon(x/y)$ となり，これは x/y だけで定まる.

(2)　たとえば $(x,y)=(1,1)$, $(x',y')=(2,2)$ とすると，$(x,y)\sim(x',y')$ かつ $f_2(x,y)=2\neq 4=f_2(x',y')$.

(3)　たとえば $(x,y)=(1,1)$, $(x',y')=(2,2)$ とすると，$(x,y)\sim(x',y')$ かつ $f_3(x,y)=1\neq 4=f_3(x',y')$.

(4)　たとえば $(x,y)=(0,1)$, $(x',y')=(0,2)$ とすると，$(x,y)\sim(x',y')$ かつ $f_4(x,y)=-1\neq -1/2=f_4(x',y')$.

(5)　$f_5(x,y)=\frac{xy}{x^2+y^2}=(\frac{x}{y}+\frac{y}{x})^{-1}$ （ただし $x=0$ の場合には $f_5(x,y)=0$）は x/y だけで定まる.　□

第 3 章　問

問 3.7　成り立たない．実際，たとえば $A := \mathbb{Z}$, $b_1 := 1$, $b_2 := -1$ とすると，$(b_1 + b_2)A = 0\,\mathbb{Z} = \{0\}$ であるが，$b_1 A = 1\,\mathbb{Z} = \mathbb{Z}$ と $b_2 A = (-1)\,\mathbb{Z} = \mathbb{Z}$ より $b_1 A + b_2 A = \mathbb{Z} + \mathbb{Z} = \mathbb{Z}$ となる．　□

問 3.10　(1) A は加法について閉じているから，$A + A \subset A$．また $0 \in A$ より $A + A \supset \{0\} + A = A$．以上より $A + A = A$ を得る．

(2)　まず $b > 0$ の場合，A は加法について閉じているから，任意の $a \in A$ に対して $ba = \overbrace{a + a + \cdots + a}^{b} \in A$．また $b < 0$ の場合には $|b|a \in A$ より $ba = -|b|a \in A$ となり，$b = 0$ の場合には $ba = 0 \in A$ となる．以上より，いずれの場合にも $ba \in A$ が成り立つことがわかり，$bA \subset A$ を得る．　□

問 3.20　(1) $(a\mathbb{Z} + b\mathbb{Z}) + c\mathbb{Z} = a\mathbb{Z} + (b\mathbb{Z} + c\mathbb{Z}) = a\mathbb{Z} + b\mathbb{Z} + c\mathbb{Z}$ であることによる．

(2) $(a\mathbb{Z} \cap b\mathbb{Z}) \cap c\mathbb{Z} = a\mathbb{Z} \cap (b\mathbb{Z} \cap c\mathbb{Z}) = a\mathbb{Z} \cap b\mathbb{Z} \cap c\mathbb{Z}$ であることによる．

(3) $ab\mathbb{Z} + ac\mathbb{Z} = a(b\mathbb{Z} + c\mathbb{Z}) = |a|(b\mathbb{Z} + c\mathbb{Z})$ であることによる．

(4) $ab\mathbb{Z} \cap ac\mathbb{Z} = a(b\mathbb{Z} \cap c\mathbb{Z}) = |a|(b\mathbb{Z} \cap c\mathbb{Z})$ であることによる．　□

問 3.35　例題 3.19 より，$g_i = \min(e_i, f_i)$ とおくと，

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)} = p_1^{e_1 + f_1 - g_1} p_2^{e_2 + f_2 - g_2} \cdots p_r^{e_r + f_r - g_r}.$$

ここで，$g_i + h_i = e_i + f_i$ より $e_i + f_i - g_i = h_i$ であるから，$\operatorname{lcm}(a, b) = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$ を得る．　□

第 3 章　演習問題

演習 1　まず $32 \equiv 1 \pmod{31}$ より $2^{340} = (2^5)^{68} \equiv 1^{68} \equiv 1 \pmod{31}$．また $32 \equiv -1 \pmod{11}$ より $2^{340} = (2^5)^{68} \equiv (-1)^{68} \equiv 1 \pmod{11}$．ここで $\gcd(11, 31) = 1$ であるから，命題 3.46 より $2^{340} \equiv 1 \pmod{341}$ となり，求める余りは 1 である．　□

演習 2　まず $8 \cdot 9 = 72$ と $7 \cdot 9 = 63$ に対してユークリッドの互除法を適用すると，

$$72 = 63 \cdot 1 + 9, \qquad 63 = 9 \cdot 7 + 0$$

より $\gcd(72, 63) = 9 = 72 \cdot 1 + 63 \cdot (-1)$ を得る．続いて $7 \cdot 8 = 56$ と 9 に対してユークリッドの互除法を適用すると，

$$56 = 9 \cdot 6 + 2, \qquad 9 = 2 \cdot 4 + 1, \qquad 2 = 1 \cdot 2 + 0$$

より $\gcd(56,9)=1=56\cdot(-4)+9\cdot 25$ を得る．以上より

$$\begin{aligned}\gcd(72,63,56)&=\gcd(\gcd(72,63),56)=\gcd(9,56)=1\\&=56\cdot(-4)+9\cdot 25=56\cdot(-4)+(72\cdot 1+63\cdot(-1))\cdot 25\\&=72\cdot 25+63\cdot(-25)+56\cdot(-4).\end{aligned}$$

よって

$$3\cdot 72\cdot 25+1\cdot 63\cdot(-25)+4\cdot 56\cdot(-4)=2929\equiv 409 \pmod{504}$$

より $a=409$ が求めるものである． □

演習 3　まず，$a\in\mathbb{Z}$ について

$$\begin{aligned}a\equiv 0 \pmod 2 &\iff a\equiv 0 \pmod 4 \text{ または } a\equiv 2 \pmod 4,\\ a\equiv 1 \pmod 2 &\iff a\equiv 1 \pmod 4 \text{ または } a\equiv 3 \pmod 4\end{aligned}$$

が成り立つこと，ならびに

$$0^2\equiv 0 \pmod 4,\qquad 1^2\equiv 1 \pmod 4,\qquad 2^2\equiv 4\equiv 0 \pmod 4,\qquad 3^2\equiv 9\equiv 1 \pmod 4$$

より

$$a^2\equiv\begin{cases}0 \pmod 4 & (a\equiv 0 \pmod 2 \text{ の場合})\\ 1 \pmod 4 & (a\equiv 1 \pmod 2 \text{ の場合})\end{cases}$$

がわかる．いま $x,y\in\mathbb{Z}$ とすると，上で示したように x^2,y^2 は 4 を法として 0 または 1 に合同であるから，x^2+y^2 は 4 を法として

$$0+0=0,\qquad 0+1=1+0=1,\qquad 1+1=2$$

のいずれかに合同である．他方，$z\in\mathbb{Z}$ とすると，$3z^2$ は 4 を法として

$$3\cdot 0=0,\qquad 3\cdot 1=3$$

のいずれかに合同である．したがって，$x^2+y^2=3z^2$ ならば $x\equiv y\equiv z\equiv 0 \pmod 2$，すなわち x,y,z は全て偶数でなければならない．このとき，$x_1=\frac{x}{2}$, $y_1=\frac{y}{2}$, $z_1=\frac{z}{2}$ と置くと，これらは整数で，$x_1^2+y_1^2=3z_1^2$ をみたす．よって，上と同じ議論を適用することにより，x_1,y_1,z_1 は全て偶数であることがわかる．つまり，$x\equiv y\equiv z\equiv 0 \pmod 4$ が成り立つ．この議論を繰り返すと，任意の $n\in\mathbb{Z}_{>0}$ に対して $x\equiv y\equiv z\equiv 0 \pmod{2^n}$ が成り立つことがわかるが，そのような整数は $x=y=z=0$ に限る． □

演習 4　$e>f$ であるとして一般性を失わない．$e=f+g$ とすると $g>0$ で，$a^{2^f}\equiv -1 \pmod{a^{2^f}+1}$ より

$$a^{2^e}=a^{2^{f+g}}=a^{2^f\cdot 2^g}=(a^{2^f})^{2^g}\equiv(-1)^{2^g}\equiv 1 \pmod{a^{2^f}+1}.$$

したがって $a^{2^e}+1 \equiv 1+1 \equiv 2 \pmod{a^{2^f}+1}$ となるから，

$$\gcd(a^{2^e}+1,\ a^{2^f}+1) = \gcd(2,\ a^{2^f}+1) = \begin{cases} 1 & (2 \nmid (a^{2^f}+1) \text{ の場合}) \\ 2 & (2 \mid (a^{2^f}+1) \text{ の場合}) \end{cases}.$$

よって

$$2 \mid (a^{2^f}+1) \quad \Longleftrightarrow \quad a^{2^f} \equiv 1 \pmod 2 \quad \Longleftrightarrow \quad a \equiv 1 \pmod 2$$

より主張を得る． □

演習 5 $A = (a_{ij})$ とすると，$\det(A) = \sum_\sigma \operatorname{sgn}(\sigma)\, a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$ （n 次の置換 σ すべてに渡る和）において，恒等置換に対応する項 $a_{11}a_{22}\cdots a_{nn}$ は奇数であるが，それ以外の項はすべて偶数である．したがって $\det(A)$ は奇数であり，とくに 0 でない． □

第 4 章　問

問 4.11　(1) $\mathrm{Map}(S,S)$ の元の合成は再び $\mathrm{Map}(S,S)$ の元となるので，$\mathrm{Map}(S,S)$ の元の合成写像を与える操作は $\mathrm{Map}(S,S)\times\mathrm{Map}(S,S)$ から $\mathrm{Map}(S,S)$ への写像であり，よって，$\mathrm{Map}(S,S)$ の演算である．命題 1.8 より写像の合成は結合律をみたし，恒等写像が単位元であるので，$\mathrm{Map}(S,S)$ は恒等写像を単位元にもつ半群となる．

(2) $\mathrm{Map}(S,S)$ の元 σ が写像の合成による演算に関して可逆であることは，id を恒等写像とするとき，$\sigma\circ\rho=\rho\circ\sigma=\mathrm{id}$ となる $\rho\in\mathrm{Map}(S,S)$ が存在することであるが，このことは σ が逆写像をもつことと同値であり，よって，命題 1.12 より σ が全単射であることと同値である．　□

問 4.16　演算表から演算で閉じていることはすぐにわかる．次に結合律 $(xy)z=x(yz)$ を示す．$x=a$ であれば，任意の $y,z\in G$ について $(ay)z=yz=a(yz)$ となり結合律が成り立つ．y や z が a である場合にも同様に示せるので，x,y,z の中に a があれば結合律は成り立つ．また a が含まれていなければ，$x=y=z=b$ であるので，$(xy)z=(bb)b=ab=b=ba=b(bb)=x(yz)$ となり，この場合にも結合律は成り立つ．よって，この演算は結合律をみたす．演算表より a が単位元であり，各元の逆元は自分自身である．以上より，G はこの演算で群になる（演算表より $ab=ba$ もわかるので G は可換群である）．　□

問 4.19　結合律より

$$\begin{aligned}(a_1a_2\cdots a_n)(a_n^{-1}\cdots a_2^{-1}a_1^{-1}) &= a_1a_2\cdots a_{n-1}(a_na_n^{-1})a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}\\ &= (a_1a_2\cdots a_{n-1})e(a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1})\\ &= (a_1a_2\cdots a_{n-1})(a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1})\end{aligned}$$

となる．これを繰り返せば，$(a_1a_2\cdots a_n)(a_n^{-1}\cdots a_2^{-1}a_1^{-1})=\cdots=(a_1a_2)(a_2^{-1}a_1^{-1})=a_1a_1^{-1}=e$ を得る．同様に $(a_n^{-1}\cdots a_2^{-1}a_1^{-1})(a_1a_2\cdots a_n)=e$ もわかるので，$a_1a_2\cdots a_n$ の逆元は $a_n^{-1}\cdots a_2^{-1}a_1^{-1}$ である．　□

問 4.28　$c\in G$ を一つとる．仮定より $cx=c$ となる $x\in G$ が存在する．そこで $e=x$ とおく．このとき $a\in G$ について，仮定より $yc=a$ となる $y\in G$ が存在し，$ae=(yc)x=y(cx)=yc=a$ が成り立つ．これは（y に依らず）任意の $a\in G$ に対して成り立つので，e は G の右単位元である．また $a\in G$ について，仮定より $ax=e$ となる $x\in G$ が存在するので，G の任意の元は右逆元をもつ．演算は結合律を満たしていたので，以上より定理 4.27 から G が群であることが従う．　□

問 4.30　演算表からこの演算に関して閉じている．次にこの演算が結合律 $(xy)z=x(yz)$ をみたすことを示す．まず，x,y,z のいずれかの元が 1 であれば，両辺とも同じ元の積であるので結合律は成り立つ．そこで，x,y,z はどれも 1 ではないとする．$x=y=z$ であれば両辺とも x^3 に等しいので結合律は成り立つ．次に同じ元がちょうど 2 つだけ含まれている場合には，たとえば

$x = y \neq z$ として，演算表より 1 でない相異なる元の積が 1 でない残りの元になることに注意すれば，w を $x = y$ でも z でも 1 でもない元として，$(xy)z = x^2z = z$ かつ $x(yz) = xw = z$ となり結合律が成り立つ．$x = z \neq y$ や $x \neq y = z$ の場合にも同様に示せる．最後にすべて異なる場合には，再び 1 でない相異なる元の積が 1 でない残りの元になることより，$x(yz) = xx = 1$ かつ $(xy)z = zz = 1$ となり，この場合にも結合律が成り立つ．以上より，この演算に関して結合律が成り立つ．演算表から，1 が単位元であり，各元の逆元は自分自身である．また，演算表の対称性より G は交換律をみたしている．以上より，$|G| = 4$ であったので，G は位数 4 の可換群である． □

問 4.31 行列の計算を行えば，$I^2 = J^2 = K^2 = -E,\ IJ = -JI = K,\ JK = -KJ = I,\ KI = -IK = J$ となることはわかる．これより演算表として

積	E	$-E$	I	$-I$	J	$-J$	K	$-K$
E	E	$-E$	I	$-I$	J	$-J$	K	$-K$
$-E$	$-E$	E	$-I$	I	$-J$	J	$-K$	K
I	I	$-I$	$-E$	E	K	$-K$	$-J$	J
$-I$	$-I$	I	E	$-E$	$-K$	K	J	$-J$
J	J	$-J$	$-K$	K	$-E$	E	I	$-I$
$-J$	$-J$	J	K	$-K$	E	$-E$	$-I$	I
K	K	$-K$	J	$-J$	$-I$	I	$-E$	E
$-K$	$-K$	K	$-J$	J	I	$-I$	E	$-E$

が得られる．とくに，この演算に関して閉じており，単位元は E である．また，$\pm E$ の逆元は自分自身，$\pm E$ 以外の元の逆元は自分自身の (-1) 倍である．演算は行列の積であるので結合律も成り立つ．以上より，G は群である．さらに，たとえば $IJ = -JI\ (\neq JI)$ より G は非可換群である． □

問 4.39 (1) 単位元 e について $e \in H_1 \cap H_2$ より，$H_1 \cap H_2 \neq \emptyset$ である．$a, b \in H_1 \cap H_2$ とする．このとき，$a, b \in H_1$ かつ $a, b \in H_2$ であり，H_1 と H_2 が部分群であることから，$ab^{-1} \in H_1$ かつ $ab^{-1} \in H_2$ となる．よって，$ab^{-1} \in H_1 \cap H_2$ を得る．したがって，定理 4.35（部分群の判定定理）より $H_1 \cap H_2$ は G の部分群である．

(2) H_i は部分群であるので G の単位元 e を含む．よって，$e \in \bigcap_i H_i \neq \emptyset$ である．$a, b \in \bigcap_i H_i$ とすると，任意の i について $a, b \in H_i$ であるから，H_i が部分群であることより，任意の i について $ab^{-1} \in H_i$ となる．よって，$ab^{-1} \in \bigcap_i H_i$ を得る．したがって，定理 4.35 より $\bigcap_i H_i$ は G の部分群である． □

問 4.49 $h \in H$ とする．任意の $a \in H$ について，H は部分群より $ha \in H$ となる．よって，$hH \subset H$ を得る．また，$h^{-1} \in H$ であるので，任意の $a \in H$ について $h^{-1}a \in H$ も従う．つまり，$h^{-1}a = b$（$b \in H$）とかける．よって，$a = hb \in hH$ であり，$H \subset hH$ を得る．以上より，$hH = H$ となる． □

