環論 期末試験的なレポート問題 (略解)

- 問題は致命的な出題間違いがあった際には予告なく変更される可能性があります。ご注意ください。
- 答えは論理的に、貴方の考えが伝わるように書くこと。数値的な答えだけではほとんど点はありません。

問題 20.1. 次の各々の命題を証明しなさい。

(1) $\mathbb{Z}[\frac{1}{3}] = \{\frac{m}{3^k}; m \in \mathbb{Z}; k \in \mathbb{Z}_{\leq 0}\}$ を示しなさい。(10)

(右辺) は環であって、$\mathbb{Z}$ と $\frac{1}{3}$ は (右辺) の元であるから (左辺) $\subset$ (右辺) である。(生成する環の定義 (定義 2.1))

逆に、$\mathbb{Z}$ の任意の元 m と 0 以上の整数 k に対して、$m\cdot|(\frac{1}{3})^k$ は ((左辺) が環であることから掛け算について閉じているので)(左辺) の元である。

(2) $\mathbb{Z}[X]/(3X-1) \cong \mathbb{Z}[\frac{1}{3}]$ を証明しなさい。(20)

$$\varphi : \mathbb{Z}[X] \to \mathbb{Z}[\frac{1}{3}]$$

を $\varphi(p) = p(\frac{1}{3})$ で定義すれば φ は ($\varphi(\frac{1}{3}) \in \mathbb{Z}[\frac{1}{3}]$ であることが確かめられるから上手く定義されていて、) 環の準同型である (代入原理 (命題 6.7))。(1) をもちいれば、φ は全射であることがわかる ($\varphi(m \cdot X^k) = m \cdot \frac{1}{3^k}$ だから。)

$\mathrm{Ker}(\varphi(p)) = (3X-1)$ を示そう。 「$\supset$」 は明らか。

$$a(X)\sum_{k=0}^{n} a_k X^k \in \ker(\varphi)$$

とすると、$\sum_{k=0}^{n} a_k \frac{1}{3^k} = 0$ で、そこから $a_n \in 3\mathbb{Z}$, $a(X)$ が $3X-1$ で「一回割れる」すなわち

$$b(X) \stackrel{\mathrm{def}}{=} (a(X) - (3X-1)a_n X^{n-1})$$

の次数は $n-2$ 以下 であることがわかり、あとは $a(X)$ の次数に関する帰納法を用いればいい。

[別解] φ　から環準同形

$$f : \mathbb{Z}[X]/(3X-1) \to \mathbb{Z}[1/3]$$

が誘導される。これは全射であることも (1) からすぐにわかる。つぎに

$$g : \mathbb{Z}[1/3] \to \mathbb{Z}[X]/(3X-1)$$

を

$$g(\frac{m}{3^k}) = \overline{mX^k}$$

で定義する。これは上手く定義されている。即ち

$$\frac{m_1}{3^{k_1}} = \frac{m_2}{3^{k_2}} \quad \Longrightarrow \quad \overline{m_1 X^{k_1}} = \overline{m_2 X^{k_2}}$$

である。対称性から $k_1 \geq k_2$ と仮定して良いからそうすると、

$$\frac{m_1}{3^{k_1}} = \frac{m_2}{3^{k_2}}$$

から、

$$m_1 = m_2 \cdot 3^{k_2 - k_1}$$

がわかり、

$$m_1 X^{k_1} = m_2 \cdot 3^{k_2-k_1} X^{k_2} = m_2 \cdot (3X)^{k_2-k_1} X^{k_1}$$

がわかり、

$$\overline{m_1X^{k_1}} == \overline{m_2}\cdot\overline{(3X)}^{k_2-k_1}\overline{X^{k_1}} = \overline{m_2}\cdot\overline{1}^{k_2-k_1}\overline{X^{k_1}} = \overline{m_2}\cdot\overline{X^{k_1}} = \overline{m_2X^{k_2}}$$

だからである。

[g は環準同型である。手順は定石通りだから省略する。]

$g\circ f = \mathrm{id}$. これも容易。とくに f は単射である。

(3) $\mathbb{Z}[\frac{1}{3}]$ から $\mathbb{Z}/5\mathbb{Z}$ への環準同型がちょうど一つ存在することを示せ。(20)

一意性: $\mathbb{Z}[\frac{1}{3}]$ から $\mathbb{Z}/5\mathbb{Z}$ への環準同型のひとつを ψ とする。$\psi(\frac{1}{3}) = 2$ でなければならない。

(存在)

$$\Psi : \mathbb{Z}[X] \to \mathbb{Z}/5\mathbb{Z}$$

を $\Psi(p) = p(2)$ で定めれば Ψ は上手く定義されて、$\mathrm{Ker}(\Psi) \in 3X-1$ がわかるから、環の準同型定理により、環準同型 $\mathbb{Z}[\frac{1}{3}] \to \mathbb{Z}/5\mathbb{Z}$ の存在がわかる。

問題 20.2. 環の同型 $\mathbb{Q}[X]/(X^2-6) \cong \mathbb{Q}[\sqrt{6}]$ がなりたつこと、両辺は体であることを示しなさい。次のことを示すことが重要である。

- X^2-6 は $\mathbb{Q}[X]$ の既約元であること。
- 左辺の 0 でない元が 可逆であること。

[Hint]: 本問の前半についてはつぎのような手順でやればいいだろう。(絶対にこのとおりにやらなければいけないという意味ではない。)

(1) 写像 $\varphi : \mathbb{Q}[X] \to \mathbb{C}$ を $\varphi(p(X)) = p(\sqrt{6})$ で定義すれば φ は環準同型である。(10)

(2) $X^2-6 \in \mathrm{Ker}(\varphi)$.(10) $\varphi(X^2-6) = \sqrt{6}^2 - 6 = 0$ だからである。$(X^2-6) \supset \mathrm{Ker}(\varphi)$. を示そう。(これは Hint には入れていなかったが本題の証明のためにはぜひとも必要なことである。) ($\mathbb{Q}[X]$ は ED だから PID. (ゆえに UFD でもある。) (2) により、$\mathrm{Ker}(\varphi) = (a(X))$ となる $a(X) \in \mathbb{Q}[X]$ が存在するが、下の (4) により (X^2-6) は $\mathbb{Q}[X]$ の元として既約であるから、$a(X)$ と X^2-6 とは同伴であるほかはない。

(3) X^2-6 は $\mathbb{Q}[X]$ 上既約 (※ 20) X^2-6 は $\mathbb{Z}$ 上既約であることと、ガウスの補題をもちいる。

(4) 本講義の諸定理のうち、本題にもっとも有用な一つを高らかに唱えて... 環の準同型定理により、(10)

$$\mathbb{Q}[X]/(X^2-6) \cong \mathbb{Q}[\sqrt{6}]$$

$\mathbb{Q}[X]/(X^2-6)$ の 0 でない元 β をとる。β はある $c(X) \in \mathbb{Q}[X]$ のクラスである。$c(X)$ は X^2-6 で割り切れず、X^2-6 は $\mathbb{Q}[X]$ のなかで既約であるから、互除法により、

$$c(X)l(X) + (X^2-6)\cdot m(X) = 1$$

をみたす $l, m \in \mathbb{Q}[X]$ が存在する。$l(X)$ のクラスが $c(X)$ のクラスの逆元である。(20) □