試験

つぎの二問を解きなさい。

問題 12.1. (70 **点**) **つぎの命題のうち、正しいものが二つある。正しい命題のうち一つを選び、答案用紙に書いて、その証明をしなさい。**(**複数を解答した場合には零点とする。**)

(A) **環としての同型** $\mathbb{R}[X]/(X^2+2) \cong \mathbb{R}\times\mathbb{R}$ **が存在する。**
(B) **環としての同型** $\mathbb{R}[X]/(X^2+2) \cong \mathbb{C}$ **が存在する。**
(C) **環としての同型** $\mathbb{R}[X]/(X^2-2) \cong \mathbb{R}\times\mathbb{R}$ **が存在する。**
(D) **環としての同型** $\mathbb{R}[X]/(X^2-2) \cong \mathbb{C}$ **が存在する。**

必要ならばつぎの事実を証明なしで用いても良い。

(1) $\sqrt{2} \in \mathbb{R}$.
(2) $\sqrt{-1} \notin \mathbb{R}$.
(3) $\sqrt{-2} \notin \mathbb{R}$.

解答: (B) **と** (C) **が正しい。**

問題文にあるように、片方だけの答案を書くべきところであるが、ここでは諸君の便のため、いちおう両方の証明を書いておく。

(B) **の証明**

$$f : \mathbb{R}[X] \to \mathbb{C}$$

を、

$$f(p) = p(\sqrt{-2})$$

で定義する。 f **は環の準同型写像であることが容易に確かめられる。**

任意の複素数 z **にたいし、その実部、虚部をそれぞれ** a, b **とおくと、**

$$z = a + b\sqrt{-1} = f(a + \frac{\sqrt{2}}{2}bX)$$

が成り立つ ($\sqrt{2} \in \mathbb{R}$ (1) **をここで用いる。**)**。**

したがって、 f **は全射。**

つぎに、 $\mathrm{Ker}(f) = (X^2+2)$ **であるということをしめそう。**

まず $\mathrm{Ker}(f) \subset (X^2+2)\mathbb{R}[X]$ **であることを示そう。** $p(X) \in (X^2+2)\mathbb{R}[X]$ **を任意にとると、定義により、**

$$p(X) = (X^2+2)q(X)$$

なる $q(X) \in \mathbb{R}[X]$ **が存在する。**

$$f(p) = p(\sqrt{-2}) = (\sqrt{-2}^2+2)q(\sqrt{-2}) = 0 \cdot q(\sqrt{-2}) = 0$$

すなわち、 $f \in \mathrm{Ker}(f)$ **である。**

つぎに、逆の包含関係を示そう。 $p \in \mathrm{Ker}(f)$ **を任意にとる。** p **を** (X^2+2) **で割った商を** q, **余りを** r **とおくと、二次式で割っているのだから** r **は** X **の一次式で**

$$r = aX + b \qquad (a, b \in \mathbb{R})$$

とかける。

$$p(X) = (X^2+2)q(X) + aX + b$$

両辺に $\sqrt{-2}$ **を代入すると、**

$$0 = f(p) = p(\sqrt{-2}) = 0 \cdot q(\sqrt{-2}) + a\sqrt{-2} + b = a\sqrt{-2} + b$$

$\sqrt{-2} \in \mathbb{R}$ (3) だから、これがおこるのは $a = 0$ かつ $b = 0$ のときのみである。すなわち、

$$p(X) = (X^2 + 2)q(X) \in (X^2 + 2)\mathbb{R}[X]$$

つまり、

$$\mathrm{Ker}(f) \subset (X^2 - 2)\mathbb{R}[X]$$

がわかった。
以上により、 f は同型 (B) を誘導することがわかる。

(C) の証明

$$f : \mathbb{R}[X] \to \mathbb{R} \times \mathbb{R}$$

を、

$$f(p) = (p(\sqrt{2}), p(-\sqrt{2}))$$

で定義する。 f は環の準同型写像であることが容易に確かめられる。
任意の $(a, b) \in \mathbb{R} \times \mathbb{R}$ にたいして、

$$(a, b) = f\left(\frac{1}{2\sqrt{2}}(X + \sqrt{2})a + \frac{1}{2\sqrt{2}}(X - \sqrt{2})b\right)$$