問 4.51　G の単位元 e は $e \in Z(G)$ であるので，$Z(G) \neq \emptyset$ である．そこで，$a, b \in Z(G)$ とする．任意の $x \in G$ に対して $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$ より $ab \in Z(G)$ が従う．また，任意の $x \in G$ に対して，$ax^{-1} = x^{-1}a$ も成り立つので，この両辺の逆元をとれば，$xa^{-1} = (ax^{-1})^{-1} = (x^{-1}a)^{-1} = a^{-1}x$ より $a^{-1} \in Z(G)$ が従う．よって，定理 4.35 より $Z(G)$ は G の部分群である．さらに，$Z(G)$ の元は G のすべての元と交換可能であるので，とくに $Z(G)$ において $ab = ba$ が成り立つ．よって，$Z(G)$ は G の可換な部分群となる．　□

問 4.52　G の単位元 e は $e \in C_a(G)$ であるので，$C_a(G) \neq \emptyset$ である．そこで，$x, y \in C_G(a)$ とする．$a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$ より $xy \in C_G(a)$ が従う．さらに $ax = xa$ の両辺に左右から x^{-1} をかければ，$x^{-1}a = ax^{-1}$ となる．よって $x^{-1} \in C_G(a)$ を得る．したがって，定理 4.35 より $C_G(a)$ は G の部分群となる．

また $a \in Z(G)$ とすれば，任意の $x \in G$ に対して $ax = xa$ が成り立つので，$C_G(a) \supset G$ であり，よって $C_G(a) = G$ となる．逆に，$C_G(a) = G$ であれば，a と交換可能な元は G のすべての元であるので，$a \in Z(G)$ となる．以上より，最後の同値も得られた．　□

問 4.57　(1) $(i_1\ i_2\ i_3\ \cdots\ i_{r-1})(i_{r-1}\ i_r)$ は

$$
\begin{array}{ccccc}
i_1 & \overset{(i_{r-1}\ i_r)}{\longmapsto} & i_1 & \overset{(i_1\ i_2\ i_3\ \cdots\ i_{r-1})}{\longmapsto} & i_2 \\
i_2 & \longmapsto & i_2 & \longmapsto & i_3 \\
\vdots & & \vdots & & \vdots \\
i_{r-2} & \longmapsto & i_{r-2} & \longmapsto & i_{r-1} \\
i_{r-1} & \longmapsto & i_r & \longmapsto & i_r \\
i_r & \longmapsto & i_{r-1} & \longmapsto & i_1
\end{array}
$$

となり，これは $(i_1\ i_2\ i_3\ \cdots\ i_{r-1}\ i_r)$ と一致し，最初の等式が従う．このことがわかれば，次の等式は最初の等式の関係を繰り返すことによって得られる．つまり，

$$
\begin{aligned}
(i_1\ i_2\ i_3\ \cdots\ i_{r-1})(i_{r-1}\ i_r) &= (i_1\ i_2\ i_3\ \cdots\ i_{r-2})(i_{r-2}\ i_{r-1})(i_{r-1}\ i_r) \\
&\vdots \\
&= (i_1\ i_2\ i_3)(i_3\ i_4)\cdots(i_{r-2}\ i_{r-1})(i_{r-1}\ i_r) \\
&= (i_1\ i_2)(i_2\ i_3)(i_3\ i_4)\cdots(i_{r-2}\ i_{r-1})(i_{r-1}\ i_r)
\end{aligned}
$$

となる．

(2) $(i\ j)(i\ k)(i\ j)$ は

$$
\begin{array}{ccccc}
i & \overset{(i\ j)}{\longmapsto} & j & \overset{(i\ k)}{\longmapsto} & j & \overset{(i\ j)}{\longmapsto} & i \\
j & \longmapsto & i & \longmapsto & k & \longmapsto & k \\
k & \longmapsto & k & \longmapsto & i & \longmapsto & j
\end{array}
$$

となり，これは $(j\ k)$ と一致する．

(3) $\sigma,\tau \in S_n$ とするとき，任意の $i \in X_n$ に対して $(\sigma\tau)(i) = (\sigma\tau\sigma^{-1})(\sigma(i))$ である．つまり，

$$\sigma\tau\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ (\sigma\tau)(1) & (\sigma\tau)(2) & \cdots & (\sigma\tau)(n) \end{pmatrix}$$

が成り立つ．よって，とくに $\tau = (i_1\ i_2\ \cdots\ i_r)$ をとるとき，$j \neq i_k$ ならば $(\sigma\tau\sigma^{-1})(\sigma(j)) = (\sigma\tau)(j) = \sigma(j)$ であるので，

$$\begin{aligned} \sigma(i_1\ i_2\ \cdots\ i_r)\sigma^{-1} &= \begin{pmatrix} \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_r) \\ (\sigma\tau)(i_1) & (\sigma\tau)(i_2) & \cdots & (\sigma\tau)(i_r) \end{pmatrix} \\ &= \begin{pmatrix} \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_{r-1}) & \sigma(i_r) \\ \sigma(i_2) & \sigma(i_3) & \cdots & \sigma(i_r) & \sigma(i_1) \end{pmatrix} \\ &= (\sigma(i_1)\ \sigma(i_2)\ \sigma(i_3)\ \cdots\ \sigma(i_{r-1})\ \sigma(i_r)) \end{aligned}$$

が得られる． □

問 4.62 まず，$3 \leq i \neq j \leq n$ に対して，$(1\ 2)(1\ j) = (1\ 2\ j)^2$，$(1\ i)(1\ j) = (1\ 2\ i)(1\ 2\ j)^2$ が成り立つ．たとえば，$(1\ 2)(1\ j)$ と $(1\ 2\ j)^2$ は，

$$\begin{array}{lll} 1 \overset{(1\ j)}{\longmapsto} j \overset{(1\ 2)}{\longmapsto} j & \qquad & 1 \overset{(1\ 2\ j)}{\longmapsto} 2 \overset{(1\ 2\ j)}{\longmapsto} j \\ 2 \longmapsto 2 \longmapsto 1 & & 2 \longmapsto j \longmapsto 1 \\ j \longmapsto 1 \longmapsto 2 & & j \longmapsto 1 \longmapsto 2 \end{array}$$

より一致することがわかる．$(1\ i)(1\ j) = (1\ 2\ i)(1\ 2\ j)^2$ についても同様に示せる．定理 4.52 より S_n は $(1\ i), (2 \leq i \leq n)$ の形の互換で生成されるので，A_n は $(1\ j)(1\ k), (2 \leq j,k \leq n)$ の形の互換の積で生成される．最初に与えた 2 つの関係式より，互換の積 $(1\ j)(1\ k)$ は $(1\ 2\ i), (3 \leq i \leq n)$ によって書けるので，A_n は $(1\ 2\ i), (3 \leq i \leq n)$ の形の巡回置換によって生成されることが従う． □

問 4.77 中心 $Z(G)$ が G の部分群であることは問 4.51 で示した．そこで正規性を示す．$g \in G$ と $a \in Z(G)$ を任意にとる．このとき，$Z(G)$ の定義より $ag = ga$ であるので，$gag^{-1} = a \in Z(G)$ が従う．よって，定理 4.73（正規部分群の判定定理）より $Z(G)$ は G の正規部分群である． □

問 4.102 (1) $f(e) = e' \in H'$ より $e \in f^{-1}(H')$ なので $f^{-1}(H) \neq \emptyset$ である．そこで $a,b \in f^{-1}(H')$ とする．このとき，$f(a) = a'$, $f(b) = b'$（$a', b' \in H'$）と表せば，f の準同型性と H' が G' の部分群であることより $f(ab^{-1}) = f(a)f(b)^{-1} = a'(b')^{-1} \in H'$ となる．よって，$ab^{-1} \in f^{-1}(H')$ を得る．したがって，定理 4.35 より $f^{-1}(H')$ は G の部分群である．

(2) $f(e) = e' \in f(H)$ より $f(H) \neq \emptyset$ である．そこで $a', b' \in f(H)$ とする．このとき．$f(a) = a'$, $f(b) = b'$（$a, b \in H$）と表せて，f の準同型性と H が G の部分群であることより $a'(b')^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(H)$ となる．よって，定理 4.35 より $f(H)$ は G' の部分群である．

(3) (1) より $f^{-1}(H')$ は G の部分群であるので，あとは正規性を示せばよい．任意の $g \in G$ と $a \in f^{-1}(H')$ に対して，$f(a) = a' \in H'$ と表せば，f の準同型性と H' が G' の正規部分群である

ことより $f(gag^{-1}) = f(g)a'f(g)^{-1} \in H'$ となる．よって，$gag^{-1} \in f^{-1}(H')$ を得る．したがって，定理 4.73 より $f^{-1}(H')$ は G の正規部分群である．

(4) (2) より $f(H)$ は G' の部分群であるので，あとは正規性を示せばよい．任意の $g' \in G'$ と $a' \in f(H)$ をとる．f の全射性より $f(g) = g'$ となる $g \in G$ が存在し，また，$f(a) = a'$（$a \in H$）と表せる．f の準同型性と H が G の正規部分群であることより $g'a'(g')^{-1} = f(g)f(a)f(g)^{-1} = f(gag^{-1}) \in f(H)$ となる．よって，定理 4.73 より $f(H)$ は G' の正規部分群である． □

問 4.110 N が G の正規部分群であるので，

$$HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH$$

が成り立つ．よって，定理 4.50 より HN は G の部分群であり，N は HN の正規部分群である．$f(a) \in f(H)$（$a \in H$）とすれば，$f(a) = aN \subset HN$ であるので，$f(a) \in HN/N$ である．よって，$f(H) \subset HN/N$ が従う．また，$hN \in HN/N$ とすれば，$hN = f(h) \in f(H)$ であるので，逆向きの包含関係も従い，$f(H) = HN/N$ を得る． □

問 4.113 g を G から G/M への自然な準同型写像とする．まず，$\mathrm{Ker}(g) = M \supset N$ であるので，$aN = bN$ ならば $a^{-1}b \in N \subset M$ より $aM = bM$ がなりたつ．よって，g により全準同型写像

$$\overline{g} : G/N \ni aN \longmapsto g(a) = aM \in G/M$$

が得られる．このとき，$\mathrm{Ker}(\overline{g}) = M/N$ であるので，準同型定理より $(G/N)/(M/N) \simeq G/M$ が従う． □

問 4.114 (1) 例 4.25 より G 上の全単射全体の集合 $S(G)$ は写像の合成により群であるので，$\mathrm{Aut}(G)$ がその部分群であることを示せば主張が得られる．まず，G 上の恒等写像 id_G は $\mathrm{Aut}(G)$ の元であるので，$\mathrm{Aut}(G) \neq \emptyset$ である．命題 4.91 より $\mathrm{Aut}(G)$ の元の合成は G から G への同型写像であり，$\mathrm{Aut}(G)$ の元の逆写像も再び G から G への同型写像である．つまり，$f, g \in \mathrm{Aut}(G)$ に対して，$fg \in \mathrm{Aut}(G)$ かつ $f^{-1} \in \mathrm{Aut}(G)$ が成り立つ．よって，定理 4.35 より $\mathrm{Aut}(G)$ は $S(G)$ の部分群であるので主張が示せた．

(2) $a \in G$ を固定する．$x, y \in G$ に対して，$\iota_a(xy) = a(xy)a^{-1} = axa^{-1}aya^{-1} = \iota_a(x)\iota_a(y)$ となるので，ι_a は G から G への準同型である．$\iota_a(x) = \iota_a(y)$ とすれば，$axa^{-1} = aya^{-1}$ より $x = y$ を得る．よって，ι_a は単射である．さらに，任意の $y \in G$ に対して $x = a^{-1}ya \in G$ をとれば $\iota_a(x) = a(a^{-1}ya)a^{-1} = y$ より f は全射である．以上より，$\iota_a \in \mathrm{Aut}(G)$ が従う．

(3) (2) より $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$ であり，恒等写像 ι_e は $\mathrm{Inn}(G)$ の元であるので，$\mathrm{Inn}(G)$ は $\mathrm{Aut}(G)$ の空でない部分集合である．$\iota_a, \iota_b \in \mathrm{Inn}(G)$（$a, b \in G$）とする．$(\iota_a\iota_b)(x) = \iota_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \iota_{ab}(x)$ であるので，$\iota_a\iota_b \in \mathrm{Inn}(G)$ となる．また，$\iota_{a^{-1}}(x) = a^{-1}x(a^{-1})^{-1} = a^{-1}xa$ より $(\iota_a\iota_{a^{-1}})(x) = x$ かつ $(\iota_{a^{-1}}\iota_a)(x) = x$ となるので，ι_a の逆写像は

$\iota_{a^{-1}}$ であり，$(\iota_a)^{-1} = \iota_{a^{-1}} \in \mathrm{Inn}(G)$ となる．よって，定理 4.35 より $\mathrm{Inn}(G)$ は $\mathrm{Aut}(G)$ の部分群である．さらに，$\sigma \in \mathrm{Aut}(G)$ について，

$$(\sigma\iota_a\sigma^{-1})(x) = \sigma(a\sigma^{-1}(x)a^{-1}) = \sigma(a)\sigma(\sigma^{-1}(x))\sigma(a^{-1}) = \sigma(a)x\sigma(a)^{-1} = \iota_{\sigma(a)}(x)$$

より $\sigma\iota_a\sigma^{-1} = \iota_{\sigma(a)} \in \mathrm{Inn}(G)$ となる．したがって，定理 4.73 より $\mathrm{Inn}(G)$ は $\mathrm{Aut}(G)$ の正規部分群である．

(4) G から $\mathrm{Inn}(G)$ への写像 f を

$$f \,:\, G \ni a \longmapsto \iota_a \in \mathrm{Inn}(G)$$

と定める．このとき，$a, b \in G$ に対して，(3) で示したように $\iota_a\iota_b = \iota_{ab}$ であるので，$f(ab) = \iota_{ab} = \iota_a\iota_b = f(a)f(b)$ となる．よって，f は準同型である．また，作り方より f は全射である．さらに，

$$\begin{aligned}
\mathrm{Ker}(f) &= \{\, a \in G \mid \iota_a = \mathrm{id}_G \,\} \\
&= \{\, a \in G \mid \text{任意の } x \in G \text{ について } axa^{-1} = x \,\} \\
&= \{\, a \in G \mid \text{任意の } x \in G \text{ について } ax = xa \,\} = Z(G)
\end{aligned}$$

である．したがって，準同型定理より $G/Z(G) \simeq \mathrm{Inn}(G)$ が得られる． □

問 4.122 G の元で位数が d であるものの全体を G_d とする．このとき，$|G_d| \neq 0$ ならば位数 d の元 $a \in G$ が存在し，a で生成される巡回部分群を H とすれば，$|H| = d$ である．いま，$b \in G$ を位数 d の任意の元とすれば，$|\langle b\rangle| = d$ であるので，定理の仮定より $\langle b\rangle = H$ を得る．よって，とくに $b \in H$ となる．つまり，$G_d = H_d$ である．H は位数 d の巡回群であるので，系 4.118 より $|H_d| = \varphi(d)$ となる．したがって，$|G_d| = \varphi(d)$ である．以上より，$|G_d| = 0$ または $|G_d| = \varphi(d)$ であり，n の任意の正の約数 d に対して $|G_d| \leq \varphi(d)$ が成り立つ．

ところで，オイラー関数は $\sum_{d|n,\, d\geq 1} \varphi(d) = n$ をみたす．実際，X を x で生成される位数 m の巡回群とすると，定理 4.117 より X の任意の元の位数は m のある約数 d である．よって，$X = \bigcup_{d|n,\, d\geq 1} X_d$ と表せて，相異なる n の正の約数 d と d' については $X_d \cap X_{d'} = \emptyset$ となる．ここで，定理 4.120 より m の正の約数 d について巡回群 X の位数 d の部分群は唯一つであるので，系 4.118 より $|X_d| = \varphi(d)$ を得る．よって，$n = |G| = \sum_{d|n,\, d\geq 1} \varphi(d)$ が従う．

このオイラー関数の性質とラグランジュの定理より

$$n = \sum_{d|n,\, d\geq 1} |G_d| \leq \sum_{d|n,\, d\geq 1} \varphi(d) = n$$

が得られる．したがって，n の任意の正の約数 d に対して $|G_d| = \varphi(d)$ でなければならない．とくに，G の位数 n について $|G_n| = \varphi(n) \neq 0$ となるので，$G_n \neq \emptyset$ である．つまり，G は位数 $n = |G|$ の元をもつ．よって，G は巡回群である． □

