

代数学演習 I 問題 NO.7

《イデアルの生成元》・素イデアル・極大イデアル編

定義 7.1. R を環、 I をそのイデアル、 S を R の部分集合とします。 I が S で(イデアルとして)生成されるとは、次の二条件を満たすときに言います。

- (1) I は S を部分集合として含む。
- (2) I は、 S を部分集合として含むイデアルの中で最小のものである。すなわち、 S を含む R の任意のイデアル J に対し、 $I \subset J$ が成り立つ。

S が有限集合 $S = \{x_1, \dots, x_n\}$ のとき、 S で生成されるイデアルを普通 (x_1, \dots, x_n) と丸括弧を用いて書きます。

例題 7.1. $\{9, 12\}$ で生成される \mathbb{Z} のイデアル $I = (9, 12)$ を求めよ。

解答 I は引き算について閉じているから、

$$I \ni 12 - 9 = 3.$$

さらに、 I は \mathbb{Z} による掛け算により閉じているから、

$$3\mathbb{Z} \subset I.$$

ところが、 $3\mathbb{Z}$ は $\{9, 12\}$ を含む \mathbb{Z} のイデアルであるから、 I の最小性により、

$$I \subset 3\mathbb{Z}$$

以上により、 $I = 3\mathbb{Z}$ が分かった。 $(I = (3))$ と書いても良い。次の問題も参照)

問題 7.1. R を環、 S をその部分集合とします。この時 S で生成される R のイデアル I がただひとつ存在することを次の順序で示しなさい。

- (1) (一意性) I, J がともに S で生成される R のイデアル(すなわち定義 7.1 の (1),(2) を満たす)ならば、 I, J 両方の最小性を用いて、 $I = J$ が分かる。
- (2) (存在 I) S を含む R のイデアルは一つは必ず存在することを示しなさい。
- (3) (存在 II) S を含む R のイデアルの全体を $\{I_\lambda\}_{\lambda \in \Lambda}$ とすると、それらすべての共通部分

$$I_0 = \bigcap_{\lambda \in \Lambda} I_\lambda$$

も R のイデアルで、かつ S を含むことを示しなさい。

- (4) (存在 III) 上の I_0 が S を含む最小のイデアルであることを示しなさい。

問題 7.2. 次の \mathbb{Z} のイデアルを簡単な形になおしなさい。

- (1) $I_1 = (4, 6)$
- (2) $I_2 = (12, 18, 30)$
- (3) $I_3 = (78, 54, 62)$

問題 7.3. 次の $\mathbb{C}[X]$ のイデアルを簡単な形になおしなさい。

- (1) $I_1 = (X^3, X^2)$
- (2) $I_2 = (X^3 - 1, X^2 - 1)$
- (3) $I_3 = (X(X - 1), (X + 1)(X - 1), X(X + 1))$

定義 7.2. R を単位元を持つ可換環、 I をそのイデアルとします。このとき、

- (1) I が R の素イデアルであるというのは、「 $f, g \in A, fg \in I$ ならば、 f か g の一方が I の元である」が成り立つときに言います。
- (2) I が R の極大イデアルであると言うのは、 I を部分集合として含む R のイデアルが R と I 自身以外には存在しないときに言います。

問題 7.4~7.18 では、「環」といえば単位元を持つ可換環を指すことにします。

問題 7.4. 環 R のイデアル I が素イデアルであるための必要十分条件は、 R/I が整域であることなのを示しなさい。

問題 7.5. \mathbb{Z} のイデアル $n\mathbb{Z}$ が素イデアルになるのは、 $n = 0$ 又は n が素数のときであることを示しなさい。

問題 7.6. 環 R のイデアル I 、 R の要素 h が、 $Rh + I = R$ を満たすならば、 h の剰余類 \bar{h} は R/I の可逆元であることを示しなさい。

問題 7.7. 環 R の極大イデアル I が与えられたとき、 R/I は体であることを、次の順序で示しなさい。

- (1) R の任意の元 h に対して、 $Rh + I$ は I を部分集合として含むイデアルである。
- (2) $Rh + I = I \Leftrightarrow h \in I$.
- (3) R/I において、 $\bar{h} \neq 0$ ならば \bar{h} は R/I の可逆元である。

問題 7.8. 極大イデアルは素イデアルであることを示しなさい。

問題 7.9. (1) \mathbb{Z} のイデアル $n\mathbb{Z}, m\mathbb{Z}$ (n, m は正の整数) について、

$$n\mathbb{Z} \cap m\mathbb{Z} \Leftrightarrow n \text{ は } m \text{ の倍数である}$$

を示しなさい。

- (2) \mathbb{Z} の極大イデアルをすべて求めなさい。

問題 7.10. $\mathbb{Z}[X]$ のイデアル $I = (X)$ は素イデアルであって、極大イデアルではないことを示しなさい。

問題 7.11. 次の $\mathbb{Z}[\sqrt{2}]$ のイデアルは素イデアルかどうか答えなさい。

- (1) $I_1 = (5)$
- (2) $I_2 = (7)$

問題 7.12. 環の間の準同型写像 $f: R \rightarrow S$ が与えられたとします。この時 I が S の素イデアルなら、 $f^{-1}(I)$ は R の素イデアルであることを示しなさい。

問題 7.13. 次の条件を満足する f, R, S, I を見つけなさい。

- (1) $f: R \rightarrow S$ は環の間の準同型写像。
- (2) I は S の極大イデアル。
- (3) $f^{-1}(I)$ は R の極大イデアルでない。

(ヒント: 0 は体の極大イデアルです。)

問題 7.14. $R = \mathbb{Z}/6\mathbb{Z}$ 上の多項式環 $R[X]$ の元 f, g で、次の2条件を同時に満足するものを作りなさい。

- (1) $\deg(f) = \deg(g) = 2$.
 (2) $\deg(fg) = 3 (< \deg(f) + \deg(g))$.

