Algebra-A Final Exam: 2008.1.28 (過)

自己責任で使うこと!

1

[1] $\mathbb{R}[X]$ の素 ideal を全て求めよ.

$\mathbb{R}[X]$: PID ゆえ 任意のイデアルは $(f(X))$ とかける $(f \in \mathbb{R}[X])$

$(f(x))$ が素 ideal $\underset{\text{iff (必要十分)}}{\Longleftrightarrow}$ $f(x)$ が素元.

$\downarrow$

$\mathbb{R}[X]$ は PID ゆえ UFD. つまりこれは f が既約元であることに同値

$\mathbb{R}[X]$ の既約元は 1次式 or 実根をもたない2次式 i.e.

$$(0),\ (X-a)\ (a \in \mathbb{R}),\ (X^2+bX+c)\ \left(\begin{matrix} b, c \in \mathbb{R} \\ b^2-4c<0 \end{matrix}\right)$$

の3つ.

[2] (1) $\phi_{\mathbb{R}} : \mathbb{R}[X] \longrightarrow \mathbb{C}$: hom に対し. $\operatorname{Ker}\phi_{\mathbb{R}} = ?$

$f(x) \longmapsto f(\sqrt{-3})$

$\sqrt{-3}$ は $X^2+3 \in \mathbb{R}[X]$ の根なので $(X^2+3) \subset \operatorname{Ker}\phi_{\mathbb{R}}$

$(X^2+3) \supset \operatorname{Ker}\phi_{\mathbb{R}}$ を示す. $(f \in \operatorname{Ker}\phi_{\mathbb{R}}$ とする.$)$ $\mathbb{R}[X]$ の互除法を適用し ($\because$ $\mathbb{R}$は体)

$$f(x) = (X^2+3)\,g(x) + r(x)$$

$$g(x), r(x) \in \mathbb{R}[X].\quad \deg r(x) \leq 1.$$

がわかる. 今 $f(\sqrt{-3}) = 0$ を仮定していたので $r(\sqrt{-3}) = 0$

となるが. $\deg r(x) \leq 1$ から $r(X) = 0$ がわかる.

$$\therefore\ f(x) = (X^2+3)\,g(x) \quad \text{ゆえ.} \quad f(x) \in (X^2+3).$$

$$\therefore\ \operatorname{Ker}\phi_{\mathbb{R}} = (X^2+3)$$

(2) ((1) と違い, $\mathbb{Z}[X]$ では互除法が使えない.)

$\phi_{\mathbb{Z}} : \mathbb{Z}[X] \longrightarrow \mathbb{C}$: hom に対し. $\operatorname{Ker}\phi_{\mathbb{Z}} = ?$

$f(x) \longmapsto f(\sqrt{-3})$

$(X^2+3) \subset \operatorname{Ker}\phi_{\mathbb{Z}}$ は OK. 逆を示す. $f \in \operatorname{Ker}\phi_{\mathbb{Z}}$ とする.

(1) より. $f(x) = (X^2+3)\,g(x)$, $g(x) \in \mathbb{R}[X]$

は分かっていたから. 後は $g(x) \in \mathbb{Z}[X]$ を示せば OK.

$g(X)$ の deg に関する帰納法で示す.

- $\deg g(X) = 0$ のときは $g(X) = c \in \mathbb{R}$ と書けば

$f(X) = (X^2+3) \cdot c = cX^2 + 3c$, 仮定より $f(X) \in \mathbb{Z}[X]$

ゆえ. $c \in \mathbb{Z}$ とならなければならない. $\therefore g(X) \in \mathbb{Z}[X]$.

- ($\deg g(X) \leq n-1$ までOKと仮定. $\deg g(X) = n$ を示す.)

$\deg g(X) = n$ とすると. $g(X) = \sum_{k=0}^{n} a_k X^k$ とかけるが.