問 4.124　(1) ab の位数を s とする．$g = 1$ なので例題 3.19 より $l = mn$ である．まず，$(ab)^l = (a^m)^n(b^n)^m = e$ より，$s \mid l$ が成り立つ．一方，$(ab)^s = e$ より $a^s = b^{-s}$ であるので，$a^{sn} = (b^{-s})^n = (b^n)^{-s} = e$ となる．よって，$m \mid ns$ であり，$g = 1$ より $m \mid s$ を得る．同様にして，$b^{sm} = e$ より，$n \mid s$ が得られる．したがって，再び $g = 1$ より $l \mid s$ が成り立つ．以上より，$l = s$ が従う．よって，ab の位数は l である．

(2) ab の位数を t とする．$m = m'g$, $n = n'g$（$m', n' \in \mathbb{Z}$）とおくと，$\gcd(m', n') = 1$ であり，例題 3.19 より $l = m'n'g = m'n = mn' = \frac{mn}{g}$ となる．まず，$a' = a^g$, $b' = b^g$ とおけば，a' の位数は m'，b' の位数は n' であり，$\gcd(m', n') = 1$ より (1) から $a'b' = (ab)^g$ の位数は $m'n'$ である．一方，定理 4.117 より $(ab)^g$ の位数は $\frac{t}{\gcd(t,g)}$ であり，仮定より $\gcd(t, g) = g$ なので，$m'n' = \frac{t}{g}$ となる．よって，$t = m'n'g = l$ が得られる．以上より，ab の位数は l である．　□

問 4.131　$\mathbb{R}_{>0}$ と T は共に $\mathbb{C}^\times$ の部分群であり，$\mathbb{R}_{>0} \cap T = \{1\}$ をみたす．したがって系 4.128 より $\mathbb{R}_{>0}T = \mathbb{R}_{>0} \times T$ がわかる（$\mathbb{C}^\times$ はアーベル群なので，条件 (a) は明らかに成り立っている）．また，任意の $z \in \mathbb{C}^\times$ は $z = re^{i\theta}$ $(r = |z|,\ \theta = \arg z)$ と極表示されるが，$r \in \mathbb{R}_{>0}$ かつ $e^{i\theta} \in T$ である．よって $\mathbb{R}_{>0}T = \mathbb{C}^\times$ となり，$\mathbb{C}^\times = \mathbb{R}_{>0} \times T$ を得る．　□

第 4 章　演習問題

演習 1　任意の $a, b \in G$ をとる．仮定より $a^2 = b^2 = e$ であるので，$a = a^{-1}$ かつ $b = b^{-1}$ が成り立つ．$(ab)^2 = e$ であるので $ab = (ab)^{-1}$ も成り立つ．よって，$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ が得られる．したがって G は可換群である．　□

演習 2　例 4.45 の記号を用いれば，

$$D_4 = \langle \sigma, \tau \rangle = \{ e, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3 \}$$

であり，$\sigma^4 = e$, $\tau^2 = e$, $\tau\sigma\tau = \sigma^{-1}$ が成り立つ．簡単な計算により，e の位数は 1，σ と σ^3 の位数は 4，その他の元の位数は 2 であることがわかる．D_4 の位数は 8 なので，ラグランジュの定理より部分群の位数は 1,2,4,8 のいずれかである．

位数 1 の部分群は $\langle e \rangle = \{ e \}$ だけである．また，位数 2 の部分群は $\langle \sigma^2 \rangle$，$\langle \tau \rangle$，$\langle \tau\sigma \rangle$，$\langle \tau\sigma^2 \rangle$，$\langle \tau\sigma^3 \rangle$ の 5 つである．位数 4 の部分群は，一つの元で生成されるものは $\langle \sigma \rangle = \langle \sigma^3 \rangle$ だけであり，2 つの元で生成されるものは，$\langle \sigma^2, \tau \rangle = \langle \sigma^2, \tau\sigma^2 \rangle = \langle \tau, \tau\sigma^2 \rangle = \{ e, \sigma^2, \tau, \tau\sigma^2 \}$ と $\langle \sigma^2, \tau\sigma \rangle = \langle \sigma^2, \tau\sigma^3 \rangle = \langle \tau\sigma, \tau\sigma^3 \rangle = \{ e, \sigma^2, \tau\sigma, \tau\sigma^3 \}$ の 2 つである（これ以外の位数 2 の 2 つの元が生成する群は D_4 となる）．よって，位数 4 の部分群は 3 つある．最後に，位数 8 の部分群は D_4 自身だけである．以上より，D_4 の部分群は $\langle e \rangle$，$\langle \sigma^2 \rangle$，$\langle \tau \rangle$，$\langle \tau\sigma \rangle$，$\langle \tau\sigma^2 \rangle$，$\langle \tau\sigma^3 \rangle$，$\langle \sigma \rangle$，$\{ e, \sigma^2, \tau, \tau\sigma^2 \}$，$\{ e, \sigma^2, \tau\sigma, \tau\sigma^3 \}$，$D_4$ のちょうど 10 個である．

さらに，この中で自明な部分群である $\langle e \rangle$ と D_4 は正規部分群である．また，位数 4 の部分群は D_4 の指数 2（$= \frac{8}{4}$）の部分群であるので，本章演習問題の演習 6 よりすべて正規部分群である．最後に位数 2 の部分群について調べる．まず，$\langle \sigma^2 \rangle$ について，$\sigma^i\sigma^2\sigma^{-i} = \sigma^2 \in \langle \sigma^2 \rangle$，か

つ，$(\tau\sigma^i)\sigma^2(\tau\sigma^i)^{-1} = \tau\sigma^2\tau^{-1} = \sigma^2 \in \langle\sigma^2\rangle$ であるので，定理 4.73 より $\langle\sigma^2\rangle$ は D_4 の正規部分群である．一方，$\sigma\tau\sigma^{-1} = \sigma^2\tau \notin \langle\tau\rangle$，$\tau(\tau\sigma)\tau^{-1} = \tau\sigma^3 \notin \langle\tau\sigma\rangle$，$\sigma(\tau\sigma^2)\sigma^{-1} = \tau \notin \langle\tau\sigma^2\rangle$，$\tau(\tau\sigma^3)\tau^{-1} = \tau\sigma \notin \langle\tau\sigma^3\rangle$ より，残り 4 つの位数 2 の部分群は D_4 の正規部分群ではない．以上より，D_4 の正規部分群は $\langle e\rangle$，$\langle\sigma^2\rangle$，$\langle\sigma\rangle$，$\{\, e, \sigma^2, \tau, \tau\sigma^2 \,\}$，$\{\, e, \sigma^2, \tau\sigma, \tau\sigma^3 \,\}$，$D_4$ の 6 個である． □

演習 3　S_4 の元は $4! = 24$ 個である．恒等置換 e は $X_4 = \{\, 1, 2, 3, 4 \,\}$ の元をすべて固定するので，本書ではとくに用いなかったが巡回置換として表せば，すべての数が省略できて $e = (\ )$ と表せ，位数は 1 である．次に，互換は (1 2)，(1 3)，(1 4)，(2 3)，(2 4)，(3 4) の 6 個あり，位数は 2 である．長さ 3 の巡回置換は (1 2 3)，(1 2 4)，(1 3 2)，(1 3 4)，(1 4 2)，(1 4 3)，(2 3 4)，(2 4 3) の 8 個あり，位数は 3 である．長さ 4 の巡回置換は (1 2 3 4)，(1 2 4 3)，(1 3 2 4)，(1 3 4 2)，(1 4 2 3)，(1 4 3 2) の 6 個あり，位数は 4 である．一つの巡回置換で表せる S_4 の元は以上の 21 個である．これ以外の S_4 の元は，X_4 の元をちょうど 2 つずつ入れ替える置換であり，(1 2)(3 4)，(1 3)(2 4)，(1 4)(2 3) の 3 個があり，互いに素な互換の積であるので位数は 2 である．以上をまとめると，S_4 の元は

( )：位数 1,
(1 2), (1 3), (1 4), (2 3), (2 4), (3 4)：位数 2,
(1 2 3), (1 2 4), (1 3 2), (1 3 4), (1 4 2), (1 4 3), (2 3 4), (2 4 3)：位数 3,
(1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)：位数 4,
(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)：位数 2

となる． □

演習 4　H は部分群であるので単位元 e をもつ．よって，$aHa^{-1} \ni aea^{-1} = e$ より $aHa^{-1} \neq \emptyset$ である．$aha^{-1}, aka^{-1} \in aHa^{-1}$（$h, k \in H$）とする．$H$ は部分群であるので $hk \in H$ より，$(aha^{-1})(aka^{-1}) = ahka^{-1} \in aHa^{-1}$ が成り立つ．また，H は部分群であるので $h^{-1} \in H$ より，$(aha^{-1})^{-1} = (a^{-1})^{-1}h^{-1}a^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$ が成り立つ．よって，定理 4.35 より aHa^{-1} は G の部分群である． □

演習 5　n 次単位行列 E は $E \in O(n)$ であるので，$O(n) \neq \emptyset$ である．$A, B \in O(n)$ とする．まず，${}^t(B^{-1}){}^tB = {}^t(BB^{-1}) = {}^tE = E$ より ${}^t(B^{-1}) = ({}^tB)^{-1}$ となるので，${}^t(AB^{-1})(AB^{-1}) = {}^t(B^{-1}){}^tAAB^{-1} = {}^t(B^{-1})B^{-1} = ({}^tB)^{-1}B^{-1} = (B\,{}^tB)^{-1} = E^{-1} = E$ である．同様にして $(AB^{-1})\,{}^t(AB^{-1}) = E$ も得られる．したがって，$AB^{-1} \in O(n)$ が成り立つ．よって，定理 4.35 より $O(n)$ は $GL(n, \mathbb{R})$ の部分群である． □

演習 6　N は G の指数 2 の部分群であるので，G の N による右剰余類分解は 2 つの右剰余類によって $G = N \cup aN$（$a \in G - N$，$N \cap aN = \emptyset$）となる．まず，$x \in N$ ならば $xN = N = Nx$ が成り立つ．次に，$x \in aN$（つまり，$x \in G$ かつ $x \notin N$）ならば $xN = aN$ であり，G の N による

左剰余類分解は $G = N \cup Na$（$N \cap Na = \emptyset$）であるので，$x \notin N$ より $x \in Na = G - N = aN$ となる．よって，$xN = aN = Na = Nx$ が成り立つ．以上より，任意の $x \in G = N \cup aN$ について $xN = Nx$ が示せた．したがって，N は G の正規部分群である． □

演習 7　H を $\mathbb{R}$ の有限指数の部分群とし，$n = [\mathbb{R} : H]$（$< \infty$）とする．$\mathbb{R}$ は加法群であるので H は $\mathbb{R}$ の正規部分群である．よって，剰余群 $\mathbb{R}/H$ が得られる．$\mathbb{R}/H$ の位数は n であるので，任意の $r \in \mathbb{R}$ に対して $nr \in H$ となる．よって，$n\mathbb{R} = \{\, nr \mid r \in \mathbb{R} \,\} \subset H$ である．ところで，任意の $r \in \mathbb{R}$ は $r = n\frac{r}{n}$ と書けるので，$\mathbb{R} \subset n\mathbb{R}$ となる．つまり，$\mathbb{R} = n\mathbb{R}$ である．したがって，$\mathbb{R} \subset H$ を得る．$H \subset \mathbb{R}$ であったので，結局 $H = \mathbb{R}$ が従う．つまり，$\mathbb{R}$ の有限指数の部分群は $\mathbb{R}$ だけである．よって，加法群 $\mathbb{R}$ は $\mathbb{R}$ 以外の有限指数の部分群をもたない． □

演習 8　G を位数 4 の群とする．このとき G の元の位数は 1,2,4 のいずれかである．G が位数 4 の元をもてば，G は位数 4 の巡回群であるから $G \simeq \mathbb{Z}/4\mathbb{Z}$ である．そこで，G は位数 4 の元をもたないとする．このとき，位数が 1 の元は単位元だけなので，G は単位元 e と 3 つの位数 2 の元からなる群となる．すると，任意の $a \in G$ について $a^2 = e$ が成り立つので，本章演習問題の演習 1 より G は可換群である．G の 3 つの位数 2 の元を σ, τ, ρ で表す．もし $\sigma\tau = e$ ならば $\sigma = \tau^{-1} = \tau$ となり矛盾，もし $\sigma\tau = \sigma$ ならば $\tau = e$ となり矛盾，もし $\sigma\tau = \tau$ ならば $\sigma = e$ となり矛盾であるので，$\sigma\tau = \rho$ でなければならない．同様にして $\tau\rho = \sigma$, $\rho\sigma = \tau$ となるので，G が可換群であったことから，G の演算表は次のようになる．

積	1	σ	τ	ρ
1	1	σ	τ	ρ
σ	σ	1	ρ	τ
τ	τ	ρ	1	σ
ρ	ρ	τ	σ	1

よって，G はクラインの 4 元群（問 4.30）と一致し，$G = \langle \sigma, \tau \rangle$ である．そこで，G から $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ への写像 f を

$$f \,:\, G \ni \sigma^i\tau^j \longmapsto (\,\overline{i}, \overline{j}\,) \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \qquad (i, j \in \{\,0, 1\,\})$$

により定めれば，f は同型写像であること直ちに確かめられ，同型 $G \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ が得られる．以上より，位数 4 の群は $\mathbb{Z}/4\mathbb{Z}$ または $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ のいずれかと同型である．

なお，定理 5.14（アーベル群の基本定理）を用いれば，位数 4 の元をもたない位数 4 の可換群は，$4 = 2^2$ より $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ と同型であることが直ちに結論できる． □

演習 9　本章演習問題の演習 2 で見たように，例 4.45 の記号を用いれば，D_4 の位数 2 の元は σ^2，τ，$\tau\sigma$，$\tau\sigma^2$，$\tau\sigma^3$ の 5 つある．一方，問 4.31 の記号を用いれば，四元数群の位数 2 の元は $-E$ ただ 1 つだけである．よって，D_4 と四元数群の間に同型写像をつくることはできない．実際，f を D_4 から四元数群への同型写像とすると，f の単射性より像が E となる元は e だけである．よって，

たとえば σ^2 の像は $f(\sigma^2)^2 = f(\sigma^4) = f(e) = E$ となるが，$f(\sigma^2) \neq E$ より $f(\sigma^2)$ は位数 2 の元となり，$f(\sigma^2) = -E$ でなければならない．一方，$f(\tau$ についても $f(\tau)^2 = f(\tau^2) = f(e) = E$ となるので，同様に $f(\tau)$ も位数 2 の元となり，$f(\tau) = -E$ しかあり得ない．よって，$f(\sigma^2) = f(\tau)$ となるが，これは f の単射性に矛盾する．したがって，D_4 と四元数群は同型ではない． □

演習 10 まず $\mathrm{Aut}(\mathbb{Z})$ について考える．$f \in \mathrm{Aut}(\mathbb{Z})$ とする．$n \in \mathbb{Z}$ について n は 1 の n 個の和なので，準同型性より $f(n) = nf(1)$ が成り立つ．よって，f の像は $f(1)$ の倍数全体，つまり，$\mathrm{Im}(f) = \langle f(1) \rangle$ である．したがって，f が全射であるためには $f(1) = \pm 1$ でなければならない．

$f(1) = 1$ によって定まる準同型写像を改めて f_1 で表せば，$f_1(n) = n$ であるので，f_1 は恒等写像 $\mathrm{id}_{\mathbb{Z}}$ である．よって，f_1 は $\mathbb{Z}$ の自己同型写像である．また $f(1) = -1$ によって定まる準同型写像 f_{-1} で表せば，$f_{-1}(n) = -n$ である．よって，f_{-1} も $\mathbb{Z}$ の自己準同型写像であることが直ちに確かめられる．このとき，$f_{-1}^2(n) = f_{-1}(f_{-1}(n)) = f_{-1}(-n) = -(-n) = n$ となるので，$f_{-1}^2 = \mathrm{id}_{\mathbb{Z}}$ である．以上より，$\mathrm{Aut}(\mathbb{Z}) = \{ \mathrm{id}_{\mathbb{Z}}, f_{-1} \} = \langle f_{-1} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ となる．

