離散数学演習 14　解答例

1. (1) i) 加算表は次の通り.　　乗算表は次の通り.

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

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

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

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

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

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

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

となるから, 加法の結合則が成り立つ.

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

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

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

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

となるから, 加法の交換則が成り立つ.

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

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

となるから, 乗法の結合則が成り立つ.

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

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

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

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

となるから, 分配則が成り立つ.

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

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

となるから, 乗法の交換則が成り立つ.

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

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

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

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

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

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

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

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