$f(X) = (X^2+3)g(X)$ より f の最高次の項は $\underline{a_n X^{n+2}}$ で

$a_n \in \mathbb{Z}$ がわかる. よって.

$$f(X) - a_n X^n (X^2+3) \in \mathbb{Z}[X].$$

で. かつ.

$$f(X) - a_n X^n (X^2+3) = (X^2+3) \sum_{k=0}^{n-1} a_k X^k$$

と書け. 帰納法の仮定より $a_k \in \mathbb{Z}$ $(0 \leq k \leq n-1)$ だから.

$g(X) \in \mathbb{Z}[X]$ が分かる. $\therefore f(X) \in (X^2+3)$

$$\therefore \quad \underline{\operatorname{Ker}\phi_{\mathbb{Z}} = (X^2+3)} \quad \text{となる.}$$

[3] (1) $(X^2+3, Y) \subset \mathbb{R}[X, Y, Z]$ は素ideal?

準同型 $h: \mathbb{R}[X,Y,Z] \longrightarrow \mathbb{C}[Z]$ を考えてみると.

$$f(X,Y,Z) \longmapsto f(\sqrt{-3}, 0, Z)$$

これは [2] の $\phi_{\mathbb{R}}$ が引き起こす準同型.

$$h_2: \mathbb{R}[X,Y,Z] \longrightarrow \mathbb{C}[Y,Z]$$

$$\underbrace{\mathbb{R}[X][Y,Z]}$$ とみなす.

と. 準同型

$$h_1: \mathbb{C}[Y,Z] \longrightarrow \mathbb{C}[Z]$$

$$f(Y,Z) \longmapsto f(0,Z).$$

の合成とみなせる. $\operatorname{Ker}\phi_{\mathbb{R}} = (X^2+3)$ を使えば.

$$\operatorname{Ker} h = h_2^{-1}(\operatorname{Ker} h_1) = h_2^{-1}((Y)) = (X^2+3, Y).$$

準同型定理より. $\mathbb{R}[X,Y,Z]/\mathrm{Ker}\,h \cong \mathrm{Im}\,h$.

つまり. $\mathbb{R}[X,Y,Z]/(X^2+3,Y) \cong \mathrm{Im}\,h \subseteq \mathbb{C}[Z]$ となり.

$\mathbb{C}[Z]$ は整域ゆえその部分環 $\mathrm{Im}\,h$ (つまり $\mathbb{R}[X,Y,Z]/(X^2+3,Y)$)

も整域. よって $\underline{(X^2+3,Y)\text{ は素 ideal}}$.

(2). $(X^2+3,Y) \subset$? $\subset \mathbb{R}[X,Y,Z]$

極大 ideal ?

$\mathrm{Im}\,\phi_{\mathbb{R}} = \mathbb{R}[\sqrt{-3}] = \mathbb{C}$ に注意すると.

$$\mathrm{Im}\,h = h_1(\mathrm{Im}\,h_2) = h_1(\mathbb{C}[Y,Z]) = \mathbb{C}[Z].$$

実はぴったり一致

そこで. h に更に次の写像 $\hat{h}$ を合成させてみる:

$$\begin{array}{cccc} \hat{h}: & \mathbb{C}[Z] & \longrightarrow & \mathbb{C} \\ & f(Z) & \longmapsto & f(0) \end{array}$$

(つまり. $\hat{h}\circ h$: $\mathbb{R}[X,Y,Z] \longrightarrow \mathbb{C}$ とうつる
これを φ とかくことにする)

$$\mathrm{Im}\,\varphi = \hat{h}(\mathrm{Im}\,h) = \hat{h}(\mathbb{C}[Z]) = \mathbb{C}$$

$$\mathrm{Ker}\,\varphi = h^{-1}(\mathrm{Ker}\,\hat{h}) = h^{-1}((Z)) = (X^2+3,Y,Z).$$

(1) と同様に準同型定理を使うと.

$$\mathbb{R}[X,Y,Z]/(X^2+3,Y,Z) \cong \mathbb{C}$$

$\mathbb{C}$ は体だから. $\underline{(X^2+3,Y,Z)}$ は極大 ideal であり.