次に $\mathrm{Aut}(\mathbb{Q})$ について考える．$f \in \mathrm{Aut}(\mathbb{Q})$ とする．まず $\mathrm{Aut}(\mathbb{Z})$ のときと同様に $n \in \mathbb{Z}$ については $f(n) = nf(1)$ である．また，$m \in \mathbb{Z}$（$m \neq 0$）とするとき，1 は $\frac{1}{m}$ の m 個の和であるので，f の準同型性より $f(1) = mf(\frac{1}{m})$ となる．よって，$\frac{1}{m} f(1) = f(\frac{1}{m})$ が成り立つ．したがって，正の有理数 $r = \frac{n}{m}$ に対して，$f(r) = nf(\frac{1}{m}) = n\frac{1}{m} f(1) = rf(1)$ となる．さらに準同型性より，$f(-r) = -f(r) = -rf(1)$ であるので，任意の $q \in \mathbb{Q}$ に対して $f(q) = qf(1)$ が成り立つ．よって，$\mathrm{Aut}(\mathbb{Q})$ の元 f は $f(1)$ を決めることによって決定される．

$f(1) = 0$ と定めると，f は零写像となり，$f \notin \mathrm{Aut}(\mathbb{Q})$ である．そこで，$a \in \mathbb{Q}^\times = \mathbb{Q} - \{ 0 \}$ として，$f(1) = a$ によって定まる写像を f_a で表せば，$q \in \mathbb{Q}$ に対して $f_a(q) = qa$ となる．f_a は a 倍写像であり，例 4.88 と同様に全単射な準同型写像となる．したがって，$a \in \mathbb{Q}^\times$ ならば $f_a \in \mathrm{Aut}(\mathbb{Q})$ である．

そこで，$\mathrm{Aut}(\mathbb{Q})$ から $\mathbb{Q}^\times$ への写像 σ を

$$\sigma \ : \ \mathrm{Aut}(\mathbb{Q}) \ni f \longmapsto f(1) \in \mathbb{Q}^\times$$

と定めれば，$f(1)$ の値を一つ決めれば $f \in \mathrm{Aut}(\mathbb{Q})$ が一つ決まるので σ は単射であり，任意の $a \in \mathbb{Q}^\times$ に対して $f(1) = a$ により $f \in \mathrm{Aut}(\mathbb{Q})$ が得られたので σ は全射である．さらに，$f, g \in \mathrm{Aut}(\mathbb{Q})$ とすれば，$\sigma(fg) = (fg)(1) = f(g(1)) = g(1)f(1) = f(1)g(1) = \sigma(f)\sigma(g)$ （$g(1) \in \mathbb{Q}^\times$ であるので $g(1) = b$ とおけば $f(b) = bf(1)$ である）より σ は準同型である．したがって，σ は同型であり，$\mathrm{Aut}(\mathbb{Q}) \simeq \mathbb{Q}^\times$ となる． □

演習 11 $\mathbb{Q}/\mathbb{Z}$ は加法群 $\mathbb{Q}$ の（正規）部分群 $\mathbb{Z}$ による剰余群である．任意の $\overline{q} \in \mathbb{Q}/\mathbb{Z}$ をとれば，$q = \frac{n}{m}$（$m, n \in \mathbb{Z}$，$m \neq 0$）と表せるので，m 倍すると $m\overline{q} = \overline{n} = \overline{0}$ となる．よって，すべての $\overline{q} \in \mathbb{Q}/\mathbb{Z}$ は $\mathbb{Q}/\mathbb{Z}$ で有限位数である． □

演習 12 指数に 0 も許し共通の素数を使って，m と n の素因数分解を $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$，$n = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ （e_i と f_i は 0 以上の整数であり，$p_1, p_2, \ldots, p_r$ はすべて相異なる素数）とする．こ

のとき，$h_i = \max(e_i, f_i)$ とおけば，問 3.35 より m と n の最小公倍数は $l = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$ である．そこで，

$$m_i = \frac{m}{p_i^{e_i}} = \prod_{j=1,\, j\neq i}^{r} p_j^{e_j}, \quad n_i = \frac{n}{p_i^{f_i}} = \prod_{j=1,\, j\neq i}^{r} p_j^{f_j}$$

とおき，$c_i \in G$ を

$$c_i = \begin{cases} a^{m_i} & (h_i = e_i \geq f_i \text{ のとき}) \\ b^{n_i} & (h_i = f_i \geq e_i \text{ のとき}) \end{cases}$$

と定めると，定理 4.117 より $c_i \in G$ の位数は $p_i^{h_i}$ である．よって，$d_1 = c_1 c_2 \in G$ とおけば，$\gcd(p_1^{h_1}, p_2^{h_2}) = 1$ なので，問 4.124 より d_1 の位数は $p_1^{h_1} p_2^{h_2}$ である．さらに，$d_2 = d_1 c_3 = c_1 c_2 c_3 \in G$ とおけば，d_1 と c_3 の位数は互いに素なので，再び問 4.124 より d_2 の位数は $p_1^{h_1} p_2^{h_2} p_3^{h_3}$ となる．これを繰り返せば，$d = c_1 c_2 \cdots c_r \in G$ とおくと，d の位数は $p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r} = l$ となる．したがって，G には位数 l の元が存在する． □

演習 13　(1) (i) $[a,b] = e \Longleftrightarrow aba^{-1}b^{-1} = e \Longleftrightarrow ab = ba$ である．

(ii) $[a,b][b,a] = (aba^{-1}b^{-1})(bab^{-1}a^{-1}) = e$ であり，同様にして $[b,a][a,b] = e$ であるので，$[a,b]^{-1} = [b,a]$ が従う．

(iii) 右辺の式を定義に従って計算すれば，

$$\begin{aligned} [cac^{-1}, cbc^{-1}] &= (cac^{-1})(cbc^{-1})(cac^{-1})^{-1}(cbc^{-1})^{-1} \\ &= cabc^{-1}(ca^{-1}c^{-1})(cb^{-1}c^{-1}) \\ &= caba^{-1}b^{-1}c^{-1} = c[a,b]c^{-1} \end{aligned}$$

となる．

(2) G が可換群であれば，任意の $a, b \in G$ は $ab = ba$ であるので，(1) の (i) より $[a,b] = e$ である．よって，$D(G)$ は e で生成される G の部分群，つまり，$D(G) = \{\, e \,\}$（単位群）である．逆に，$D(G)$ が単位群であれば，すべての交換子 $[a,b]$ は e であるので，(1) の (i) より任意の $a, b \in G$ について $ab = ba$ が成り立つ．よって，G は可換群である． □

演習 14　$D(G) \subset H$ とする．$h \in H$ と $a \in G$ に対して，$aha^{-1} = [a,h]h \in H$ となるので，定理 4.73 より H は G の正規部分群である．これより G の H による剰余群 G/H が得られる．また，任意の $a, b \in G$ に対して，$D(G) \subset H$ より $[a^{-1}, b^{-1}]H = H$ である．よって，

$$(aH)(bH) = abH = ba[a^{-1}, b^{-1}]H = baH = (bH)(aH)$$

となる．したがって，剰余群 G/H は可換群となる．

逆に，(2) が成り立つとする．このとき，任意の $a, b \in G$ に対して，$(aH)(bH) = (bH)(aH)$ であるので，

$$[a,b]H = (aba^{-1}b^{-1})H = (aH)(bH)(aH)^{-1}(bH)^{-1} = H$$

となり，$[a,b] \in H$ を得る．よって，$D(G) \subset H$ である． □

演習 15　(1) S_1 と S_2 は可換群であり，$A_1 = A_2 = \{\, e \,\}$ であるので，本章末演習問題の演習 13 の (2) より $n = 1, 2$ のときには主張は成り立つ．そこで，$n \geq 3$ とする．まず，S_n の交換子は定義より偶置換であるので，$D(S_n) \subset A_n$ が成り立つ．一方，相異なる自然数 i, j, k に対して $[(i\ j), (i\ k)] = (i\ j\ k)$ となることがすぐに確かめられる．よって，とくに $i = 1$，$j = 2$ とおけば，$3 \leq k \leq n$ に対して $[(1\ 2), (1\ k)] = (1\ 2\ k)$ が成り立つ．つまり，$(1\ 2\ k) \in D(S_n)$ である．定理 4.62 より，$3 \leq k \leq n$ について $(1\ 2\ k)$ は A_n の生成系をなしたので，$D(S_n) \supset A_n$ が従う．以上より，$D(S_n) = A_n$ である．

(2) まず，$S_n \supset A_n$ より $D(S_n) \supset D(A_n)$ となるので，(1) より $A_n \supset D(A_n)$ は直ちに従う．よって，逆向きの包含関係を示す．

相異なる自然数 i, j, k, l, m に対して $[(i\ j\ m), (i\ k\ l)] = (i\ j\ k)$ となることが直ちに確かめられる．よって，とくに $i = 1$，$j = 2$ とおけば，相異なる $3 \leq k, l, m \leq n$ に対して $[(1\,2\,m), (1\,k\,l)] = (1\,2\,k)$ が成り立つ．よって，$(1\ 2\ m), (1\ k\ l) \in A_n$ より，$3 \leq k \leq n$ に対して $(1\ 2\ k) \in D(A_n)$ となる．したがって，定理 4.62 より $A_n \subset D(A_n)$ である．以上より，$D(A_n) = A_n$ を得る．　□

演習 16　(1) V に含まれる id でない 2 つの元の積は残りの id でない元になることが計算により確かめられる（これにより id でない元が交換律をみたすこともわかる）．id は単位元であるので，以上のことより V は S_4 の演算で閉じている．また，単位元 id の逆元は単位元であり，互いに素な互換の積は位数が 2 であるので自分自身が逆元となる．これより V の元は V に逆元をもつ．したがって，定理 4.35 より V は S_4 の部分群である．

さらに，$(1\ 2)(3\ 4)$ と $(1\ 3)(2\ 4)$ の積は $(1\ 4)(2\ 3)$ であるので，V は $(1\ 2)(3\ 4)$ と $(1\ 3)(2\ 4)$ によって生成されることが従う．

(2) V からクラインの 4 元群 $G = \{\, 1, \sigma, \tau, \rho \,\}$（問 4.30 の記号）への写像 f を

$$V \xrightarrow{f} G \ : \ \begin{cases} \mathrm{id} & \longmapsto & 1 \\ (1\ 2)(3\ 4) & \longmapsto & \sigma \\ (1\ 3)(2\ 4) & \longmapsto & \tau \\ (1\ 4)(2\ 3) & \longmapsto & \rho \end{cases}$$

により定めると，作り方より全単射であり，また準同型であることも直ちに確かめられる．よって，f は群の同型写像であり，V はクラインの四元群と同型である．本章演習問題の演習 8 の解答で調べたようにクラインの四元群は $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ と同型であったので，$V \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ となり，よって可換群となる．（なお，任意の $\sigma \in V$ は $\sigma^2 = \mathrm{id}$ を満たすので，本章演習問題の演習 1 からも V は可換群であることがわかる．）

(3) 任意の $\sigma \in S_4$ と 2 つの互いに素な互換の積 $\tau = (i\ j)(k\ l)$ に対して，問 4.57 により

$$\sigma\tau\sigma^{-1} = \sigma(i\ j)\sigma^{-1}\sigma(k\ l)\sigma^{-1} = (\sigma(i)\ \sigma(j))(\sigma(k)\ \sigma(l)) \in V$$

が成り立つ（σ が全単射であることも用いている）．また，任意の $\sigma \in S_4$ と id についても，$\sigma\,\mathrm{id}\,\sigma^{-1} = \mathrm{id} \in V$ が成り立つ．したがって，定理 4.73 の (4) より部分群 V は S_4 の正規部分群である．

(4) 問 4.62 より $A_4 = \langle (1\ 2\ 3), (1\ 2\ 4) \rangle$ である．また，

$$[(1\ 2\ 3), (1\ 2\ 4)] = (1\ 2)(3\ 4), \quad [(1\ 2\ 3)^2, (1\ 2\ 4)] = (1\ 3)(2\ 4)$$

となることが直ちに確かめられる．よって，V の生成系 $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4)\}$ は A_4 の交換子で与えられる．したがって，$D(A_4) \supset V$ である．一方，例 4.107 より A_4 は S_4 の正規部分群であり，(3) より V は A_4 の正規部分群であったので，ラグランジュの定理より

$$|A_4| = \frac{|S_4|}{[S_4 : A_4]} = \frac{4!}{2} = 12, \quad |A_4/V| = \frac{|A_4|}{|V|} = \frac{12}{4} = 3$$

となる．よって，剰余群 A_4/V は位数 3 の群である．位数が素数であるので，命題 4.123 より $A_4/V \simeq \mathbb{Z}/3\mathbb{Z}$ であり，とくに A_4/V は可換群である．よって，本章演習問題の演習 14 の (2) より $V \supset D(A_4)$ となる．したがって，$D(A_4) = V$ である．

最後に，V は可換群であるので，本章演習問題の演習 13 より，$D(V) = \{\,\mathrm{id}\,\}$ であることもわかる． □

第 5 章　問

問 5.3　(1)　行列の積の定義より明らか.

(2)　まず (1) より $\gcd(A) \mid \gcd(QAP)$．また，$A = Q^{-1}(QAP)P^{-1}$ であり，P^{-1} と Q^{-1} の成分はすべて整数であるから，再び (1) より $\gcd(QAP) \mid \gcd(A)$．以上より $\gcd(QAP) = \gcd(A)$ を得る．　□

問 5.4　容易に確かめられるように

$$S_{ij}^2 = E, \qquad T_i^2 = E, \qquad U_{ij}(a)\,U_{ij}(b) = U_{ij}(a+b)$$

が成り立つ．これより直ちに主張を得る．　□

問 5.12　(1)　$x, y \in G_{\mathrm{tor}}$ とすると，$mx = ny = 0$ となるような $m, n \in \mathbb{Z}_{>0}$ が存在する．このとき

$$(mn)(x-y) = (mn)x - (mn)y = n(mx) - m(ny) = 0 - 0 = 0$$

となるから，$x - y \in G_{\mathrm{tor}}$．また，$0 \in G_{\mathrm{tor}}$ より G_{tor} は空でない．したがって G_{tor} は G の部分群である．

(2)　$x = (x_1, x_2, \ldots, x_r) \in G$ $(x_i \in G_i)$ とするとき，$n \in \mathbb{Z}_{>0}$ に対して $nx = (nx_1, nx_2, \ldots, nx_r)$ が成り立つ．とくに $nx = (0, 0, \ldots, 0)$ であれば，各 i について $nx_i = 0$．したがって $x \in G_{\mathrm{tor}}$ ならば $x_i \in (G_i)_{\mathrm{tor}}$ となる．逆に，各 i について $n_i x_i = 0$ であれば，$n := n_1 n_2 \cdots n_r$ に対して $nx = (0, 0, \ldots, 0)$．したがって $x_i \in (G_i)_{\mathrm{tor}}$ ならば $x \in G_{\mathrm{tor}}$ となる．以上より，$x \in G_{\mathrm{tor}}$ であるためには，各 i について $x_i \in (G_i)_{\mathrm{tor}}$ であることが必要かつ十分であることがわかる．つまり，集合 G_{tor} は直積集合 $(G_1)_{\mathrm{tor}} \times (G_2)_{\mathrm{tor}} \times \cdots \times (G_r)_{\mathrm{tor}}$ に一致する．これが群の直積分解でもあることは，群の直積の定義より明らかである．　□

問 5.22　(1)　$\widetilde{\chi} \in \mathrm{Ker}(\varpi^*)$ とすると，任意の $a \in G$ に対して $\widetilde{\chi}(\varpi(a)) = 1$，すなわち $\widetilde{\chi}(aH) = 1$ が成り立つから，$\widetilde{\chi}$ は G/H の単位指標となる．よって ϖ^* は単射である．

(2)　まず，$a \in H$ に対しては $\widetilde{\chi}(\varpi(a)) = \widetilde{\chi}(H) = 1$ が成り立つから，$\mathrm{Im}(\varpi^*) \subset A_G(H)$．逆に，$\chi \in A_G(H)$ とするとき，$\widetilde{\chi} : G/H \to \mathbb{C}^\times$ を $\widetilde{\chi}(aH) = \chi(a)$ により定めることができる．実際，$aH = bH$ をみたす $a, b \in G$ に対し，$b = ah$ $(h \in H)$ とすると，$\chi(h) = 1$ より $\chi(b) = \chi(ah) = \chi(a)\,\chi(h) = \chi(a)$ となる．こうして定めた写像 $\widetilde{\chi}$ は，容易にわかるように群の準同型であり，G/H の指標を与える．また，明らかに $\varpi^*(\widetilde{\chi}) = \chi$．以上より $\mathrm{Im}(\varpi^*) = A_G(H)$ を得る．　□

