演習問題2の解答 (環論)

演習問題 2-1 の解答

(1)

$$\overline{2}^1 = \overline{2},\quad \overline{2}^2 = \overline{4},\quad \overline{2}^3 = \overline{8},\quad \overline{2}^4 = \overline{16} = \overline{5},\quad \overline{2}^5 = \overline{32} = \overline{10}.$$

また $\overline{2}^5 = \overline{-1}$ に注意すると,

$$\begin{aligned}&\overline{2}^6 = \overline{-1}\cdot\overline{2}^1 = \overline{9},\quad \overline{2}^7 = \overline{-1}\cdot\overline{2}^2 = \overline{7},\quad \overline{2}^8 = \overline{-1}\cdot\overline{2}^3 = \overline{3},\\ &\overline{2}^9 = \overline{-1}\cdot\overline{2}^4 = \overline{6},\quad \overline{2}^{10} = \overline{-1}\cdot\overline{2}^5 = \overline{1}.\end{aligned}$$

(2) (1) より $\overline{2}^n$ $(n = 1, 2, ..., 10)$ は $\overline{1}, \overline{2}, ..., \overline{10}$ の全ての値を 1 回ずつ取るので,

$$\overline{1}\cdot\overline{2}\cdots\overline{10} = \overline{2}^{1+2+\cdots+10} = \overline{2}^{55} = \left(\overline{2}^5\right)^{11} = \overline{-1}.$$

[**補足**] 任意の素数 p に対して, $(p-1)! \equiv -1 \pmod p$ が成り立つ (ウィルソンの定理). (2) はこの定理の $p = 11$ の場合である.

演習問題 2-2 の解答

(1) $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) \in I$ より $\overline{x}^5 = \overline{1}$.

(2) $\overline{x}^5 = \overline{1}$ より

$$\begin{aligned}\overline{x^3}\cdot(\overline{(x^8+x^2)} - \overline{(x^2+1)}) &= \overline{x^3}\cdot(\overline{(x^3+x^2)} - \overline{(x^2+1)})\\ &= \overline{x^3}\cdot\overline{(x^3-1)}\\ &= \overline{x^6 - x^3}\\ &= \overline{-x^3 + x}.\end{aligned}$$

(3) $\overline{x}^5 = \overline{1}$ および $\overline{x^4} = \overline{-x^3 - x^2 - x - 1}$ より

$$\overline{x^{20} + x^9 + 1} = \overline{x^4 + 2} = \overline{-x^3 - x^2 - x + 1}.$$

よって求める余りは $-x^3 - x^2 - x + 1$.

(4) ユークリッドの互除法より

$$1 = (x^3+1)(x^2+x+1) + (-x)(x^4+x^3+x^2+x+1)$$

を得る. よって

$$\overline{1} = \overline{x^3+1}\cdot\overline{x^2+x+1}.$$

従って $\overline{x^2+x+1}$ の逆元は $\overline{x^3+1}$.

演習問題 2-3 の解答

(1) 仮に $1 \in I$ とすると, $1 = xg_1(x,y)+yg_2(x,y)$ $(g_1(x,y),\ g_2(x,y) \in A)$ と表せる. $(x,y)=(0,0)$ を代入すると $1=0$ となり矛盾. よって $1 \notin I$ であり, 特に $I \neq A$.

次に $I \subsetneq K \subseteq A$ となるイデアル K を取る. $f(x,y) \in K \setminus I$ を取り,

$$f(x,y) = a + xh_1(x,y) + yh_2(x,y) \quad (a \in \mathbb{C},\ h_1(x,y),\ h_2(x,y) \in A)$$

と表す. $a=0$ ならば, $f(x,y) \in I$ となり矛盾. よって $a \in \mathbb{C}^\times = \mathbb{C}[x,y]^\times$. 一方, $f(x,y) \in K$ および $xh_1(x,y)+yh_2(x,y) \in I \subseteq K$ より $a \in K$. よって $K = A$. 以上より I は A の極大イデアル.

(2) 1 変数多項式環 $\mathbb{C}[t]$ と環準同型 $\varphi : A \to \mathbb{C}[t]$ $(f(x,y) \mapsto f(t,t^2))$ を考える. まず, $\ker\varphi = (y-x^2)$ を示す. $y-x^2 \in \ker\varphi$ より $(y-x^2) \subseteq \ker\varphi$. 逆に $f(x,y) \in \ker\varphi$ とする. $f(x,y)$ を y の多項式と見て $y-x^2$ で割ると,

$$f(x,y) = q(x,y)(y-x^2) + r(x) \quad (q(x,y) \in A,\ r(x) \in \mathbb{C}[x])$$

と表せる. $f(x,y) \in \ker\varphi$ より $0 = f(t,t^2) = r(t)$. 従って $f(x,y) = q(x,y)(y-x^2) \in (y-x^2)$. 以上より $\ker\varphi = (y-x^2)$.

$f(t) \in \mathbb{C}[t]$ に対して, $h(x,y) = f(x)$ と置くと, $\varphi(h(x,y)) = f(t)$. よって φ は全射となる. 準同型定理から

$$A/(y-x^2) = A/\ker\varphi \simeq \varphi(A) = \mathbb{C}[t].$$

これより, $A/(y-x^2)$ は整域だが, 体ではない. 定理 9-3 より $(y-x^2)$ は素イデアルだが, 極大イデアルでない.