しかも (X^2+3,Y) を含む. //

[4]　hom: $M_n(\mathbb{R}) \longrightarrow \mathbb{R}$ は？　④

上を ϕ とおく．$\mathrm{Ker}\,\phi \subset M_n(\mathbb{R})$ は両側 ideal ゆえ

$\mathrm{Ker}\,\phi = \{0\}$ or $M_n(\mathbb{R})$ となる（← 演習でやったはず）

しかし．$\mathrm{Ker}\,\phi = \{0\}$ とすると．準同型定理より．

$$\underbrace{M_n(\mathbb{R})}_{\text{非可換環}} = M_n(\mathbb{R})/\{0\} \cong \mathrm{Im}\,\phi \subseteq \underbrace{\mathbb{R}}_{\text{可換環}}.$$

$M_n(\mathbb{R})$ は非可換で．これと同型な $\mathrm{Im}\,\phi$ は $\mathbb{R}$ の部分環ゆえ

可換となり矛盾．　∴ ϕ は零写像 1つのみ．//

[5]．(1) $\mathbb{Z}/125\mathbb{Z}$，$\mathbb{Z}/1000\mathbb{Z}$ の巾零元の個数は？

(2) $n \in \mathbb{N} \longrightarrow n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ とかくと．（素因数分解）

$\mathbb{Z}/n\mathbb{Z}$ の巾零元の個数は？

先に(2)からやった方が早い：

(2)　$m + n\mathbb{Z} \ (\in \mathbb{Z}/n\mathbb{Z})$ が巾零 $\overset{\text{iff}}{\Longleftrightarrow}$ （n が m のある巾を割り切る）

つまり．m の素因数が n の素因数を全て含むことが必要十分．

∴　$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ と書けているのなら．$\mathbb{Z}/n\mathbb{Z}$ の

巾零元は $p_1 p_2 \cdots p_r$ の倍数の個数だけある．

$$\therefore \quad n/p_1p_2\cdots p_r = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}/p_1p_2\cdots p_r = \underline{p_1^{m_1-1} p_2^{m_2-1} \cdots p_r^{m_r-1}\text{（個）}}\,//$$

(1)　(2)の結果に代入すればおしまい．$125 = 5^3$．$1000 = 2^3 5^3$．

∴　$\mathbb{Z}/125 \leadsto 5^2 = \underline{25\text{個}}$ //

$\mathbb{Z}/1000\mathbb{Z} \leadsto 2^2 \cdot 5^2 = \underline{100\text{ 個}}$ //

[6] (1) $\mathbb{Q}[[X]]$ の単元群 $\mathbb{Q}[[X]]^{\times} = ?$

$f(x) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}[[X]]$ と書いたとき

$a_n \neq 0$ なら、$f(x)$ に対し、$\begin{cases} g(x) = \sum_{n=0}^{\infty} b_n X^n \in \mathbb{Q}[[X]] \\ b_0 = a_0^{-1},\ b_n = a_0^{-1} \sum_{k=0}^{n-1} a_{n-k} b_k \end{cases}$

と $g(x)$ を定めれば $f(x)g(x) = 1$ がわかる (check!)

$a_n = 0$ なら、${}^{\forall} g(x) \in \mathbb{Q}[[X]]$ に対し、$f(x)g(x)$ の定数項は 0 。つまり、$f(x)g(x) = 1$ とは絶対にならない。

以上より、

$$\mathbb{Q}[[X]]^{\times} = \{ f(x) \in \mathbb{Q}[[X]] \text{ で定数項が } 0 \text{ でない} \}$$
$$= \left\{ f(x) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}[[X]] \,\middle|\, a_0 \neq 0 \ (\text{or } a_0 \in \mathbb{Q}^{\times}) \right\}$$

ちょっと難?

(2) $\mathbb{Q}[[X]]$ の ideal は? また素 ideal は?