第 5 章　演習問題

演習 1　$M = \langle \boldsymbol{a} \rangle$ に定理 5.2 を適用すると，1 次独立なベクトル $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n \in \mathbb{Z}^n$ と $c \in \mathbb{Z}_{>0}$ で

$$\mathbb{Z}^n = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n \rangle, \qquad M = \langle c\boldsymbol{u}_1 \rangle$$

をみたすものが存在することがわかる．後者の等式より $\boldsymbol{a} = \pm c\boldsymbol{u}_1$ がわかるから，c は $a_1, a_2, \ldots, a_n$ の公約数である．したがって仮定より $c = 1$ となり，$\boldsymbol{a} = \pm \boldsymbol{u}_1$ を得る．他方，前者の等式より行列 $\begin{pmatrix} \boldsymbol{u}_1 & \boldsymbol{u}_2 & \ldots & \boldsymbol{u}_n \end{pmatrix}$ は正則，したがってその行列式は ± 1 であることがわかる．以上より $\det\begin{pmatrix} \boldsymbol{a} & \boldsymbol{u}_2 & \ldots & \boldsymbol{u}_n \end{pmatrix} = \pm 1$ がわかる．この行列式が -1 の場合には，$\boldsymbol{u}_2$ を $-\boldsymbol{u}_2$ で置き換えれば行列式が 1 となるようにできる．　□

演習 2　定理 5.6 より，n 次の正則行列 P, Q と $a_1, a_2, \ldots, a_s \in \mathbb{Z}_{>0}$ で

$$QAP = \begin{pmatrix} a_1 & & & & 0 \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_s & \\ 0 & & & & \end{pmatrix}$$

をみたすものが存在する．このとき，$|\det(P)| = |\det(Q)| = 1$ より，

$$|\det(A)| = \begin{cases} a_1 a_2 \cdots a_n & (s = n \text{ の場合}) \\ 0 & (s < n \text{ の場合}) \end{cases}.$$

また，$\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n \in \mathbb{Z}^n$ を

$$Q^{-1} = \begin{pmatrix} \boldsymbol{u}_1 & \boldsymbol{u}_2 & \ldots & \boldsymbol{u}_n \end{pmatrix}$$

により定めると，定理 5.2 の証明と同様にして

$$\mathbb{Z}^n = \langle \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n \rangle, \qquad \mathrm{Im}(f) = \langle a_1\boldsymbol{u}_1, a_2\boldsymbol{u}_2, \ldots, a_s\boldsymbol{u}_s \rangle$$

がわかる．さらに，補題 5.10 より

$$\mathbb{Z}^n / \mathrm{Im}(f) \cong (\mathbb{Z}/a_1\mathbb{Z}) \times (\mathbb{Z}/a_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_s\mathbb{Z}) \times \mathbb{Z}^{n-s}$$

となるから，

$$[\mathbb{Z}^n : \mathrm{Im}(f)] = \begin{cases} a_1 a_2 \cdots a_n & (s = n \text{ の場合}) \\ \infty & (s < n \text{ の場合}) \end{cases}.$$

以上より主張を得る．　□

演習 3　(1) 位数 1 の（アーベル）群は単位群 $\{0\}$ の 1 通り．

(2) 素数 $p = 2, 3, 5, 7$ に対し，位数 p の（アーベル）群は $\mathbb{Z}/p\mathbb{Z}$ の 1 通り（命題 4.123 も参照のこと）．

(3) 位数 4 のアーベル群は $\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ の 2 通り．

(4) 位数 6 のアーベル群は $\mathbb{Z}/6\mathbb{Z}$ の 1 通り．

(5) 位数 8 のアーベル群は $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ の 3 通り．

(6) 位数 9 のアーベル群は $\mathbb{Z}/9\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ の 2 通り．

(7) 位数 10 のアーベル群は $\mathbb{Z}/10\mathbb{Z}$ の 1 通り．　□

演習 4　$\widehat{f}_\chi, \widehat{g}_\chi$ の定義より

$$\sum_{\chi \in \widehat{G}} \widehat{f}_\chi \, \overline{\widehat{g}_\chi} = \sum_{\chi \in \widehat{G}} \Big(\sum_{a \in G} f(a) \, \overline{\chi}(a) \Big) \overline{\Big(\sum_{b \in G} g(b) \, \overline{\chi}(b) \Big)} = \sum_{a \in G} \sum_{b \in G} f(a) \, \overline{g(b)} \sum_{\chi \in \widehat{G}} \overline{\chi}(a) \, \chi(b).$$

ここで，命題 5.25 の (2) より

$$\sum_{\chi \in \widehat{G}} \overline{\chi}(a) \, \chi(b) = \sum_{\chi \in \widehat{G}} \chi(a^{-1}b) = \begin{cases} |G| & (a = b \text{ の場合}) \\ 0 & (a \neq b \text{ の場合}) \end{cases}$$

がわかるから，

$$\sum_{\chi \in \widehat{G}} \widehat{f}_\chi \, \overline{\widehat{g}_\chi} = |G| \sum_{a \in G} f(a) \, \overline{g(a)}$$

となる．　□

演習 5　数列の周期性より，群 $\mathbb{Z}/m\mathbb{Z}$ 上の複素数値関数 f を

$$f(k + m\mathbb{Z}) := a_k \qquad (k \in \mathbb{Z}_{\geq 0})$$

により定義することができる．また，指標群 $(\mathbb{Z}/m\mathbb{Z})^\wedge$ は

$$\chi(k + m\mathbb{Z}) := \zeta_m^k \qquad (k \in \mathbb{Z})$$

により定義される χ で生成される，位数 m の巡回群である．したがって，関数 f に系 5.26 を適用すると，

$$\widehat{f}_{\chi^l} = \sum_{k=0}^{m-1} f(k + m\mathbb{Z}) \, \overline{\chi^l}(k + m\mathbb{Z}) = \sum_{k=0}^{m-1} a_k \, \zeta_m^{-kl} \qquad (0 \leq l \leq m-1)$$

に対して

$$f(k + m\mathbb{Z}) = \frac{1}{m} \sum_{l=0}^{m-1} \widehat{f}_{\chi^l} \, \chi^l(k + m\mathbb{Z}) = \frac{1}{m} \sum_{l=0}^{m-1} \widehat{f}_{\chi^l} \, \zeta_m^{kl} \qquad (0 \leq k \leq m-1)$$

が成り立つことがわかる．　□

第 6 章　問

問 6.16　$n \cdot a = (\sum_{i=1}^{n} 1)a = \sum_{i=1}^{n} 1 \cdot a = \sum_{i=1}^{n} a = na$ となる．

なお，$\mathbb{Z} \subset R$ であれば，整数倍の定め方から $1 \in \mathbb{Z}$ は R の単位元である．$\mathbb{Z}$ の元の差や積も再び $\mathbb{Z}$ の元であるので，6.2 節の用語を用いれば，定理 6.39 より $\mathbb{Z}$ は R の部分環ということになる．□

問 6.17　(1) 分配律を用いると，差の定義と命題 6.15 より，$a(b-c) = a(b+(-c)) = ab+a(-c) = ab+(-ac) = ab-ac$ となる．同様にして，$(a-b)c = ac-bc$ も示せる．

(2) $(a+b)+(-a-b) = a+b+(-a+(-b)) = a+b+(-a)+(-b) = a+(-a)+b+(-b) = 0+0 = 0$ であり，加法は交換律をみたすので，$a+b$ の加法の逆元は $-a-b$ である．つまり，$-(a+b) = -a-b$ が成り立つ．同様にして，$(a-b)+(-a+b) = 0$ より，$-(a-b) = -a+b$ が成り立つこともわかる．□

問 6.18　A が左零因子であるとすると，$AB = O$ となる n 次正方行列 $B \neq O$ が存在する．とくに，B の列ベクトル $\mathbf{x} \in \mathbb{R}^n$，$\mathbf{x} \neq \mathbf{o}$ で $A\mathbf{x} = \mathbf{o}$ となるものが存在するので，$\det(A) = 0$ である．よって，(1) $\Rightarrow$ (3) が従う．

次に，$\det(A) = 0$ とすると，$A\mathbf{x} = \mathbf{o}$ なる列ベクトル $\mathbf{x} \in \mathbb{R}^n$，$\mathbf{x} \neq \mathbf{o}$ が存在する．そこで，すべての列ベクトルが $\mathbf{x}$ である n 次正方行列を $B = (\mathbf{x}\ \mathbf{x}\ \cdots\ \mathbf{x})$ とすれば，$B \neq O$ かつ $AB = O$ となるので，A は左零因子である．よって，(3) $\Rightarrow$ (1) が得られる．

ところで，A が左零因子であれば，$\det(A) = 0$ なので，A の転置行列 ${}^tA$ についても $\det({}^tA) = 0$ となる．よって，${}^tA$ も左零因子であり，${}^tAC = O$ となる n 次正方行列 $C \neq O$ が存在する．この両辺の転置をとれば，${}^tCA = O$ かつ ${}^tC \neq O$ であるので，A は右零因子でもある．A が右零因子である場合にも，同様にして A は左零因子となることがわかるので，(1) $\Leftrightarrow$ (2) が従う．

以上より，(1), (2), (3) は同値である．□

問 6.50　次数 n に関する数学的帰納法で示す．$n = 0$ とすると，$f(x) = a$（$a \in R$，$a \neq 0$）であるので，任意の $c \in R$ に対して $f(c) = a \neq 0$ である．つまり．根は 0 個である．$n = 1$ のときは，1 次多項式 $f(x) = ax + b$（$a, b \in R$，$a \neq 0$）が 2 つの根 $c, c' \in R$ をもったとすると，$ac + b = 0 = ac' + b$ より $ac = ac'$ となるが，R は整域であるので，命題 6.21 より $c = c'$ を得る．よって，R における根は高々1 つである．

$n > 1$ とし，n 未満のときには主張が成り立つと仮定する．$a \in R$ を $f(x)$ の根とすれば，系 6.49（因数定理）より $f(x) = (x-a)f_1(x)$ となる $f_1(x) \in R[x]$ が存在する．命題 6.46 より $\deg(f_1) = n-1$ であるので，帰納法の仮定より R における $f_1(x)$ の相異なる根は高々 $n-1$ 個である．$b \in R$ を $b \neq a$ なる $f(x)$ の根とすると，$0 = f(b) = (b-a)f_1(b)$ であるが，R が整域であるので，命題 6.21 より $b \neq a$ から $f_1(b) = 0$ が従う．つまり，R における a と異なる $f(x)$ の根は $f_1(x)$ の高々 $n-1$ 個の根のいずれかと一致する．したがって，R における $f(x)$ の相異なる根は高々 n 個である．□

問 6.61　(1) まず $I \cap J \ni 0$ より，$I \cap J \neq \emptyset$ である．$a, b \in I \cap J$ とする．$a, b \in I$ かつ $a, b \in J$ であり，I も J も左イデアルであるので，$a+b \in I$ かつ $a+b \in J$ となる．よって，$a+b \in I \cap J$ である．また，$r \in R$ とすると，再び I と J は左イデアルであることより，$ra \in I$ かつ $ra \in J$ となる．よって，$ra \in I \cap J$ である．以上より，$I \cap J$ は R の左イデアルである．

次に I_0 を I にも J にも含まれる R の左イデアルとすると，$I_0 \subset I \cap J$ である．$I \cap J \subset I$ かつ $I \cap J \subset J$ であるから，$I \cap J$ は I にも J にも含まれる R の左イデアルのうち包含関係において最大のものである．

(2) $I \cup J$ を R の左イデアルと仮定すると，$a \in I$，$b \in J$ について，$a, b \in I \cup J$ より $a+b \in I \cup J$ となる．よって，$a+b \in I$ または $a+b \in J$ である．仮に $a+b \in I$ とすれば，$a+b = c$（$c \in I$）と書けるので，$b = c - a \in I$ を得る．つまり，$J \subset I$ が従う．また $a+b \in J$ とすれば，同様にして $I \subset J$ が従う．以上より，$I \cup J$ が R の左イデアルならば，$J \subset I$ または $I \subset J$ となる．この逆が成り立つことも直ちにわかるので，次が成り立つ．

$$I \cup J \text{ は } R \text{ の左イデアルである} \iff J \subset I \text{ または } I \subset J \text{ となる}$$

したがって，$J \subset I$ または $I \subset J$ を満たさない I と J の組を選べば，$I \cup J$ は R の左イデアルとはならない．たとえば，$\mathbb{Z}$ のイデアルとして $I = (10)$ と $J = (6)$ をとれば，$I \cup J$ は $\mathbb{Z}$ のイデアルではない（$10, 6 \in I \cup J$ であるが，$10 + 6 = 16 \notin I \cup J$ である）．

(3) $\bigcap_i I_i \ni 0$ より $\bigcap_i I_i \neq \emptyset$ である．$a, b \in \bigcap_i I_i$ とすると，任意の i について $a, b \in I_i$ であり，I_i は左イデアルであるから，各 i について $a+b \in I_i$ となる．よって，$a+b \in \bigcap_i I_i$ が成り立つ．また，$r \in R$ とすれば，再び I_i は R の左イデアルより，各 i について $ra \in I_i$ となる．よって，$ra \in \bigcap_i I_i$ が成り立つ．以上より．$\bigcap_i I_i$ は R の左イデアルである．　□

問 6.62　(1) $I + J \ni 0 + 0 = 0$ であるので，$I + J \neq \emptyset$ である．$c, d \in I + J$，$r \in R$ とする．このとき，$c = a + b$，$d = a' + b'$（$a, a' \in I$，$b, b' \in J$）と書けて，I と J が R の左イデアルなので，$a+a' \in I$，$b+b' \in J$，$ra \in I$，$rb \in J$ より，$c+d = (a+a')+(b+b') \in I+J$，$rc = ra+rb \in I+J$ となる．したがって，$I + J$ は R の左イデアルである．

次に I_0 を I と J を含む R の左イデアルとする．$a \in I$ と $b \in J$ について $a, b \in I_0$ であるので，$a + b \in I_0$ となる．よって，$I + J \subset I_0$ である．$I, J \subset I + J$ であるから，$I + J$ は包含関係において I と J を含む最小の R の左イデアルである．

(2) $IJ \ni 0 \cdot 0 = 0$ より $IJ \neq \emptyset$ である．$c, d \in IJ$，$r \in R$ とする．このとき，$c = \sum_i a_i b_i$，$d = \sum_i a'_i b'_i$ （$a_i, a'_i \in I$，$b_i, b'_i \in J$，c と d は有限和）と書けて，$c + d$ は I と J の元の積の有限和であるので，$c + d \in IJ$ となる．また，I が R の左イデアルより $ra_i \in I$ となるので，$rc = \sum_i (ra_i) b_i \in IJ$ である．したがって，IJ は R の左イデアルである．

次に I_0 を S を含む R の左イデアルとすると，I_0 は S の元の有限和も含むので，IJ の元はすべて I_0 に含まれる．よって，$IJ \subset I_0$ である．一方，$S \subset IJ$ であるから，IJ は S を含む R の左イデアルのうち包含関係において最小のものである．

(3) I と J が右イデアルであれば，IJ が右イデアルであることは (2) と同様に示すことができる．よって，このことと (2) より，I と J が両側イデアルであれば，IJ は R の両側イデアルである．

また，$\sum_i a_i b_i \in IJ$（$a_i \in I$，$b_i \in J$，和は有限和）とすると，I と J は（両側）イデアルであるので，a_i を R の元とみれば $a_i b_i \in J$ であり，b_i を R の元とみれば $a_i b_i \in I$ となる．よって，各 i について $a_i b_i \in I \cap J$ である．$I \cap J$ はイデアルであるので，$\sum_i a_i b_i \in I \cap J$ が従う．よって，$IJ \subset I \cap J$ を得る．

(4) n に関する数学的帰納法で示す．まず $n = 2$ のときを示す．(3) より $I_1 I_2 \subset I_1 \cap I_2$ であるので，この逆向きの包含関係を示す．仮定より $b_1 + b_2 = 1$ となる $b_i \in I_i$ が存在する．任意の $a \in I_1 \cap I_2$ について，$a = a \cdot 1 = ab_1 + ab_2$ と書ける．ここで，$a \in I_2$ とみれば，$b_1 \in I_1$ より $ab_1 \in I_2 I_1 = I_1 I_2$ である．また，$a \in I_1$ とみれば，$b_2 \in I_2$ より $ab_2 \in I_1 I_2$ である．よって，$a = ab_1 + ab_2 \in I_1 I_2$ を得る．したがって，$I_1 \cap I_2 \subset I_1 I_2$ である．以上より，$I_1 I_2 = I_1 \cap I_2$ が成り立つ．

