離散数学演習 11　解答例

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

2.
$$
\begin{array}{rll}
 & (x^2+2x)u(x)+(x^3+5x^2+7x+2)v(x) & \\
= & (x^2+2x)(u(x)+(x+3)v(x))+(x+2)v(x) & \\
= & (x^2+2x)w(x)+(x+2)v(x) & (w(x)=u(x)+(x+3)v(x)) \\
= & (x+2)(xw(x)+v(x)) &
\end{array}
$$

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

3. (1) 加算表は次の通り.　　乗算表は次の通り.

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

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

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

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

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

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

(6) (1)〜(5) から, 以下のことは明らかである.

- 任意の $m, n, k \in \mathbf{Z}_4$ に対して, $m+_4(n+_4 k)=(m+_4 n)+_4 k$. すなわち, 加法の結合則が成り立つ.
- 加法の単位元が存在する.
- 任意の $n \in \mathbf{Z}_4$ に対して, 加法の逆元 $-n$ が存在する.
- 任意の $m, n \in \mathbf{Z}_4$ に対して, $m+_4 n=n+_4 m$. すなわち, 加法の交換則が成り立つ.
- 任意の $m, n, k \in \mathbf{Z}_4$ に対して, $m\cdot_4(n\cdot_4 k)=(m\cdot_4 n)\cdot_4 k$. すなわち, 乗法の結合則が成り立つ.
- 乗法の単位元が存在する.
- 任意の $m, n, k \in \mathbf{Z}_4$ に対して, $m\cdot_4(n+_4 k)=(m\cdot_4 n)+_4(m\cdot_4 k)$. また, $(m+_4 n)\cdot_4 k=(m\cdot_4 k)+_4(n\cdot_4 k)$. すなわち, 分配則が成り立つ.

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

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

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

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

(3) i) 任意の $(a,b), (c,d), (e,f) \in \mathbf{Z}^2$ に対して,
$$\begin{aligned}((a,b)+(c,d))+(e,f) &= (a+c, b+d)+(e,f)\\ &= ((a+c)+e, (b+d)+f)\\ &= (a+(c+e), b+(d+f))\\ &= (a,b)+(c+e, d+f)\\ &= (a,b)+((c,d)+(e,f))\end{aligned}$$
となるから, 加法の結合則が成り立つ.

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

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

iv) 任意の $(a,b), (c,d) \in \mathbf{Z}^2$ に対して,
$$\begin{aligned}(a,b)+(c,d) &= (a+c, b+d)\\ &= (c+a, d+b)\\ &= (c,d),(a,b)\end{aligned}$$
となるから, 加法の交換則が成り立つ.

v) 任意の $(a,b), (c,d), (e,f) \in \mathbf{Z}^2$ に対して,
$$\begin{aligned}((a,b)\cdot(c,d))\cdot(e,f) &= (ac, bd)\cdot(e,f)\\ &= ((ac)e, (bd)f)\\ &= (a(ce), b(df))\\ &= (a,b)\cdot(ce, df)\\ &= (a,b)\cdot((c,d)\cdot(e,f))\end{aligned}$$
となるから, 乗法の結合則が成り立つ.

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

vii) 任意の $(a,b), (c,d), (e,f) \in \mathbf{Z}^2$ に対して,
$$\begin{aligned}(a,b)\cdot((c,d)+(e,f)) &= (a,b)\cdot(c+e, d+f)\\ &= (a(c+e), b(d+f))\\ &= (ac+ae, bd+bf)\\ &= (ac,bd)+(ae,bf)\\ &= ((a,b)\cdot(c,d))+((a,b)\cdot(e,f))\end{aligned}$$
$$\begin{aligned}((a,b)+(c,d))\cdot(e,f)) &= ((a+c, b+d)\cdot(e,f)\\ &= ((a+c)e, (b+d)f)\\ &= (ae+ce, bf+df)\\ &= (ae,bf)+(ce,df)\\ &= ((a,b)\cdot(e,f))+((c,d)\cdot(e,f))\end{aligned}$$
となるから, 分配則が成り立つ.

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

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

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

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

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

となるから, 乗法の結合則が成り立つ.

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

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

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

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

となるから, 分配則が成り立つ.

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

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

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

任意の $A,B,C\in\mathcal{P}(X)$ に対して,

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

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

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

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

iv) 任意の $A,B\in\mathcal{P}(X)$ に対して,

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

ゆえに, 加法の交換則が成り立つ.

v) 任意の $A,B,C\in\mathcal{P}(X)$ に対して,

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

ゆえに, 乗法の結合則が成り立つ.

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

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

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

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

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

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

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

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

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

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

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