がなりたつ ($\sqrt{2} \in \mathbb{R}$ (1) をここで用いる。)。
ゆえに、 f は全射。
つぎに、$\mathrm{Ker}(f) = (X^2 - 2)$ であるということをしめそう。
まず $\mathrm{Ker}(f) \subset (X^2 - 2)\mathbb{R}[X]$ であることを示そう。$p(X) \in (X^2 + 2)\mathbb{R}[X]$ を任意にとると、定義により、

$$p(X) = (X^2 - 2)q(X)$$

なる $q(X) \in \mathbb{R}[X]$ が存在する。

$$f(p) = (p(\sqrt{2}, p(-\sqrt{2}) = (0, 0)$$

すなわち、$f \in \mathrm{Ker}(f)$ である。
つぎに、逆の包含関係を示そう。$p \in \mathrm{Ker}(f)$ を任意にとる。p を $(X^2 - 2)$ で割った商を q, 余りを r とおくと、二次式で割っているのだから r は X の一次式で

$$r = aX + b \qquad (a, b \in \mathbb{R})$$

とかける。

$$p(X) = (X^2 - 2)q(X) + aX + b$$

両辺に $\sqrt{2}$ を代入すると、

$$p(\sqrt{2}) = 0 \cdot q(\sqrt{2}) + a\sqrt{2} + b = a\sqrt{2} + b$$

同様に、

$$p(-\sqrt{2}) = 0 \cdot q \cdot (-\sqrt{2}) + a \cdot (-\sqrt{2}) + b = a \cdot (-\sqrt{2}) + b$$

$0 = f(p) = (p(\sqrt{2}), p(-\sqrt{2}))$ であるから、

$$a\sqrt{2} + b = 0 \quad \text{かつ } a \cdot (-\sqrt{2}) + b = 0$$

これがおこるのは $a = 0$ かつ $b = 0$ のときのみである。すなわち、

$$p(X) = (X^2 - 2)q(X) \in (X^2 - 2)\mathbb{R}[X]$$

つまり、

$$\mathrm{Ker}(f) \subset (X^2 - 2)\mathbb{R}[X]$$

がわかった。
以上により、 f は同型 (C) を誘導することがわかる。

問題 12.2. (30 点) $R = \mathbb{F}_{17}[X]/(X^2 + X + 6)$ **において、** 7 **の平方根を二つ求めなさい。すなわち、** X **の** R **でのクラスを** α **とおくとき、**

$$(c_1\alpha + c_2)^2 = 7$$

をみたす $c_1, c_2 \in \mathbb{F}_{17}$ **を二組求めなさい。**

(**答**)

$$\pm(8 - \alpha)$$

実際、 R **において、**

$$\alpha^2 = -\alpha - 6$$

が成り立つことに注意して、 $(8-\alpha)^2$ **を計算すれば** 7 **であることが確かめられる。**

以下は、考え方。

$$(c_1\alpha+c_2)^2 = c_1^2\alpha^2+2c_1c_2\alpha+c_2^2 = c_1^2(-\alpha-6)+2c_1c_2\alpha+c_2^2 = (-c_1^2+2c_1c_2)\alpha+(-6c_1^2+c_2^2)$$

この式が 7 **に等しいための十分条件は**

$$(-c_1^2 + 2c_1c_2) = 0$$
$$-6c_1^2 + c_2^2 = 7$$

である。(必要条件であることも容易にわかるがいまはそれはいわなくてもよい。)

第一式において、

$$c_1(-c_1 + 2c_2) = 0$$

$\mathbb{F}_{17}$ **は体であるから、これが成り立つのは** $c_1 = 0$ **または** $c_1 = 2c_2$ **のいずれかの場合のみである。**

(**ア**) $c_1 = 0$ **の場合**

この場合、 $c_2^2 = 7$ **となるはずであるが、そのような** c_2 **がないことが総当たりにより確かめられる。**

(**イ**) $c_1 = 2c_2$ **の場合**

この式を第二式に代入して

$$11c_2^2 = 7$$

を得る。 11 **と** 17 **とでユークリッドの互除法を用いると、**

$$11 \cdot 14 = 1 \qquad (\text{ in } \mathbb{F}_{17})$$

すなわち、 $\mathbb{F}_{17}$ **における** 11 **の逆元は** 14 **であることがわかる。**

$$c_2^2 = 7 \cdot 14 = 13$$

総当たりにより、これをみたす c_2 **は確かにあって、**

$$c_2 = \pm 8$$

ゆえに、

$$c_1\alpha + c_2 = \pm(8 \cdot 2\alpha + 8) = \pm(8 - \alpha)$$

が答えである。確かめてみるとよい。