次に $n-1$ まで成り立つとして n のときを示す．まず，相異なる i と j について $I_i + I_j = R$ であるので，後述の注意 6.101 より $I_1 \cap I_2 \cap \cdots \cap I_{n-1} + I_n = R$ が従う．よって，帰納法の仮定より $I_1 \cdots I_{n-1} + I_n = R$ が成り立つ．これより $n = 2$ の場合が適用できて，帰納法の仮定より $I_1 I_2 \cdots I_{n-1} I_n = (I_1 I_2 \cdots I_{n-1}) I_n = I_1 I_2 \cdots I_{n-1} \cap I_n = (I_1 \cap I_2 \cap \cdots \cap I_{n-1}) \cap I_n = I_1 \cap I_2 \cap \cdots \cap I_n$ が得られる．したがって，n のときにも主張が成り立つ． □

問 6.63　まず左イデアルについての主張を示す．$a \in R$ とする．$Ra \ni 1 \cdot a = a$ であるので，$Ra \neq \emptyset$ である．$b, c \in Ra$，$r \in R$ とする．$b = pa$, $c = qa$（$p, q \in R$）と書けて，$p + q \in R$ より $b + c = (p + q)a \in Ra$ である．また，$rp \in R$ より $rb = (rp)a \in Ra$ である．よって，Ra は R の左イデアルである．$a_i \in R$ について Ra_i は a_i を含む R の左イデアルであるので，問 6.62 より $Ra_1 + Ra_2$ は R の左イデアルであり，$a_1 = a_1 + 0, a_2 = 0 + a_2 \in Ra_1 + Ra_2$ をみたす．これよりさらに問 6.62 を用いれば，$Ra_1 + Ra_2 + Ra_3 = (Ra_1 + Ra_2) + Ra_3$ も R の左イデアルであり，$a_1, a_2, a_3 \in Ra_1 + Ra_2 + Ra_3$ をみたす．よって，これを繰り返せば，$Ra_1 + \cdots + Ra_n$ は $M = \{ a_1, \ldots, a_n \}$ を含む R の左イデアルである．一方，I_l は M を含む左イデアルであるので，各 i について $I_l \supset Ra_i$ であり，よって，$I_l \supset Ra_1 + \cdots + Ra_n$ となる．ところで，I_l は M を含む最小の左イデアルであり，$Ra_1 + \cdots + Ra_n$ も M を含む左イデアルであるので，最小性より $I_l = Ra_1 + \cdots + Ra_n$ となる．

I_r と I についての主張も同様に示すことができる． □

問 6.67　$(a) = a\mathbb{Z}$，$(b) = b\mathbb{Z}$ であるので，定理 3.16 より，$I + J = a\mathbb{Z} + b\mathbb{Z} = g\mathbb{Z} = (g)$，および，$I \cap J = a\mathbb{Z} \cap b\mathbb{Z} = l\mathbb{Z} = (l)$ を得る．

あとは $IJ = (ab)$ を示せばよい．まず $IJ \ni ab$ より $IJ \supset (ab)$ が成り立つ．一方，$\sum_i a_i b_i \in IJ$（$a_i \in I$，$b_i \in J$，和は有限和）とすると，a_i は a の倍数，b_i は b の倍数であるので，$ab \mid a_i b_i$ であり，$ab \mid \sum_i a_i b_i$ となる．よって，$IJ \subset (ab)$ が成り立つ．したがって，$IJ = (ab)$ を得る． □

問 6.68　仮に $(x, 2)$ が単項イデアルとすると，ある $f(x) \in \mathbb{Z}[x]$ があって $(f(x)) = (x, 2)$ となる．よって，$x = f(x)g(x)$ かつ $2 = f(x)h(x)$（$g(x), h(x) \in \mathbb{Z}[x]$）と書ける．命題 6.46 より，$2 = f(x)h(x)$ であることから $f(x)$ は 0 でない定数（整数）であり，よって，$f(x) = \pm 1$ または

$f(x) = \pm 2$ のいずれかである．$f(x) = \pm 2$ とすれば，$x = \pm 2g(x)$ となるが，左辺はモニックであり，右辺はすべての係数が 2 の倍数であるので，これは矛盾となる．したがって，$f(x) = \pm 1$ でなければならない．しかし，$f(x) = \pm 1$ とすると，$\pm 1 \in (x, 2)$ より $\pm 1 = xp(x) + 2q(x)$（$p(x), q(x) \in \mathbb{Z}[x]$）と書けて，これに $x = 0$ を代入すると $\pm 1 = 2p(0)$ という $\mathbb{Z}$ での等式が従い，これも矛盾である．以上より，$(x, 2)$ は単項イデアルではない． □

問 6.69 $c \in I + J$ とすると，$c = a + b$（$a \in I$，$b \in J$）であり，$a = r_1 a_1 + r_2 a_2$，$b = r_3 b_1 + r_4 b_2$（$r_i \in R$）と書けるので，$c = r_1 a_1 + r_2 a_2 + r_3 b_1 + r_4 b_2 \in (a_1, b_1, a_2, b_2)$ となる．よって，$I + J \subset (a_1, b_1, a_2, b_2)$ である．一方，$I \ni 0, a_1, a_2$ かつ $J \ni 0, b_1, b_2$ であるので，$I + J \ni a_1, a_2, b_1, b_2$ となる．$I + J$ はイデアルであるので，これより $I + J \supset (a_1, b_1, a_2, b_2)$ である．以上より，$I + J = (a_1, b_1, a_2, b_2)$ が従う．

$IJ = (a_1 b_1, a_1 b_2, a_2 b_1, a_2 b_2)$ についても同様に示すことができる． □

問 6.81 まず例 6.80 より，剰余環 $\mathbb{Z}/m\mathbb{Z}$ の完全代表系として $\{\, a \mid 0 \leq a \leq m - 1 \,\}$ がとれる．$\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ となることは，$\overline{a}\overline{b} = \overline{1}$ となる $b \in \mathbb{Z}$ が存在することである．$\overline{a}\overline{b} = \overline{1}$ は $ab \equiv 1 \pmod{m}$ をみたすことであるので，$\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ となることは，$ab + mc = 1$ となる $b, c \in \mathbb{Z}$ が存在することと同値であり，定理 3.21 より後者の条件は $\gcd(a, m) = 1$ となることと同値である．よって，$\mathbb{Z}/m\mathbb{Z}$ の単元群は $1 \leq a \leq m - 1$ となる自然数のうち $\gcd(a, m) = 1$ をみたす a の代表する剰余類 $\overline{a}$ で構成される．（なお，a が m と互いに素ならば，$\overline{a}$ に含まれる元 a' は $a \equiv a' \pmod{m}$ をみたすので，$\overline{a}$ はどの代表元をとっても m と互いに素である．） □

問 6.91 (1) $0 \in I$ より $f(0) = 0 \in f(I)$ であるので $f(I) \neq \emptyset$ である．$a' = f(a), b' = f(b) \in f(I)$（$a, b \in I$），$r' = f(r) \in \mathrm{Im}(f)$（$r \in R$）とすると，$f$ の準同型性と I が左イデアルであることより，$a' + b' = f(a) + f(b) = f(a + b) \in f(I)$，および，$r'a' = f(r)f(a) = f(ra) \in f(I)$ が成り立つ．よって，$f(I)$ は $\mathrm{Im}(f)$ の左イデアルである．

I が右イデアルや両側イデアルの場合も同様に示せる．

(2) $0 \in I'$ より $f^{-1}(I') \supset f^{-1}(0) \ni 0$ であるので $f^{-1}(I') \neq \emptyset$ である．$a, b \in f^{-1}(I')$，$r \in R$ とする．$a' = f(a), b' = f(b) \in I'$ とおけば，f の準同型性と I' が左イデアルであることより，$f(a + b) = f(a) + f(b) \in I'$，および，$f(ra) = f(r)f(a) \in I'$ となる．よって，$a + b \in f^{-1}(I')$，および，$ra \in f^{-1}(I')$ が成り立つ．したがって，$f^{-1}(I')$ は R の左イデアルである．

I' が右イデアルや両側イデアルの場合も同様に示せる． □

問 6.94 まず，f の準同型性と $I = \mathrm{Ker}(f)$ であることより

$$a + I = b + I \Longleftrightarrow a - b \in I \Longleftrightarrow f(a - b) = 0' \Longleftrightarrow f(a) = f(b)$$

が成り立つ．ここで，$0'$ は R' の零元である．よって，この右向きの矢印より写像 $\overline{f}$ は代表元のとり方に依らず定義されることがわかり，この左向きの矢印と $\overline{f}(\overline{a}) = f(a)$ より $\overline{f}$ が単射であること

が従う．また，$\overline{a}, \overline{b} \in R/I$ について，$\overline{f}(\overline{a}+\overline{b}) = \overline{f}(\overline{a+b}) = f(a+b) = f(a)+f(b) = \overline{f}(\overline{a})+\overline{f}(\overline{b})$，$\overline{f}(\overline{a}\overline{b}) = \overline{f}(\overline{ab}) = f(ab) = f(a)f(b) = \overline{f}(\overline{a})\overline{f}(\overline{b})$，および，$\overline{f}(\overline{1_R}) = f(1_R) = 1_{R'}$ となるので，$\overline{f}$ は環準同型写像であり，よって，環の単準同型写像である．さらに，$\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$ であるので，最後の環同型も従う． □

問 6.106 $(a_1, \ldots, a_r) \in R_1^\times \times \cdots \times R_r^\times$ とする．各 i について $a_i \in R_i^\times$ より $a_i b_i = e_{R_i}$ となる $b_i \in R_i$ が存在する．このとき，$(a_1, \ldots, a_r)(b_1, \ldots, b_r) = (e_{R_1}, \ldots, e_{R_r})$ であるので，$(a_1, \ldots, a_r) \in (R_1 \times \cdots \times R_r)^\times$ が従う．つまり，$R_1^\times \times \cdots \times R_r^\times \subset (R_1 \times \cdots \times R_r)^\times$ である．そこで，$(a_1, \ldots, a_r) \in R_1^\times \times \cdots \times R_r^\times$ に $(a_1, \ldots, a_r)$ 自身を対応させることにより，$R_1^\times \times \cdots \times R_r^\times$ から $(R_1 \times \cdots \times R_r)^\times$ への写像 f を定める．このとき，f の定め方（f は包含写像である）より f は群の単準同型である．また，任意の $(a_1, \ldots, a_r) \in (R_1 \times \cdots \times R_r)^\times$ に対して，$(a_1, \ldots, a_r)(b_1, \ldots, b_r) = (e_{R_1}, \ldots, e_{R_r})$ となる $(b_1, \ldots, b_r) \in (R_1 \times \cdots \times R_r)^\times$ が存在する．とくに $a_i b_i = e_{R_i}$ であるので，各 i について $a_i \in R_i^\times$ が従う．よって，$(a_1, \ldots, a_r) \in R_1^\times \times \cdots \times R_r^\times$ となるので，f は全射である．したがって，f は群同型であり，$(R_1 \times \cdots \times R_r)^\times \simeq R_1^\times \times \cdots \times R_r^\times$ が従う． □

問 6.109 (1) $\varphi(10!) = \varphi(2^8 \cdot 3^4 \cdot 5^2 \cdot 7) = \varphi(2^8)\varphi(3^4)\varphi(5^2)\varphi(7) = 2^7 \cdot (3^3 \cdot 2) \cdot (5 \cdot 4) \cdot 6 = 2^{11} \cdot 3^4 \cdot 5 = 829,440$.

(2) まず，オイラー関数の値は $\varphi(1) = \varphi(2) = 1$ 以外は偶数になることに注意する．実際，n が奇素数 p を素因子にもてば，命題 6.108 より $(p-1) \mid \varphi(n)$ となるので $\varphi(n)$ は偶数である．また，n が 2 以外の偶数べキ 2^e（$e \geq 2$）であれば，再び命題 6.108 より $\varphi(n) = 2^{e-1} \geq 2$ となるので $\varphi(n)$ は偶数である．

$\varphi(n) = 18$ となる自然数 n を求めるためには，命題 6.108 より，18 の約数による分解を考えればよい（このとき，$\varphi(2) = 1$ であるので約数として 1 も対象に考える）．$18 = 1 \cdot 2 \cdot 3^2$ であるので，$1, 2, 3$ の組み合わせで 18 の分解を作ればよいが，オイラー関数は 1 以外の奇数にはならないので，考える分解は $18 = 18$ と $18 = 1 \cdot 18$ の 2 つだけである．よって，p を奇素数とするとき，$n = p^e$ または $n = 2p^e$（e は自然数）のいずれかである．まず $n = p^e$ の場合，$\varphi(p^e) = p^{e-1}(p-1)$ であるので，$e = 1$ ならば $n = 19$ であり，$e \geq 2$ ならば $n = 3^3$ であることがわかる．$n = 2p^e$ の場合はこれに 2 をかけた値であるので，$n = 2 \cdot 19$ と $n = 2 \cdot 3^3$ が得れれる．したがって，$\varphi(n) = 18$ となる自然数 n は $n = 19, 27, 38, 54$ の 4 つである． □

問 6.112 $37^{37^{37}}$ の法 17 での値を求めればよい．まず，17 は素数であるので，フェルマーの小定理（系 6.111）より，法 17 における肩の指数部分は法 $\varphi(17) = 16$ で考えれば十分である．フェルマー-オイラーの定理（定理 6.110）を用いれば，肩の指数部分は，$\varphi(16) = 8$ より

$$37^{37} \equiv 5^{4 \cdot 8 + 5} \equiv 5^5 \equiv 25^2 \cdot 5 \equiv 9^2 \cdot 5 \equiv 5 \pmod{16}$$

となる．よって，

$$37^{37^{37}} \equiv 3^5 \equiv 27 \cdot 9 \equiv 10 \cdot 9 \equiv 5 \pmod{17}$$

が得られる．したがって，$37^{37^{37}}$ を 17 で割った余りは 5 である． □

問 6.142　$\alpha = a + b\sqrt{5}i, \beta = c + d\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ （$a, b, c, d \in \mathbb{Z}$）について $11 \mid \alpha\beta$ であるとする．複素共役をとれば $11 \mid \overline{\alpha}\overline{\beta}$ である．よって，複素共役との積をとれば，$\mathbb{Z}$ において $11 \mid (a^2 + 5b^2)(c^2 + 5d^2)$ が得られる．11 は素数（$\mathbb{Z}$ の素元）なので，これより $11 \mid (a^2 + 5b^2)$ または $11 \mid (c^2 + 5d^2)$ である．そこで，仮に $11 \mid (a^2 + 5b^2)$ とする．このとき，a, b の可能な組み合わせを法 11 で探すと，次の表の結果を得る．ここで，縦は法 11 での a の値，横は法 11 での b の値であり，縦と横に対応する部分は法 11 での $a^2 + 5b^2$ の値である．

$a\backslash b$	0	1, 10	2, 9	3, 8	4, 7	5, 6
0	0	5	9	1	3	4
1, 10	1	6	10	2	4	5
2, 9	4	9	2	5	7	8
3, 8	9	3	7	10	1	2
4, 7	5	10	3	6	8	9
5, 6	3	8	1	4	6	7

これより，$11 \mid (a^2 + 5b^2)$ となるのは $a \equiv b \equiv 0 \pmod{11}$ だけである．したがって，$\mathbb{Z}[\sqrt{5}i]$ において $11 \mid \alpha$ が得られる．仮に $11 \mid (c^2 + db^2)$ とすれば同様にして $11 \mid \beta$ が得られるので，11 は $\mathbb{Z}[\sqrt{5}i]$ の素元である．　□

第 6 章　演習問題

演習 1　$\mathbb{Z}[\sqrt{2}]$ は実数体 $\mathbb{R}$ の部分集合である．$\alpha = a + b\sqrt{2}, \beta = c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ （$a, b, c, d \in \mathbb{Z}$）とすると，$\alpha - \beta = (a - c) + (b - d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$，かつ，$\alpha\beta = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ であり，また $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ であるので，定理 6.39（部分環の判定定理）より $\mathbb{Z}[\sqrt{2}]$ は実数体 $\mathbb{R}$ の部分環である．したがって，命題 6.42 より $\mathbb{Z}[\sqrt{2}]$ は整域である．　□

