問4.1

(1) $\mathbb{Z}[X] \ni {}^{\forall} f(X), g(X)$ $\left(f(X) = \sum a_i X^i, g(X) = \sum b_i X^i\right)$ に対し.

(積)

$$\pi_p(f(X)g(X)) = \pi_p\left(\left(\sum_i a_i X^i\right)\left(\sum_j b_j X^j\right)\right)$$
$$= \pi_p\left(\sum_k \left(\sum_{i+j=k} a_i b_j\right) X^k\right)$$
$$= \sum_k \left(\sum_{i+j=k} a_i b_j\right) (\mathrm{mod}\ p)\, X^k$$

$$\pi_p(f(X))\pi_p(g(X)) = \pi_p\left(\sum_i a_i X^i\right)\pi_p\left(\sum_j b_j X^j\right)$$
$$= \left(\sum_i a_i\ (\mathrm{mod}\ p)\, X^i\right)\left(\sum_j b_j\ (\mathrm{mod}\ p)\, X^j\right)$$
$$= \sum_k \left(\sum_{i+j=k} a_i (\mathrm{mod}\ p)\, b_j (\mathrm{mod}\ p)\right) X^k$$
$$= \sum_k \left(\sum_{i+j=k} a_i b_j\right) (\mathrm{mod}\ p)\, X^k$$

$\therefore \mathbb{Z}[X] \ni {}^{\forall} f(X), g(X),\ \pi_p(f(X)g(X)) = \pi_p(f(X))\pi_p(g(X))$

(和)

$$\pi_p(f(X)+g(X)) = \pi_p\left(\sum_i a_i X^i + \sum_j b_j X^j\right)$$
$$= \sum_i a_i\ (\mathrm{mod}\ p)\, X^i + \sum_j b_j\ (\mathrm{mod}\ p)\, X^j$$

$$\pi_p(f(X)) + \pi_p(g(X)) = \pi_p\left(\sum_i a_i X^i\right) + \pi_p\left(\sum_j b_j X^j\right)$$
$$= \sum_i a_i\ (\mathrm{mod}\ p)\, X^i + \sum_j b_j\ (\mathrm{mod}\ p)\, X^j$$

$\therefore \mathbb{Z}[X] \ni {}^{\forall} f(X), g(X),\ \pi_p(f(X)+g(X)) = \pi_p(f(X)) + \pi_p(g(X))$

(単位元)

$\mathbb{Z}[X], \mathbb{Z}/p\mathbb{Z}[X]$ の乗法の単位元は,いずれも 1 であり.

$\pi_p(1) = 1\ (\mathrm{mod}\ 2) = 1$ であるから

$\mathbb{Z}[X], \mathbb{Z}/p\mathbb{Z}[X]$ の乗法の単位元 $1_{\mathbb{Z}[X]}, 1_{\mathbb{Z}/p\mathbb{Z}[X]}$ に対し.

$\pi_p(1_{\mathbb{Z}[X]}) = 1_{\mathbb{Z}/p\mathbb{Z}[X]}$ が成り立つ.

以上より. $\pi_p : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$ は環準同型写像である.

(2) $f(x)=(x+2)(x^3+2x^2+2x+2)=x^4+x^3+1$ であり、

$\deg(x+2)\geqq 1,\ \deg(x^3+2x^2+2x+2)\geqq 1$ であるから可約である。□

(3) 補題：$\mathbb{Z}/p\mathbb{Z}\ni{}^{\exists}\alpha,\ f(\alpha)=0 \Leftrightarrow f(x)$ が $x-\alpha$ で割り切れる。

($\Leftarrow$) $f(x)$ が $(x-\alpha)$ で割り切れるから $f(x)=(x-\alpha)g(x)$ なる

$g(x)$ が存在する。よって $f(\alpha)=(\alpha-\alpha)g(\alpha)=0$

($\Rightarrow$) $f(\alpha)=0$ であるから $f(x)=(x-\alpha)g(x)+r(x)$ となる

$g(x), r(x)\in\mathbb{Z}/p\mathbb{Z}[x]$ が存在する。ただし、

$\deg(r(x))\leqq\deg(g(x))-1=1-1=0$ ∴ $r(x)=\beta\in\mathbb{Z}/p\mathbb{Z}$ とかける

$0=f(\alpha)=(\alpha-\alpha)g(\alpha)+\beta=\beta$ だから

$f(x)=(x-\alpha)g(x)$ ■

対偶をとることで、$\mathbb{Z}/p\mathbb{Z}\ni{}^{\forall}\alpha,\ f(\alpha)\neq 0 \Rightarrow f(x)$ が $x-\alpha$ で割り切れない

を導ける

$p=2$ の時、$f(0)=1\neq 0,\ f(1)=1\neq 0$ より $f(x)$ は1次の式では割り切れない。

$\mathbb{Z}/2\mathbb{Z}[x]$ 上の次数2の多項式は以下の4つである：

$x^2,\ x^2+1,\ x^2+x,\ x^2+x+1$

ただし、$x^2=x\cdot x,\ x^2+1=(x+1)^2,\ x^2+x=x(x+1)$ であり、

$f(x)$ は次数1の因数を持たないから $f(x)=g(x)h(x)$ とかけるとき、

$g(x), h(x)$ も次数1の因数をもたない。

よって $g(x)=h(x)=x^2+x+1$ でなければならないが、

$g(x)h(x)=(x^2+x+1)^2=x^4+x^2+1\neq f(x)$ であるから $f(x)$ は次数2の

因数はもたない。

さらに $f(x)$ が次数3の因数をもつとき同時に次数1の因数を

もつこととなるが、$f(x)$ は次数1の因数をもたないから次数3

の因数ももたない。

よって $f(x)$ は $\mathbb{Z}/2\mathbb{Z}$ 上で既約であるから $p=2$ //

(4) $f(x)$ が $\mathbb{Z}$ 上可約であるとすると、$f(x)$ は次の2種類のうち、いずれかに分解できる。($a_i, b_i, c_i, d_i \in \mathbb{Z}$)

(i) $f(x) = (x - a_0)(x^3 + b_2 x^2 + b_1 x + b_0)$

(ii) $f(x) = (x^2 + c_1 x + c_0)(x^2 + d_1 x + d_0)$

(i) のとき、

$$\pi_2(f(x)) = \pi_2(x - a_0)\,\pi_2(x^3 + b_2 x^2 + b_1 x + b_0)$$

$$= (x - a_0 \pmod 2)(x^3 + b_2 \pmod 2\, x^2 + b_1 \pmod 2\, x + b_0 \pmod 2)$$

$\in \mathbb{Z}/2\mathbb{Z}[x]$ であり、$f(x)$ は $\mathbb{Z}/2\mathbb{Z}$ 上で可約となるはずだが、これは(3)と矛盾。

(ii) についても、同様の議論により、$f(x) \in \mathbb{Z}/2\mathbb{Z}[x]$ となるが、これは(3)と矛盾。

すなわち、$f(x)$ が $\mathbb{Z}$ 上可約という仮定が間違っていたということであり、$f(x)$ は $\mathbb{Z}$ 上既約となる。■