(1) で準同型定理を使う方法

環準同型 $\psi : \mathbb{C}[x,y] \to \mathbb{C}$ $(f(x,y) \mapsto f(0,0))$ を考える. ψ は全射で, $\ker\psi = I$ であることが確かめられる. 準同型定理から

$$A/I = A/\ker\varphi \simeq \varphi(A) = \mathbb{C}.$$

$\mathbb{C}$ は体より, I は極大イデアルである.

演習問題 2-4 の解答

(1) 仮に同型写像 $f : \mathbb{C} \to \mathbb{R}$ が存在したとする. $\alpha = f(\sqrt{-1})$ と置くと, $\alpha \in \mathbb{R}$ で,

$$\alpha^2 = f(\sqrt{-1})^2 = f((\sqrt{-1})^2) = f(-1) = -f(1) = -1$$

となるから矛盾. 従って $\mathbb{C}$ と $\mathbb{R}$ は同型ではない.

(2) 仮に同型写像 $g : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が存在したとする. 整数 a と自然数 n に対して, $[a]_n = a + n\mathbb{Z}$ とする. g は環準同型より $g([1]_4) = ([1]_2, [1]_2)$. よって

$$g([2]_4) = 2g([1]_4) = 2 \cdot ([1]_2, [1]_2) = ([0]_2, [0]_2).$$

g は単射より $[2]_4 = [0]_4$ となり矛盾. 従って $\mathbb{Z}/4\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ は同型ではない.

演習問題 2-5 の解答

(1) φ が環準同型であること.

(i) $\varphi(1) = (1,1)$.

(ii) $f(t), g(t) \in \mathbb{C}[t]$ に対して,

$$\begin{aligned} \varphi(f(t)+g(t)) &= (f(a)+g(a), f(b)+g(b)) \\ &= (f(a), f(b)) + (g(a), g(b)) \\ &= \varphi(f(t)) + \varphi(g(t)). \end{aligned}$$

(iii) $f(t), g(t) \in \mathbb{C}[t]$ に対して,

$$\begin{aligned} \varphi(f(t) \cdot g(t)) &= (f(a)g(a), f(b)g(b)) \\ &= (f(a), f(b)) \cdot (g(a), g(b)) \\ &= \varphi(f(t)) \cdot \varphi(g(t)). \end{aligned}$$

よって φ は環準同型である.

(2) $f(t) \in I$ とする. $f(t) = (t-a)(t-b)g(t) \ \ (g(t) \in \mathbb{C}[t])$ と表せるので,

$$\varphi(f(t)) = (f(a), f(b)) = (0.0).$$

よって $f(t) \in \ker\varphi$. 逆に $f(t) \in \ker\varphi$ とすると, $(f(a), f(b)) = (0,0)$. 因数定理から

$$f(t) = (t-a)(t-b)h(t) \quad (h(t) \in \mathbb{C}[t])$$

と表せる. よって $f(t) \in I$. 以上より $I = \ker\varphi$.
次に $(p,q) \in \mathbb{C} \times \mathbb{C}$ に対して,

$$f(t) = \frac{p-q}{a-b}(t-b) + q$$

と置く ($f(a) = p,\ f(b) = q$ となる 1 次式を考える). このとき,

$$\varphi(f(t)) = (f(a), f(b)) = (p, q).$$

よって φ は全射. 準同型定理より

$$\mathbb{C}[t]/I = \mathbb{C}[t]/\ker\varphi \simeq \varphi(\mathbb{C}[t]) = \mathbb{C} \times \mathbb{C}.$$

演習問題 2-6 の解答

(1) $3=(2+\sqrt{7})(-2+\sqrt{7})\in I$ より $3\mathbb{Z}\subseteq I\cap\mathbb{Z}$. 逆に $x\in I\cap\mathbb{Z}$ とすると

$$x=(2+\sqrt{7})(a+b\sqrt{7})\quad(a,b\in\mathbb{Z})$$

と表せる. $x=(2a+7b)+(a+2b)\sqrt{7}$ であり, $x\in\mathbb{Z}$ なので $a+2b=0$. これより $x=3b\in 3\mathbb{Z}$. よって $I\cap\mathbb{Z}\subseteq 3\mathbb{Z}$. 以上より $3\mathbb{Z}=I\cap\mathbb{Z}$.

(2) について.

$$\frac{\sqrt{7}-1}{2+\sqrt{7}}=3-\sqrt{7}$$

より $\sqrt{7}-1=(3-\sqrt{7})(2+\sqrt{7})\in I$. よって $\sqrt{7}+I=1+I$.

(3) 環準同型 $\pi:\mathbb{Z}\to A/I$ $(x\mapsto x+I)$ を考える. $x\in\mathbb{Z}$ に対して, (1) から

$$x\in\ker\pi\iff x\in I\cap\mathbb{Z}=3\mathbb{Z}.$$

よって $\ker\pi=3\mathbb{Z}$. また $y=a+b\sqrt{7}\in A$ $(a,b\in\mathbb{Z})$ に対して, (2) より $y+I=(a+b)+I$. よって $\pi(a+b)=y+I$. よって π は全射. 準同型定理から

$$\mathbb{Z}/3\mathbb{Z}\simeq A/I.$$

(4) $\mathbb{Z}/3\mathbb{Z}$ は体なので, A/I も体である. 従って I は A の極大イデアルである.