演習 2　$\mathbb{Q}[\sqrt{3}]$ は実数体 $\mathbb{R}$ の部分集合であり，本章末演習問題の演習 1 と同様にして定理 6.39 と命題 6.42 より $\mathbb{Q}[\sqrt{3}]$ は整域であることがわかる．また，$\alpha = a + b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$（$a, b \in \mathbb{Q}$）について，$\alpha \neq 0$ ならば，$\frac{1}{\alpha} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$ が α の逆元となるので，$\alpha \neq 0$ は可逆である．したがって，$\mathbb{Q}[\sqrt{3}]$ は体である．（なお，$\mathbb{Q}[\sqrt{3}]$ は $\mathbb{Z}[\sqrt{3}]$ の商体であり，通常 $\mathbb{Q}(\sqrt{3})$ と表される．）　□

演習 3　(1) 2 次の行列の計算を行えば直ちに確かめられる．

(2) $X = aE + bI + cJ + dK, \overline{X} = aE - bI - cJ - dK \in \mathbb{H}$ について，(1) の関係を利用すれば，$X\overline{X} = (aE + bI + cJ + dK)(aE - bI - cJ - dK) = a^2E - abI - acJ - adK + abI + b^2E - bcK + bdJ + acJ + bcK + c^2E - cdI + adK - bdJ + cdI + d^2E = a^2E + b^2E + c^2E + d^2E = (a^2 + b^2 + c^2 + d^2)E$ となる．$\overline{X}X = (a^2 + b^2 + c^2 + d^2)E$ も同様にして確かめられる．

(3) $X = aE + bI + cJ + dK = \begin{pmatrix} a+bi & c+di \\ -c+di & a+bi \end{pmatrix} \in M(2,\mathbb{C})$（ここで，複素数 α に対して $\overline{\alpha}$ は α の複素共役である）より

$$\mathbb{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \,\middle|\, \alpha, \beta \in \mathbb{C} \right\}$$

となる．とくに，$\mathbb{H}$ は複素数成分の 2 次正方行列の全体のなす環 $M(2,;\mathbb{C})$ の部分集合である．ここで，$X = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}, Y = \begin{pmatrix} \alpha' & \beta' \\ -\overline{\beta'} & \overline{\alpha'} \end{pmatrix} \in \mathbb{H}$ について，

$$X - Y = \begin{pmatrix} \alpha - \alpha' & \beta - \beta' \\ -\overline{\beta - \beta'} & \overline{\alpha - \alpha'} \end{pmatrix}, \quad XY = \begin{pmatrix} \alpha\alpha' - \beta\overline{\beta'} & \alpha\beta' + \overline{\alpha'}\beta \\ -\alpha\beta' + \overline{\alpha'}\beta & \alpha\alpha' - \beta\overline{\beta'} \end{pmatrix}$$

より $X - Y, XY \in \mathbb{H}$ が成り立ち，$E \in \mathbb{H}$ であるので，定理 6.39 より $\mathbb{H}$ は $M(2,\mathbb{C})$ の部分環である．さらに，$X = aE + bI + cJ + dK \in \mathbb{H}$ について，$X \neq 0$ であれば，$a^2 + b^2 + c^2 + d^2 \neq 0$ であるので，(2) より $X\frac{1}{a^2+b^2+c^2+d^2}\overline{X} = \frac{1}{a^2+b^2+c^2+d^2}\overline{X}X = E$ が従う．よって，$\frac{1}{a^2+b^2+c^2+d^2}\overline{X}$ は X の逆元であり，$X \neq 0$ は可逆元となる．したがって，$\mathbb{H}$ は斜体である．とくに，(1) より，たとえば $IJ = -JI \neq JI$ であるので，$\mathbb{H}$ は非可換である． □

演習 4　p を素数とし，p 個の元からなる可換環を R，$a \in R$ を 0 でない元とする．a の生成する単項イデアル (a) は R を加法群とみたとき R の部分群である．よって，ラグランジュの定理（定理 4.69）より (a) の位数は 1 または p である．いま $a \neq 0$ かつ $(a) \ni 0, a$ なので，(a) の位数は p である．よって，$(a) = R$ であり，とくに $1 \in (a)$ であるので，$ra = 1$ となる $r \in R$ が存在する．したがって，a は R の可逆元である．以上より，R は体である． □

演習 5　剰余環 $\mathbb{Z}/7\mathbb{Z}$ における和と積を計算すれば次の演算表が得られる．

$\mathbb{Z}/7\mathbb{Z}$ での和

和	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

$\mathbb{Z}/7\mathbb{Z}$ での積

積	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

同様にして，剰余環 $\mathbb{Z}/8\mathbb{Z}$ における和と積の演算表は，

$\mathbb{Z}/8\mathbb{Z}$ での和

和	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$

$\mathbb{Z}/8\mathbb{Z}$ での積

積	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

となり，剰余環 $\mathbb{Z}/12\mathbb{Z}$ における和と積の演算表は，

$\mathbb{Z}/12\mathbb{Z}$ での和

和	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{8}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{9}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{10}$	$\overline{10}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{11}$	$\overline{11}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$

$\mathbb{Z}/12\mathbb{Z}$ での積

積	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{3}$	$\overline{8}$	$\overline{1}$	$\overline{6}$	$\overline{11}$	$\overline{4}$	$\overline{9}$	$\overline{2}$	$\overline{7}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{2}$	$\overline{9}$	$\overline{4}$	$\overline{11}$	$\overline{6}$	$\overline{1}$	$\overline{8}$	$\overline{3}$	$\overline{10}$	$\overline{5}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{10}$	$\overline{0}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{11}$	$\overline{0}$	$\overline{11}$	$\overline{10}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

となる．□

演習 6　問 6.81 より $\mathbb{Z}/60\mathbb{Z}$ の可逆元は 60 と互いに素な代表元をもつ剰余類であるので，$\overline{1}$, $\overline{7}$, $\overline{11}$, $\overline{13}$, $\overline{17}$, $\overline{19}$, $\overline{23}$, $\overline{29}$, $\overline{31}$, $\overline{37}$, $\overline{41}$, $\overline{43}$, $\overline{47}$, $\overline{49}$, $\overline{53}$, $\overline{59}$ の $\varphi(60) = 16$ 個が可逆元である．つまり，単元群は

$$(\mathbb{Z}/60\mathbb{Z})^\times = \{\,\overline{1}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}, \overline{31}, \overline{37}, \overline{41}, \overline{43}, \overline{47}, \overline{49}, \overline{53}, \overline{59}\,\}$$

となる．

命題 6.30 より可逆元は零因子ではない．一方，60 と互いに素でない代表元をもつ剰余類 $\overline{a}$ はすべて零因子となる．実際，$a \in \mathbb{Z}$，$0 \leq a < 60$ について $\gcd(a, 60) = b \neq 1$ とすると，$bc = 60$ となる $c \in \mathbb{Z}$（$0 < c < 60$）が存在して，$\overline{c} \neq \overline{0}$ かつ $\overline{a}\,\overline{c} = \overline{0}$ となるので，$\overline{a}$ は零因子となる．したがって，可逆元でない元はすべて零因子である．具体的に書けば，$\overline{0}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{8}$, $\overline{9}$, $\overline{10}$, $\overline{12}$, $\overline{14}$, $\overline{15}$, $\overline{16}$, $\overline{18}$, $\overline{20}$, $\overline{21}$, $\overline{22}$, $\overline{24}$, $\overline{25}$, $\overline{26}$, $\overline{27}$, $\overline{28}$, $\overline{30}$, $\overline{32}$, $\overline{33}$, $\overline{34}$, $\overline{35}$, $\overline{36}$, $\overline{38}$, $\overline{39}$, $\overline{40}$, $\overline{42}$, $\overline{44}$, $\overline{45}$, $\overline{46}$, $\overline{48}$, $\overline{50}$, $\overline{51}$, $\overline{52}$, $\overline{54}$, $\overline{55}$, $\overline{56}$, $\overline{57}$, $\overline{58}$ の $60 - \varphi(60) = 44$ 個が零因子である．□

演習 7　命題 6.114 より，剰余環 $\mathbb{Z}/60\mathbb{Z}$ のイデアルは (60) を含む $\mathbb{Z}$ のイデアルと一対一に対応する．よって，命題 6.70 より 60 の約数の生成する $\mathbb{Z}$ の単項イデアルに対応する $\mathbb{Z}/60\mathbb{Z}$ のイデアルを求めればよい．したがって，剰余環 $\mathbb{Z}/60\mathbb{Z}$ のイデアルは，$(\overline{0})$, $(\overline{1})$, $(\overline{2})$, $(\overline{3})$, $(\overline{4})$, $(\overline{5})$, $(\overline{6})$, $(\overline{10})$, $(\overline{12})$, $(\overline{15})$, $(\overline{20})$, $(\overline{30})$ の 12 個である．

次に，イデアルの包含関係を調べる．まず，$(1) = \mathbb{Z}/60\mathbb{Z}$ より (1) は極大イデアルではない．次に，$(\overline{2})$, $(\overline{3})$, $(\overline{5})$ は素数が生成する単項イデアルであるので，これらを真に含むイデアルは $(1) = \mathbb{Z}/60\mathbb{Z}$ だけである．よって，この 3 つは極大イデアルである．その他のイデアルについては，$(\overline{1}) \supset (\overline{2}) \supset (\overline{0})$，$(\overline{1}) \supset (\overline{2}) \supset (\overline{4})$，$(\overline{1}) \supset (\overline{2}) \supset (\overline{6})$，$(\overline{1}) \supset (\overline{2}) \supset (\overline{10})$，$(\overline{1}) \supset (\overline{2}) \supset (\overline{12})$，$(\overline{1}) \supset (\overline{3}) \supset (\overline{15})$，$(\overline{1}) \supset (\overline{2}) \supset (\overline{20})$，$(\overline{1}) \supset (\overline{2}) \supset (\overline{30})$ であるので，極大イデアルではない．したがって，極大イデアルは $(\overline{2})$, $(\overline{3})$, $(\overline{5})$ の 3 個である．

最後に，$\mathbb{Z}/60\mathbb{Z}$ の素イデアルを求める．まず $\mathbb{Z}/60\mathbb{Z}$ は整域ではないので，系 6.117 より (0) は素イデアルではない．また，系 6.116 より極大イデアルである $(\overline{2})$, $(\overline{3})$, $(\overline{5})$ は素イデアルである．この他に素イデアルがないことを確認する．$a \neq 0$ とし，(a) を $\mathbb{Z}/60\mathbb{Z}$ のイデアルとする．a は 60 の正の約数ととれるので，$\gcd(a, 60) = a$ である．よって，命題 5.11 より $(\mathbb{Z}/m\mathbb{Z})/(a) = (\mathbb{Z}/m\mathbb{Z})/a(\mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/a\mathbb{Z}$ となる．したがって，命題 6.34 と定理 6.115 より，(a) が素イデアルであることと a が素数であることが同値となるので，$a = 2, 3, 5$ のいずれかである．以上より，素イデアルは $(\overline{2})$, $(\overline{3})$, $(\overline{5})$ の 3 個である． □

演習 8　$\mathbb{Z}$ 上の多項式環 $\mathbb{Z}[x]$ から $\mathbb{Z}[\sqrt{2}]$ への写像 φ を

$$\varphi : \mathbb{Z}[x] \ni f(x) \longmapsto f(\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$$

と定める．このとき，$\varphi(f+g) = f(\sqrt{2})+g(\sqrt{2}) = \varphi(f)+\varphi(g)$，$\varphi(fg) = f(\sqrt{2})g(\sqrt{2}) = \varphi(f)\varphi(g)$，かつ，$\varphi(1) = 1$ となるので，φ は環準同型である．また，任意の $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ $(a, b \in \mathbb{Z})$ について，$f(x) = a + bx \in \mathbb{Z}[x]$ をとれば $\varphi(f) = a + b\sqrt{2}$ より，φ は環の全準同型である．さらに，$\mathrm{Ker}(\varphi)$ は多項式 $x^2 - 2$ の生成する単項イデアル $(x^2 - 2)$ である．実際，$x^2 - 2$ において $x = \sqrt{2}$ を代入すると 0 を得るので，$x^2 - 2 \in \mathrm{Ker}(\varphi)$ であり，よって $(x^2 - 2) \subset \mathrm{Ker}(\varphi)$ である．一方，$f(x) \in \mathrm{Ker}(\varphi)$ とすると，定理 6.48 より $f(x) = (x^2 - 2)h(x) + r(x)$, $\deg(r) \leq 1$ となる $h(x), r(x) \in \mathbb{Z}[x]$ が存在する．このとき，$r(\sqrt{2}) = f(\sqrt{2}) - (\sqrt{2}^2 - 2)h(\sqrt{2}) = 0$ となるが，$\deg(r) \leq 1$ かつ $\sqrt{2} \notin \mathbb{Z}$ より $r(x) = 0$ であるので．$f(x) = (x^2 - 2)h(x)$ となる．よって，$f(x) \in (x^2 - 2)$ であり，$\mathrm{Ker}(\varphi) \subset (x^2 - 2)$ を得る．したがって，$\mathrm{Ker}(\varphi) = (x^2 - 2)$ である．以上より，環準同型定理を適用すれば，環同型 $\mathbb{Z}[x]/(x^2 - 2) \simeq \mathbb{Z}[\sqrt{2}]$ が得られる． □

演習 9　仮に環同型であったとし，$\mathbb{Z}[\sqrt{2}]$ から $\mathbb{Z}[\sqrt{3}]$ への環同型写像を f とする．f は全射であるので，$f(a+b\sqrt{2}) = \sqrt{3}$ となる $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$（$a, b, \in \mathbb{Z}$）が存在する．このとき，$f$ は準同型より $f((a+b\sqrt{2})^2) = f(a+b\sqrt{2})^2 = 3$ となる．一方，f は準同型より $f(1) = 1$ であり，$f(3) = 3$ が従う．よって，$f(3) = 3 = f((a+b\sqrt{2})^2)$ が得られる．したがって，f の単射性より $3 = (a+b\sqrt{2})^2$ である．つまり，$3 = a^2 + 2b^2 + 2ab\sqrt{2}$ となる．しかし，この等式をみたす $a, b \in \mathbb{Z}$ は存在しないので，これは矛盾である．したがって，$\mathbb{Z}[\sqrt{2}]$ と $\mathbb{Z}[\sqrt{3}]$ は環同型ではない． □

演習 10　(1) $T + I \ni 0 + 0 = 0$ より $T + I \neq \emptyset$ である．$\alpha = t + a, \beta = s + b \in T + I$（$t, s \in T$, $a, b \in I$）について，T も I も減法で閉じているので $\alpha - \beta = (t - s) + (a - b) \in T + I$ であり，また，T は積で閉じていて，I は（両側）イデアルであることより，$\alpha\beta = ts + (tb + as + ab) \in T + I$ である．さらに，$T + I \ni 1 + 0 = 1$ である．したがって，定理 6.39（部分環の判定定理）より $T + I$ は R の部分環である．

次に，I が $T + I$ のイデアルであることは，I が R のイデアルであり，かつ，$T + I$ は R の部分環で $I \subset T + I$ であることから直ちに従う．

最後に $T \cap I$ についての主張を示す．まず，$T \cap I \ni 0$ より $T \cap I \neq \emptyset$ である．$a, b \in T \cap I$ について，$a, b \in T$ かつ $a, b \in I$ より $a + b \in T$ かつ $a + b \in I$ となるので，$a + b \in T \cap I$ が従う．ま

た，$t \in T$ とすると，T は積で閉じていて（$ta, at \in T$）かつ I は R のイデアル（$ta, at \in I$）より $ta, at \in T \cap I$ が従う．よって，$T \cap I$ は T のイデアルである．

(2) T から剰余環 $(T+I)/I$ への写像 f を

$$f \ : \ T \ni t \longmapsto t + I \in (T+I)/I$$

と定めると，$t, s \in T$ について $f(t+s) = (t+s)+I = (t+I)+(s+I) = f(t)+f(s)$，$f(ts) = (ts)+I = (t+I)(s+I) = f(t)f(s)$，かつ，$f(1_R) = 1_R + I = 1_{(T+I)/I}$ より，f は環準同型である．任意の $(t+a)+I \in (T+I)/I$（$t \in T$，$a \in I$）について，$(t+a)+I = t+I$ であるので $f(t) = (t+a)+I$ となる．よって，f は環の全準同型である．さらに，

$$\mathrm{Ker}(f) = \{\, t \in T \mid t + I = I \,\} = \{\, t \in T \mid t \in I \,\} = T \cap I$$

となる（このことからも命題 6.90 より $T \cap I$ は T のイデアルであることがわかる）．したがって，環準同型定理より $T/(T \cap I) \simeq (T+I)/I$ が得られる． □

