代数学演習 IB 問題 NO.3

$\boxed{\text{イデアルの定義、「生成するイデアル」編}}$

定義 3.1. 環 R の部分集合が R の**イデアル**であるとは、

(1) I は $(R,+)$ の部分加群である。
(2) $r \in R, a \in I \implies ra \in I, ar \in I$

の二条件が成り立つときに言います。

問題 3.1. 環 R の部分集合 $\{0\}$ は R のイデアルであることを示しなさい。(通常 $\{0\}$ を単に 0 であらわします。)

問題 3.2. (各 1) 次の各 R, I の組合せにおいて、「I は環 R のイデアルである」といえるだろうか？理由をあげて答えなさい。

(1) $R = \mathbb{N}$, $I = 0$.
(2) $R = \mathbb{Z}$, $I = 2\mathbb{Z} + 1$.
(3) $R = \mathbb{Z}$, $I = \mathbb{N}$.
(4) $R = \mathbb{R}$, $I = 2\mathbb{Z}$.
(5) $R = \mathbb{C}$, $I = \mathbb{R}$.
(6) $R = \mathbb{C}[X]$, $I = \mathbb{C}$.
(7) $R = \mathbb{Z}$, $I =$(素数の全体).

定義 3.2. 環 R の部分集合 A, B にたいして、

(1) $A + B = \{a + b; a \in A, b \in B\}$.
(2) $A \underset{\text{(set)}}{\cdot} B = \{ab; a \in A, b \in B\}$.

と定義します。他に紛れがない時には、$A \underset{\text{(set)}}{\cdot} B = \{ab; a \in A, b \in B\}$ のことを単に AB とも書きます。

問題 3.3. I, J が環 R のイデアルならば、$I \cap J$ も R のイデアルであることを示しなさい。

問題 3.4. I, J が環 R のイデアルならば、$I \cup J$ も R のイデアルであるといえるだろうか。

問題 3.5. I, J が環 R のイデアルならば、

$$I + J = \{a + b; \quad a \in I, b \in J\}$$

も R のイデアルであることを示しなさい。

問題 3.6. $\mathbb{Z}[X]$ の部分集合

$$I = \{f \in \mathbb{Z}[X]; f \text{ の定数項は } 2 \text{ の倍数 }\}$$

は $\mathbb{Z}[X]$ のイデアルだろうか？

問題 3.7. $\mathbb{Z}[X]$ の部分集合 S であって、和、積について閉じているにも関わらず、$\mathbb{Z}[X]$ のイデアルでないものの例を挙げなさい。

問題 3.8. $\mathbb{Z}[X]$ の部分集合

$$J = \{f \in \mathbb{Z}[X]; f(0) \in 3\mathbb{Z} \text{ and } f'(0) \in 3\mathbb{Z}\}$$

は $\mathbb{Z}[X]$ のイデアルだろうか？

問題 3.9. I, J が可換環 R のイデアルであるにもかかわらず

$$I \underset{(\mathrm{set})}{\cdot} J = \{ab; a \in I, b \in J\}$$

(I と J の R の部分集合としての積) が R のイデアルにならないような例を具体的にあげなさい。

問題 3.10. I, J が可換環 R のイデアルならば、

$$IJ = \{\sum_i a_i b_i (\text{有限和}); a_i \in I, b_i \in J\} \quad (\text{注意})$$

も R のイデアルとなることを示しなさい。(IJ のことを I と J の**イデアルとしての積**と呼ぶ。

問題 3.11. 可換環 R の巾零元全体

$$P = \{x \in R; x^n = 0 (\exists n \in \mathbb{Z}_{>0})\}$$

は R のイデアルとなることを示しなさい。

定義 3.3. 単位元を持つ可換環 R 上の一変数多項式とは、

$$a_n X^n + a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + \cdots + a_1 X + a_0 \quad (a_n, \ldots, a_0 \in R)$$

のように表されるもののことです。R 上の一変数多項式の全体は環をなします。これを R 上の一変数多項式環と言って、$R[X]$ であらわします。以下面倒なので《一変数多項式》が出てくる問題では、R は単位元を持つ可換環であると仮定していることにします。

問題 3.12. (単位元を持つ可換) 環 R 上の一変数多項式 $f(X)$ と R の元 a について、$f(a) = 0$ ならば、

$$f(X) = (X - a) g(X) \quad g(X) \in R[X]$$

とあらわせることを示しなさい。

定義 3.4. 環 R の元 a は、

$$ab = 0$$

なる $b (\neq 0) \in R$ が存在するとき、**左零因子**と呼ばれます。**右零因子**も同様に定義されます。可換環では、左右の区別がいらないので、単に**零因子**と呼びます。零因子が 0 しかない可換環を**整域**と呼びます。

問題 3.13. 整域 R 上の 一変数多項式 $f(X)$ は、R に高々 d 個しか根を持たないことを示しなさい。

問題 3.14. 可換環 R 上の一変数多項式 $f(X)$ の係数のうちに非零因子があれば、$f(X)$ は $R[X]$ の非零因子となることを示しなさい。

問題 3.15. 有理数体 $\mathbb{Q}$ 上の二変数多項式環 $\mathbb{Q}[X, Y]$ のイデアル I が $X + Y(X+1), Y, X^2$ を元として含む時、I は X, Y も元として含むことを示しなさい。

問題 3.16. (各 1) 有理数体 $\mathbb{Q}$ 上の二変数多項式環 $\mathbb{Q}[X, Y]$ のイデアル J が $X + Y, X + Y^2, X + Y^3, X + Y^4, X + Y^5$ を元として含む時、

(1) J は $X + Y, Y^2 - Y$ を元として含むことを示しなさい。
(2) $X + Y, Y^2 - Y$ を元として含むような $\mathbb{Q}[X, Y]$ のイデアルは必ず J を部分集合として含むことを示しなさい。

定義 3.5. 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 $S = \{x_1, \ldots, x_n\}$ のとき、S で生成されるイデアルを普通 $(x_1, \ldots, x_n)$ と丸括弧を用いて書きます。

例題 3.1. $\{9, 12\}$ 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 3.17. (各 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 3.5 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

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

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 3.18. (各 1) 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 3.19. (各 1) 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) $I_3 = (X(X-1), (X+1)(X-1), X(X+1))$