$f(x) \neq 0 \ (\in \mathbb{Q}[[X]])$ とし、$f(x) = \sum_{n=N}^{\infty} a_n X^n \ (a_N \neq 0)$ と書けているとき、$\nu(f) := N$ で定義することにする。

注意

$(0) \neq \mathfrak{a} \subset \mathbb{Q}[[X]]$: ideal をとると、かならず

$$N := \min\{ \nu(f) \mid f(x) \neq 0,\ f \in \mathfrak{a} \}$$

が1通りに定まる。この定義から $\mathfrak{a} \subset (X^N)$ は明らか。

逆 ($\mathfrak{a} \supset (X^N)$) を示す。今 $f(x) \in \mathfrak{a}$ で $\nu(f) = N$ だとすると、$f(x) = X^N g(x)$ となる $g(x) \in \mathbb{Q}[[X]]$ が存在し、$g(x) \in \mathbb{Q}[[X]]^{\times}$ となる。($\because$ $g(x)$ の定数項 $\neq 0$)

$\therefore$ $(X^N) = (f(x))$ となり、$f \in \mathfrak{a}$ ゆえ $(f(x)) \subset \mathfrak{a}$。

$\therefore$ $(X^N) \subset \mathfrak{a}$ となり、$(X^N) = \mathfrak{a}$ がわかる。

よって、$\mathbb{Q}[[X]]$ の ideal は (0), (X^N) ($N \geq 0$, $N \in \mathbb{Z}$) //

$\mathbb{Q}[[X]]$ はPID ゆえ素 ideal は (0) と (X) の2つだけ //

極大ideal

[7]　$\mathbb{Z}[i]$ で次を既約分解　(1) $1-3i$　(2) 10　(3) $6+9i$

☆ $N(z)=p$ (素数) ならば z は $\mathbb{Z}[i]$ で既約.

(1) $1-3i = -\underline{(1+i)(1+2i)}$ //　(ノルムをとってcheckすること!)

(2) $10 = \underline{(1+i)(1-i)(1+2i)(1-2i)}$ //

(3) $6+9i = \underline{3(2+3i)}$ //

↑(これは $N(2+3i)=13$: 素数. OK.
3 は $(a+bi)(c+di)$ に分けてノルムをとる)

[8]. ○× questions

(1) 体の元はすべて乗法についての可逆元 … $\underline{\times}$ //
(反例 : 0 は可逆でない).

(2) $C^\infty(\mathbb{R})$ は加法 $(f+g)(x) := f(x)+g(x)$ と乗法
$(f\cdot g)(x) = g(f(x))$ で環になる …… $\underline{\times}$ //　(分配律がダメ)

(3) $M_2(\mathbb{R})$ の両側idealは (0) と $M_2(\mathbb{R})$ のみ … $\underline{○}$ //

(4) 環のhom : $f: A \longrightarrow B$ に対し. $\mathrm{Im} f$ はBのideal … $\underline{\times}$ //

(5) 〃　$\mathrm{Ker} f$ はAのideal … $\underline{○}$ //

(6) $f(x) \in \mathbb{Q}[X]$ に対し. $\mathbb{Q}[X]/(f(x))$ が体 $\Longrightarrow$ $\mathbb{R}[X]/(f(x))$ も体.
… $\underline{\times}$ //　(反例 : $\mathbb{Q}[X]/(X^2-2)$ は体 but.
$\mathbb{R}[X]/(X^2-2) \cong \mathbb{R}[X]/(X-\sqrt{2}) \times \mathbb{R}[X]/(X+\sqrt{2}) \cong \underline{\mathbb{R}\times\mathbb{R}}$).
↑
これは体ではない
(ちなみに整域でもない)

(7) 整域の商環は整域 … $\underline{\times}$ //
(反例 : $\mathbb{Z}$ は整域 but. $\mathbb{Z}/6\mathbb{Z}$ は整域でない $(\bar{2}\cdot\bar{3}=\bar{0})$)

(8) $\mathbb{Q}[X]$ はPID … $\underline{○}$ //

(9) 整域Rの素元 $\Longrightarrow$ 既約元 … $\underline{○}$ //
(注 : 逆は一般に不成立. UFDなど条件が必要).

(10) 非可換環 $\Longrightarrow$ 整域でない … $\underline{○}$ //
↑
(これは可換を仮定していた)

update : 2009. 1. 28