演習 11　剰余環 R/I から剰余環 R/J への写像 f を

$$f \ : \ R/I \ni a + I \longmapsto a + J \in R/J$$

と定めると，$a+I = b+I \Leftrightarrow a-b \in I$ であることと $I \subset J$ より，f は R/I の代表元のとり方に依らず定義できる．このとき，作り方より f は環の全準同型であることは直ちにわかる（本章章末問題の演習 10 の (2) の f の全準同型性と同様）．また，$a+I \in \mathrm{Ker}(f) \Leftrightarrow a \in J$ より，$\mathrm{Ker}(f) = J/I$ である．したがって，環準同型定理より $(R/I)/(J/I) \simeq R/J$ が得られる． □

演習 12　$K[x,y]$ のイデアル (x,y) について，$1 \notin (x,y)$ より $(x,y) \subsetneq K[x,y]$ であり，$y \notin (x)$ より $(x) \subsetneq (x,y)$ であるので，$(x) \subsetneq (x,y) \subsetneq K[x,y]$ を得る．よって，(x) は極大イデアルではない．

また，$K[x,y]$ から $K[y]$ への写像 φ を

$$\varphi \ : \ K[x,y] \ni f(x,y) \longmapsto f(0,y) \in K[y]$$

により定めると，これは作り方より環の全準同型写像となるが直ちにわかる（本章章末演習問題の演習 8 の φ の全準同型性と同様）．また，任意の $f(x,y) \in K[x,y]$ は $f(x,y) = f_1(y) + xf_2(x,y)$（$f_1(y) \in K[y]$，$f_2(x,y) \in K[x,y]$）と一意的に表せるので，

$$\mathrm{Ker}(f) = \{\, f(x,y) \in K[x,y] \mid f(0,y) = 0 \,\} = (x)$$

である．したがって，環準同型定理より $K[x,y]/(x) \simeq K[y]$ が得られる．K が体であるから命題 6.47 より $K[y]$ は整域である．よって，定理 6.115 より (x) は素イデアルである．（なお，環準同型写像

$$K[x,y] \ni f(x,y) \longmapsto f(0,0) \in K$$

から環同型 $K[x,y]/(x,y) \simeq K$ が得られるので，ここで登場したイデアル (x,y) は $K[x,y]$ の極大イデアルであることがわかる．） □

演習 13 (1) 仮に $P_1 = (2, 1+\sqrt{5}i)$ が単項イデアルであるとすると，$P_1 = (a+b\sqrt{5}i)$ となる $a+b\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ （$a, b \in \mathbb{Z}$）がとれる．よって，$2 = (a+b\sqrt{5}i)(s+t\sqrt{5}i)$，$1+\sqrt{5}i = (a+b\sqrt{5}i)(u+v\sqrt{5}i)$ となる $s+t\sqrt{5}i, u+v\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$（$s, t, u, v \in \mathbb{Z}$）が存在する．この両辺の複素共役をとり，もとの式とかけ合せれば，$\mathbb{Z}$ における 2 つの等式 $4 = (a^2+5b^2)(s^2+5t^2)$，$6 = (a^2+5b^2)(u^2+5v^2)$ を得る．よって，a^2+5b^2 は 4 と 6 の正の公約数であるので，$a^2+5b^2 = 1$ または $a^2+5b^2 = 2$ である．しかし，$a^2+5b^2 = 2$ をみたす $a, b \in \mathbb{Z}$ は存在しない．したがって，$a^2+5b^2 = 1$ であり，$a = \pm 1$ かつ $b = 0$ が従う．よって，$P_1 = (1)$ を得る．ところが，本問の (3) より $P_1^2 = (2)$ であるので，$P_1 \neq (1)$ であり，これは矛盾である．したがって，P_1 は単項イデアルでない．(後に出てくる本問の (3) を利用したが，初等的にも確かめられる．実際，$P_1 = (1)$ と仮定すれば，$1 = 2(s+t\sqrt{5}i)+(1+\sqrt{5}i)(u+v\sqrt{5}i)$ と書ける．よって，$1 = (2s+u-5v)+(2t+u+v)\sqrt{5}i$ となるので，$1 = 2s+u-5v$ かつ $0 = 2t+u+v$ を得る．したがって，両辺の差をとれば $1 = 2(s-t-3v)$ であるが，これをみたす $s, t, v \in \mathbb{Z}$ は存在しない．以上より，$P_1 \neq (1)$ である．)

P_2, Q_1, Q_2 についても同様に示すことができる．

(2) まず $P_1 = (2, 1+\sqrt{5}i)$ が極大イデアルであることを示す．$\mathbb{Z}$ から $\mathbb{Z}[\sqrt{5}i]/P_1$ への写像 f を

$$f \ : \ \mathbb{Z} \ni n \longmapsto n + P_1 \in \mathbb{Z}[\sqrt{5}i]/P_1$$

により定める．これは作り方より環準同型であることが直ちにわかる（本章章末問題の演習 10 の (2) の f の環準同型性と同様）．$a+b\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ とすると，$a+b\sqrt{5}i = (a-b)+b(1+\sqrt{5}i)$ と書けるので，$1+\sqrt{5}i \in P_1$ より $(a+b\sqrt{5}i)+P_1 = (a-b)+P_1$ となる．よって，$f(a-b) = (a+b\sqrt{5}i)+P_1$ が成り立つ．したがって，f は環の全準同型である．さらに，$\mathrm{Ker}(f) = (2)$ となる．実際，$n \in \mathrm{Ker}(f)$ とすると，$f(n) = n+P_1 = P_1$ より $n \in P_1$ となる．よって，ある $s, t, u, v \in \mathbb{Z}$ が存在して，$n = 2(s+t\sqrt{5}i)+(1+\sqrt{5}i)(u+v\sqrt{5}i)$ と書ける．右辺を展開して両辺を比べると，$n = 2(s-t-3v)$ が得られる（本問の (1) の後半の初等的な計算と同様である）．したがって，$n \in (2)$，つまり，$\mathrm{Ker}(f) \subset (2)$ となる．逆向きの包含関係は，$f(2) = 2+P_1 = P_1$ より $2 \in \mathrm{Ker}(f)$ であることから従うので，以上より $\mathrm{Ker}(f) = (2)$ である．これより，f に環準同型定理を用いれば，環同型 $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/(2) \simeq \mathbb{Z}[\sqrt{5}i]/P_1$ が得られる．この左辺は体であるので，命題 6.34 より $\mathbb{Z}[\sqrt{5}i]/P_1$ も体である．しがたって，定理 6.115 より P_1 は極大イデアルである．

P_2, Q_1, Q_2 についても同様にして $\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}[\sqrt{5}i]/P_2$，$\mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}[\sqrt{5}i]/Q_1$，および，$\mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}[\sqrt{5}i]/Q_2$ が示せるので，P_2, Q_1, Q_2 は極大イデアルであることがわかる．

(3) $P_1 = (2, 1+\sqrt{5}i) = (2, -2+(1+\sqrt{5}i)) = (2, -1+\sqrt{5}i) = (2, (-1)(-1+\sqrt{5}i)) = (2, 1-\sqrt{5}i) = P_2$ となる．よって，$P_1 = P_2$ が成り立つ．次に，問 6.69 より，$P_1^2 = P_1P_2 = (4, 2(1+\sqrt{5}i), 2(1-\sqrt{5}i), 6) = (2)(2, 1+\sqrt{5}i, 1-\sqrt{5}i, 3)$ となる．ここで $(2, 1+\sqrt{5}i, 1-\sqrt{5}i, 3) \ni 3-2 = 1$ より $(2, 1+\sqrt{5}i, 1-\sqrt{5}i, 3) = (1)$ である．よって，$P_1^2 = (2)(1) = (2)$ が成り立つ．同様に，$Q_1Q_2 = (9, 3(1+\sqrt{5}i), 3(1-\sqrt{5}i), 6) = (3)(3, 1+\sqrt{5}i, 1-\sqrt{5}i, 2) = (3)(1) = (3)$ となるので，$Q_1Q_2 = (3)$ が成り立つ．

$(1+\sqrt{5}i) = P_1Q_1$, $(1-\sqrt{5}i) = P_2Q_2$ についても同様に示すことができる．

最後に，$6 = 2 \cdot 3 = (1+\sqrt{5}i)(1-\sqrt{5}i)$ より「とくに」以下もこれらの関係式より従う． □

演習 14　（本演習は，問題文の最初の行において「UFD とする」を「UFD とし，K を R の商体とする」に,「$R[x]$ の元」を「$R[x]$ の定数でない元」に，最後の行において「R 上既約」を「K 上既約」に訂正する.）

仮に $f(x)$ が K 上可約であるとすれば，命題 6.157 より，$R[x]$ で可約であるので，$f(x) = g(x)h(x)$，$\deg(f) \geq 1$，$\deg(g) \geq 1$ となる $g(x), h(x) \in R[x]$ が存在する．そこで，

$$g(x) = b_0 + b_1 x + \cdots + b_l x^l, \quad h(x) = c_0 + c_1 x + \cdots + c_m x^m$$

とする．ここで，$b_l \neq 0$，$c_m \neq 0$，$l \geq 1$，$m \geq 1$ である．このとき，$p \nmid a_n = b_l c_m$ より $p \nmid b_l$ かつ $p \nmid c_m$ である．また，$p \mid a_0$，$p^2 \nmid a_0$ と $a_0 = b_0 c_0$ より，b_0 と c_0 のどちらか一方だけが p で割り切れる．いま仮に $p \mid b_0$，$p \nmid c_0$ とする．$p \nmid b_l$ であったので，$g(x)$ の係数がすべて p で割り切れることはない．そこで，b_0 から b_{r-1} までは p で割り切れ，b_r は p で割り切れないような $0 < r < l$ がとれる．このとき，$f(x)$ の係数 a_r は

$$a_r = b_0 c_r + b_1 c_{r-1} + \cdots + b_{r-1} c_1 + b_r c_0$$

となるので（未定義の係数は 0 とする），右辺に注目すると，最後の項以外は p で割り切れ，最後の項 $b_r c_0$ は p で割り切れない．したがって，$p \nmid a_r$ を得る．しかし，$0 < r \leq l < n$ であるので，これは仮定に反する．$p \nmid b_0$，$p \mid c_0$ とした場合にも，同様に矛盾が生じるので，$f(x)$ は K 上既約である．　□

演習 15　この問題については，代数学の基本定理（1 次以上の複素数係数多項式は少なくとも 1 つの複素数根をもつ．よって，$n \geq 1$ とするとき，因数定理より複素数係数の n 次多項式は重複も込めてちょうど n 個の複素数根をもつ）を証明無しに利用する（証明は参考文献の [4]，[8]，[11]，[13] や [15] などを参照のこと．これはガウスの基本定理とも呼ばれる）.

まず，$\mathbb{C}[x]$ の既約元を求める．$f(x) \in \mathbb{C}[x]$ を既約元とする．代数学の基本定理より $f(\gamma) = 0$ となる $\gamma \in \mathbb{C}$ が存在する．命題 4.49（因数定理）より，$f(x) = (x - \gamma)q(x)$ となる $q(x) \in \mathbb{C}[x]$ が存在する．f は既約元であったから，$q(x)$ は零でない定数である．したがって，$f(x) = \alpha x + \beta$（$\alpha, \beta \in \mathbb{C}$，$\alpha \neq 0$）と書ける．

逆に，$f(x) = \alpha x + \beta$ （$\alpha, \beta \in \mathbb{C}$，$\alpha \neq 0$）は常に既約元である．実際，$f(x) = g(x)h(x)$（$g(x), h(x) \in \mathbb{C}[x]$）と書けたとすると，命題 6.46 より $1 = \deg(f) = \deg(g) + \deg(h)$ となり，$g(x) \in \mathbb{C}^\times$ または $h(x) \in \mathbb{C}^\times$ でなくてはならない．よって，$f(x)$ は既約元である．

以上より，$\mathbb{C}[x]$ の既約元は，

$$f(x) = \alpha x + \beta \quad (\alpha, \beta \in \mathbb{C}, \alpha \neq 0)$$

である．

次に，$\mathbb{R}[x]$ の既約元を求める．$f(x) \in \mathbb{R}[x]$ を既約元とする．$\mathbb{R}[x] \subset \mathbb{C}[x]$ なので，代数学の基本定理より $f(\gamma) = 0$ となる $\gamma \in \mathbb{C}$ が存在する．このとき，$\gamma \in \mathbb{R}$ であれば，先の $\mathbb{C}[x]$ の既約元の決定と同様にして，$f(x) = ax + b$（$a, b \in \mathbb{R}$，$a \neq 0$）と書けることがわかる．そこで以下，$\gamma \notin \mathbb{R}$ とする．いま $(x - \gamma)(x - \overline{\gamma}) \in \mathbb{R}[x]$ であるので，定理 6.51（多項式の除法定理）より

$f(x)=(x-\gamma)(x-\overline{\gamma})g(x)+r(x)$ かつ $\deg(r)<2$ となる $g(x),r(x)\in\mathbb{R}[x]$ が存在する．ここで，$f(x)\in\mathbb{R}[x]$ より $f(\overline{\gamma})=\overline{f(\gamma)}=\overline{0}=0$ となる．よって，$r(\gamma)=0$ かつ $r(\overline{\gamma})=0$ が得られる．$\gamma\notin\mathbb{R}$ より $\gamma\neq\overline{\gamma}$ であるから，問 6.50 より γ は $\mathbb{R}$ 上の 1 次以下の多項式の根にはなり得ない．したがって，$r(x)=0$ であり，$f(x)=(x-\gamma)(x-\overline{\gamma})g(x)$ となる．$f(x)$ は既約元としたので，$g(x)\in\mathbb{R}^{\times}$ である．つまり，$f(x)=\delta(x-\gamma)(x-\overline{\gamma})$（$\delta\in\mathbb{R}^{\times}$）となる．これは実数根をもたない 2 次の実数係数多項式であるので，$f(x)=ax^2+bx+c$（$a,b,c,\in\mathbb{R}$，$a\neq0$，$b^2-4ac<0$）で与えられる．

逆に，$f(x)=ax+b$（$a,b\in\mathbb{R}$，$a\neq0$）と $f(x)=ax^2+bx+c$（$a,b,c,\in\mathbb{R}$，$a\neq0$，$b^2-4ac<0$）は常に $\mathbb{R}[x]$ の既約元である．実際，$f(x)$ が 1 次式であれば，$\mathbb{C}[x]$ のときと同様に $f(x)$ は常に既約元であり，また，$f(x)$ がこの形の 2 次式であれば，2 次方程式の根の公式より $f(x)$ は実数解をもたないので，命題 4.49（因数定理）より 1 次の実数係数多項式を因数をもたない．よって，$\deg(f)=2$ より $f(x)$ は既約元である．

以上より，$\mathbb{R}[x]$ の既約元は，

$$\begin{aligned} f(x) &= ax+b \quad (a,b\in\mathbb{R},a\neq0) \\ f(x) &= ax^2+bx+c \quad (a,b,c,\in\mathbb{R},a\neq0,b^2-4ac<0) \end{aligned}$$

である． □

演習 16　R が体であれば，例題 6.128 より $R[x]$ は PID であるので，以下，$R[x]$ が PID ならば R は体であることを示す．

$a\in R$，$a\neq0$ とし，$I=(a,x)$ とおく．$R[x]$ が PID より $(a,x)=(f(x))$ となる $f(x)\in R[x]$ がとれる．よって，$a=f(x)g(x)$（$g(x)\in R[x]$）と書けて，命題 6.46 より $0=\deg(f)+\deg(g)$ となるので，とくに $\deg(f)=0$ である．つまり，$f(x)=b\in R-\{0\}$ となる．したがって，$(a,x)=(b)$ となる．すると，$x=bh(x)$（$h(x)\in R[x]$）と書けて，再び命題 6.46 より $1=\deg(b)+\deg(h)$ であるから $\deg(h)=1$ となる．よって，$h(x)=cx+d$（$c,d\in R$）の形であるから，$x=bcx+bd$ となり，$bc=1$ を得る．したがって，$b\in R^{\times}$ である．ゆえに，命題 6.70 より $(a,x)=(1)=R[x]$ となる．これより，$ap(x)+xq(x)=1$ となる $p(x),q(x)\in R[x]$ が存在する．この式に $x=0$ を代入すれば，$ap(0)=1$ となる R における等式が得られるので，a は可逆元である．したがって，0 でない R の元はすべて可逆元であるので，R は体である．

以上より，$R[x]$ が PID であることと R が体であることは同値である． □