問題 7.15. R を環、 I をそのイデアルとします。《 R/I のイデアル》全体と《 I を部分集合として含む R のイデアル》全体との間には一対一対応がつくことを次のようにして示しなさい。

- (1) J を I を含む R のイデアルとするとき、

$$\bar{J} = \{\bar{x}; x \in J\} \quad (\bar{} \text{ は } ? \text{ のクラスを表す。})$$

は R/I のイデアルである。

- (2) K を R/J のイデアルとするとき、

$$\hat{K} = \{x \in R; \bar{x} \in K\}$$

は R のイデアルである。

- (3) 上の二つの対応は互いに他の逆対応になっている。すなわち、

$$\hat{\bar{J}} = J, \quad \bar{\hat{K}} = K.$$

問題 7.16. $\mathbb{C}[X]$ のイデアル I は必ずある一つの元 f で生成される ($\exists f; I = (f)$) ことを示しなさい。(ヒント: f として $I \setminus \{0\}$ の元のうち次数が最小のものをとる。)

問題 7.17. 複素数を係数に持つ多項式 $f(X) (\neq 0)$ は必ず複素数の範囲で根を持つことを用いて、 $\mathbb{C}[X]$ の素イデアルをすべて求めよ。

問題 7.18. p を素数とするとき、 $(\mathbb{Z}/p\mathbb{Z})[X]$ の元の間次の関係式を証明しなさい。

$$(X+1)^p = X^p + 1$$

問題 7.19. (1) $V = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ は体 $K = \mathbb{Z}/3\mathbb{Z}$ 上のベクトル空間であることを示しなさい。次元はいくらですか。

- (2) V の部分群は全て V の部分ベクトル空間であることを示しなさい。

- (3) V の部分群をすべて求め、それらの (K -ベクトル空間としての) 次元を求めなさい。

問題 7.20. 可換環 R 上の任意の m, n -行列 A と n, m 行列 B とにたいして、

$$\text{tr}(AB) = \text{tr}(BA)$$

が成り立つことを示しなさい。

以下の問題はかなり難しく、また後の知識が必要になる所もあるが、あえて付け加えておいた。理論の流れが掴めればよい。

問題 7.21. 環 R 上の任意の n 次正方行列 A, B にたいして、

$$(\star) \quad \det(AB) = \det(A) \det(B)$$

が成り立つのを示そう。ただし、 R が体のときに (\star) 式がなりたつのは既知とする。以下の細部を埋めなさい。

- (1) $R_0 = \mathbb{Z}[X_{11}, X_{12}, \dots, X_{nn}, Y_{11}, Y_{12}, \dots, Y_{nn}]$ を \mathbb{Z} に $2n^2$ 個の変数を付け加えてできた環とし、 $K = Q(R_0)$ (R_0 の商体) とするとき、 K 上では (\star) がなりたつから、 $A = A_X = (X_{ij}), B = B_Y = (Y_{ij})$ という変数を成分にした行列について (\star) は K の元として等しい。

- (2) $R_0 \subset K$. ゆえに、上の (★) は $A = A_X, B = B_Y$ について R_0 の元としても等しい。
 (3) 代入原理により、(★) は 任意の環 R 上正しい。

(★) 式を一から証明するには、行列式を「多重線形かつ交代的な (スカラー倍を除いて) 唯一のモノ)」として 特徴づける のがもっとも自然であろう。線形代数の教科書を参照のこと。

問題 7.22. 体 K 上の行列 $A \in M_n(K)$ をとって、その固有多項式を $\Phi_A(X) (= \det(X \cdot 1_n - A))$ とします。この時、 $\Phi_A(A) = 0$ が成り立つこと (ケーリー-ハミルトンの定理) を次の順序で示しなさい。

- (1) 以下《行列》が二つの意味で使われてややこしいので $\{A, 1_n\}$ で生成される $M_n(K)$ の部分環を R とおきます。

$$R = \{a_m A^m + a_{m-1} A^{m-1} + \cdots + a_1 A + 1_n; \quad a_m, \dots, a_0 \in K\}.$$

- (2) R は可換環になります。
 (3) R 係数の行列環 $M_n(R)$ を考えます。

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & \cdots & \cdots & a_{3n} \\ a_{41} & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

と成分表示すると、

$$B = \begin{pmatrix} A - a_{11} \cdot 1_n & -a_{12} \cdot 1_n & \cdots & -a_{1n} \cdot 1_n \\ -a_{21} \cdot 1_n & A - a_{22} \cdot 1_n & \cdots & -a_{2n} \cdot 1_n \\ -a_{31} \cdot 1_n & \cdots & \cdots & -a_{3n} \cdot 1_n \\ -a_{41} \cdot 1_n & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n1} \cdot 1_n & -a_{n2} \cdot 1_n & \cdots & A - a_{nn} \cdot 1_n \end{pmatrix}$$

は $M_n(R)$ の元で、 $\text{Det}(B) = \Phi_A(A)$. (ただし、ここで、 $\text{Det}(B) \in R$ は B の $M_n(R)$ の元としての行列式。)

- (4) e_1, \dots, e_n を K^n の基本ベクトルとすると、

$$B \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

- (5) C を B の ($M_n(R)$ の元としての) 余因子行列とすると、
 $CB = \text{Det}(B)E_R$ (ここに E_R は $M_n(R)$ の単位元 (単位行列))
 (6) $\text{Det}(B)e_i = 0 (i = 1, 2, 3, \dots, n)$. ゆえに、 $\text{Det}(B) = 0$.