代数学2,第3回の内容の理解度チェックの解答

2025/5/12 担当:那須

 $\boxed{1}$ 次の多項式 $f(x), g(x)\mathbb{Z}[x]$ に対し、多項式の割り算を実行し

$$f(x) = g(x)q(x) + r(x), \qquad \deg r(x) < \deg g(x)$$

を満たす q(x) と r(x) を求めよ.

(1)
$$f(x) = x^2 + 3x + 1$$
, $g(x) = x - 2$

(2)
$$f(x) = 2x^3 - x + 5$$
, $g(x) = x + 1$

(3)
$$f(x) = 2x^5 - x^2 + 5$$
, $g(x) = x^2 + x + 1$

(解答) 普通に割り算を実行すると以下のようになる.

(1)
$$q(x) = x + 5$$
, $r(x) = 11$

(2)
$$q(x) = 2x^2 - 2x + 1$$
, $r(x) = 4$

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

2 $f(x) \in \mathbb{R}[x]$ を実数係数の多項式とし、 $\alpha \in \mathbb{R}$ を実数とするとき次が成り立つことを証明せよ.

—— 因数定理 —

$$f(\alpha) = 0 \iff f(x)$$
 は $x - \alpha$ で割り切れる

(**解答**) まず (⇒) を示す. $f(\alpha) = 0$ と仮定する. f(x) と $g(x) = x - \alpha$ に対し、剰余定理を適用すると

$$f(x) = (x - \alpha)q(x) + c$$

を満たす $q(x) \in \mathbb{R}[x]$ と定数 $c \in \mathbb{R}$ が存在する. 両辺に $x = \alpha$ を代入すれば

$$f(\alpha) = (\alpha - \alpha)q(\alpha) + c = 0 \cdot q(\alpha) + c = c$$

より $c = f(\alpha)$ が成り立つ. 仮定より c = 0. すなわち f(x) は $x - \alpha$ で割り切れる.

次に (\Leftarrow) を示す. f(x) が $x - \alpha$ で割り切れるならば,

$$f(x) = (x - \alpha)q(x)$$

を満たす $q(x) \in \mathbb{R}[x]$ が存在する. したがって $f(\alpha) = (\alpha - \alpha)q(\alpha) = 0$.

- ③ 次の環RとR上の多項式 $f(x) \in R[x]$ に対し、f(x)のRにおける根、すなわち方程式f(x) = 0の解 $x = \alpha \ (\alpha \in R)$ をすべて求めよ.
 - (1) $R = \mathbb{Z}/13\mathbb{Z}, f(x) = 5x + 37$
 - (2) $R = \mathbb{Z}/35\mathbb{Z}, f(x) = x^2 1$
 - (3) $R = \mathbb{Z}/2\mathbb{Z}, f(x) = x^3 + 1$
 - (4) $R = \mathbb{Z}/2\mathbb{Z}, f(x) = x^4 + x^2 + 1$

(解答)

(1) $R=\mathbb{Z}/13\mathbb{Z}$ において、方程式 5x+37=0 を考える.法 13 で $37\equiv11$ なので、 $R=\mathbb{Z}/13\mathbb{Z}$ において 5x+37=5x+11 である.すなわち 5x=-11 を解けば良い.R における 5 の乗法逆元 5^{-1} を両辺にかけると.

$$x = 1x = 5^{-1} \cdot 5x = 5^{-1} \cdot (-11)$$

となる. $5 \times 8 = 40 \equiv 1 \mod 13$ より, 法 13 の下で $5^{-1} = 8$ となる. したがって $x = 8 \cdot (-11) = -88 = 3$ と求まる.

(2) $R=\mathbb{Z}/35\mathbb{Z}$ において、方程式 $f(x)=x^2-1=0$ を考える. 中国剰余定理 $\mathbb{Z}/35\mathbb{Z}\simeq\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}$ より、

$$f(x) = 0 \text{ in } \mathbb{Z}/35\mathbb{Z} \Longleftrightarrow egin{cases} x^2 = 1 & \text{in } \mathbb{Z}/5\mathbb{Z} \\ x^2 = 1 & \text{in } \mathbb{Z}/7\mathbb{Z} \end{cases}$$
 である.

 $x^2 = 1 \mod 5$ を解くと $x = \pm 1 \mod 5$, $x^2 = 1 \mod 7$ を解くと $x = \pm 1 \mod 7$ となる. したがって, 再び中国剰余定理より,

$$\begin{cases} x \equiv 1 \mod 5 \\ x \equiv 1 \mod 7 \end{cases} \begin{cases} x \equiv 1 \mod 5 \\ x \equiv -1 \mod 7 \end{cases} \begin{cases} x \equiv -1 \mod 5 \\ x \equiv 1 \mod 7 \end{cases} \begin{cases} x \equiv -1 \mod 5 \\ x \equiv -1 \mod 7 \end{cases}$$

をそれぞれ解くとx = 1.6.29.34となる.

(3) $R=\mathbb{Z}/2\mathbb{Z}$ において、方程式 $f(x)=x^3+1=0$ を考える。 $R=\{0,1\}$ なので、x=0 または x=1 を代入し、方程式が成り立つか調べれば良い。

$$f(0) = 0^3 + 1 = 1 \neq 0$$

より x = 0 は方程式の解ではない.

$$f(1) = 1^3 + 1 = 1 + 1 = 0$$

より x=1 は方程式の解である. したがって求める解は x=1 のみ.

(4) $R = \mathbb{Z}/2\mathbb{Z}$ において、方程式 $f(x) = x^4 + x^2 + 1 = 0$ を考える. $R = \{0,1\}$ なので、x = 0 または x = 1 を代入し、方程式が成り立つか調べれば良い.

$$f(0) = 0^4 + 0^2 + 1 = 1 \neq 0$$

より x=0 は方程式の解ではない.

$$f(1) = 1^4 + 1^2 + 1 = 1 \neq 0$$

より x=1 も方程式の解ではない. したがって方程式 f(x)=0 は $R=\mathbb{Z}/2\mathbb{Z}$ において解を持たない.

^{1※}この講義に関する情報はホームページを参照. https://hirokazunasu.github.io/2025/alg2.html