問題2-2 以下の$\mathbb{Z}$係数多項式たちが$\mathbb{Q}$上の既約多項式になることを示せ.

(1) x^3+2x-2.

(2) $x^4+10x^3+15x^2+35x+55$.

(3) 正の整数nに対する x^n-14.

(4) 素数pに対する $x^{p-1}+x^{p-2}+\cdots+x+1$.

例: $x+1$, x^2+x+1, $x^4+x^3+x^2+x+1$, $x^6+x^5+\cdots+x+1$, $\cdots$

記号 $a \mid b \iff a$ で b は割り切れる $\iff a$ は b の約数 $\iff b$ は a の倍数

$a \mid b$ の否定を $a \nmid b$ と書く.

例 ・ $2 \nmid 1$, $2 \mid 0$, $2 \mid 2$, $2 \mid 4$, $2 \mid 6$, $\ldots$

Eisensteinの判定法の$\mathbb{Z}$の場合

$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, $a_i\in\mathbb{Z}$ のとき, 素数pについて,

$$p\nmid a_n,\ p\mid a_{n-1},\ \ldots,\ p\mid a_1,\ p\mid a_0,\ p^2\nmid a_0 \Rightarrow f(x) \text{ は } \mathbb{Q} \text{ 上既約}.$$

$\boxed{\text{解答例}}$ (1), (2), (3) では Eisenstein の判定法を直接使える.

(1) x^3+2x-2.　　　　2|0 の 0 は x^2 の係数

$2\nmid 1$, $2 \mid 0$, $2 \mid 2$, $2 \mid -2$, $2^2 \nmid -2$ と Eisenstein の判定法より, これは $\mathbb{Q}$ 上既約.

(2) $x^4+10x^3+15x^2+35x+55$.

$5\nmid 1$, $5\mid 10$, $5\mid 15$, $5\mid 35$, $5\mid 55$, $5^2\nmid 55$ と Eisenstein の判定法より, これは $\mathbb{Q}$ 上既約.

(3) 正の整数 n に対する x^n-14.

$7\nmid 1$, $7\mid 0$, …, $7\mid 0$, $7\mid -14$, $7^2\nmid -14$ と Eisenstein の判定法より, これは $\mathbb{Q}$ 上既約.

この次の(4)には直接に Eisenstein の判定法を使えない.

任意の $a\in\mathbb{Q}$ と $f(x)\in\mathbb{Q}[x]$ について,

$$f(x) \text{ は } \mathbb{Q} \text{ 上既約} \iff f(x+a) \text{ は } \mathbb{Q} \text{ 上既約}$$

を使う.

$$\left(\because \quad f(x)=g(x)h(x) \iff f(x+a)=g(x+a)h(x+a)\right)$$

(4) 素数 p に対する $x^{p-1}+x^{p-2}+\cdots+x+1$. これを $\varphi_p(x)$ と書く.

$\varphi_2(x)=x+1$ は1次なので $\mathbb{Q}$ 上既約.

$$\varphi_3(x)=x^2+x+1=\frac{x^3-1}{x-1}$$ より,

$$\varphi_3(x+1)=\frac{(x+1)^3-1}{x}=\frac{x^3+3x^2+3x+1-1}{x}=x^2+3x+3.$$

$3\nmid 1$, $3\mid 3$, $3\mid 3$, $3^2\nmid 3$ とEisensteinの判定法より, $\varphi_3(x+1)$ は $\mathbb{Q}$ 上既約で, $\varphi_3(x)$ も $\mathbb{Q}$ 上既約.

$$\varphi_p(x)=\frac{x^p-1}{x-1}$$ より,

$$\varphi_p(x+1)=\frac{(x+1)^p-1}{x}=\frac{\sum_{k=0}^{p}\binom{p}{k}x^k-1}{x}=\sum_{k=1}^{p}\binom{p}{k}x^{k-1}=\binom{p}{p}x^{p-1}+\binom{p}{p-1}x^{p-2}+\cdots+\binom{p}{2}x+\binom{p}{1}.$$

$$\binom{p}{p}=1,\ \underbrace{\binom{p}{p-1}=p,\ \ldots,\ \binom{p}{k}=\frac{p(p-1)\cdots(p-k+1)}{k!},\ \ldots,\ \binom{p}{2}=\frac{p(p-1)}{2},\ \binom{p}{1}=p}_{p\text{ で割り切れるが }p^2\text{ で割り切れない}}.$$

$\leftarrow 1\leqq k\leqq p-1$

ゆえに, Eisensteinの判定法より, $\varphi_p(x+1)$ は $\mathbb{Q}$ 上既約で, $\varphi_p(x)$ も $\mathbb{Q}$ 上既約である. □

$\boxed{\text{注意}}$ 素数 p について, $x^{p-1}+x^{p-2}+\cdots+x+1$ は $\mathbb{Q}$ 上既約になるが,

$m,n\in\mathbb{Z}$, $m,n\geqq 2$ のとき, $x^{mn-1}+x^{mn-2}+\cdots+x+1$ は $\mathbb{Q}$ 上既約でない.

なぜならば,

$$x^{mn-1}+x^{mn-2}+\cdots+x+1=\frac{x^{mn}-1}{x-1}=\frac{x^m-1}{x-1}\;\frac{\overbrace{x^{mn}}^{(x^m)^n}-1}{x^m-1}$$

$$=(x^{m-1}+x^{m-2}+\cdots+x+1)(x^{m(n-1)}+x^{m(n-2)}+\cdots+x^m+1).$$

たとえば

$$x^3+x^2+x+1=\frac{x^4-1}{x-1}=\frac{x^2-1}{x-1}\;\frac{x^4-1}{x^2-1}=(x+1)(x^2+1)$$

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

$$x^5+x^4+x^3+x^2+x+1$$

$$=\frac{x^2-1}{x-1}\;\frac{x^6-1}{x^2-1}=(x+1)(x^4+x^2+1)=(x+1)(x^2+x+1)(x^2-x+1)$$

$$=\frac{x^3-1}{x-1}\;\frac{x^6-1}{x^3-1}=(x^2+x+1)(x^3+1)=(x^2+x+1)(x+1)(x^2-x+1)$$

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

$\square$

x^n-1 を割り切る $\mathbb{Q}$ 上既約な多項式を円分多項式と呼ぶ.