

1 次の環  $R$  と部分集合  $I$  に対し,  $I$  が  $R$  のイデアルであることを示せ.

$$(1) R = \mathbb{Z}, I = n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$$

$$(2) R = k[x] \text{ (} k \text{ は体)}, I = (f(x)) = \{f(x)g(x) \mid g(x) \in k[x]\} \text{ (} f(x) \in k[x]\text{)}$$

$$(3) R = k[x] \text{ (} k \text{ は体)}, I = \{f(x) \in k[x] \mid f(1) = 0\}$$

(解答)  $I$  が  $R$  のイデアルであることを示すには,

(a)  $I$  が  $R$  の減法について閉じていること, および

(b)  $I$  が  $R$  の元と積をとる操作について閉じていること,

の2つを示せば十分である.

(1) (a)  $a, b \in I$  とする.  $a = nx, b = ny$  を満たす  $x, y \in \mathbb{Z}$  が存在する.  $a - b = nx - ny = n(x - y) \in n\mathbb{Z}$  より,  $a - b$  は  $I$  に含まれる. したがって  $I$  は  $R$  の減法について閉じている.

(b)  $a \in I$  かつ  $b \in R$  ならば,  $ab = (nx)b = n(xb) \in n\mathbb{Z}$  より,  $ab \in I$  を満たす.

したがって  $I$  は  $R$  のイデアルである.

(2) (a)  $g(x), h(x) \in I$  とする.  $I$  の定義より,  $g(x) = f(x)g_0(x)$ ,  $h(x) = f(x)h_0(x)$  を満たす  $g_0(x), h_0(x) \in k[x]$  が存在する.

$$g(x) - h(x) = f(x)g_0(x) - f(x)h_0(x) = f(x)(g_0(x) - h_0(x)) \in I$$

より  $I$  は  $R$  の減法について閉じている.

(b)  $g(x) \in I, h(x) \in R$  とする.  $g(x) = f(x)g_0(x)$  を満たす  $g_0(x) \in R$  が存在する.

$$h(x)g(x) = h(x)f(x)g_0(x) = f(x)(h(x)g_0(x)) \in I.$$

したがって,  $I$  は  $R$  の元との積について閉じている.

したがって  $I$  は  $R$  のイデアルである.

(3) (a)  $f(x), g(x) \in I$  とする. このとき  $I$  の定義より,  $f(1) = g(1) = 0$  となる.  $(f - g)(1) = f(1) - g(1) = 0 - 0 = 0$  より  $f - g \in I$  を得る.

(b)  $f(x) \in I, g(x) \in R$  とする. このとき,  $gf(1) = g(1)f(1) = g(1) \cdot 0 = 0$  より  $gf \in I$  を得る.

したがって  $I$  は  $R$  のイデアルである.

2  $R = k[x, y]$  とする.

$$I = \{f(x, y) \in k[x, y] \mid f(0, 0) = 0\}$$

が  $R$  の単項イデアルでないことを示せ.

(解答)  $f(x, y) = x$  とおくと  $f(0, 0) = 0$  より,  $x \in I$  を得る. 同様に  $g(x, y) = y$  とおくと  $g(0, 0) = 0$  より,  $y \in I$  を得る. もし  $I = (f(x, y))$  となる多項式  $f(x, y) \in k[x, y]$  が存在したと仮定すると,

$$x = f(x, y)p(x, y)$$

を満たす多項式  $p(x, y) \in k[x, y]$  が存在する. 同様に  $y = f(x, y)q(x, y)$  を満たす多項式  $q(x, y) \in k[x, y]$  が存在する. このことは  $x, y$  をともに割り切るような  $f(x, y) \in I$  の存在を意味するが, そのような多項式は定数しか存在しない.  $f(x, y) = c$  ( $c$  は定数) とおくと  $c = f(0, 0) = 0$  となり,  $I = (0)$  となって矛盾が生じる.

3 実数を係数とする 1 変数の多項式環  $R = \mathbb{R}[x]$  とその単項イデアル  $I = (p(x))$  に対し, 剰余環  $R/I$  において次の元  $f(x)$  を計算せよ. (ただし答えは  $p(x)$  の次数未満の多項式としてこたえること.)

(1)  $I = (x^2 + 1)$ ,  $f(x) = (x + 1)(x + 2)$

(2)  $I = (x^2 - x + 1)$ ,  $f(x) = (x + 1)(x + 2)$

(3)  $I = (x^3 - x - 1)$ ,  $f(x) = (x + 1)^9$

(解答) 剰余環  $R/I = R/(p(x))$  において,  $p(x) = 0$  とおいて計算する.

(1)  $p(x) = x^2 + 1 = 0$  より,  $x^2 = -1$ . したがって

$$f(x) = (x+1)(x+2) = x^2 + 3x + 2 = (-1) + 3x + 2 = 3x + 1.$$

(2)  $p(x) = x^2 - x + 1 = 0$  より,  $x^2 = x - 1$ . したがって

$$f(x) = (x+1)(x+2) = x^2 + 3x + 2 = (x-1) + 3x + 2 = 4x + 1.$$

(3)  $p(x) = x^3 - x + 1 = 0$  より,  $x^3 = x - 1$ . したがって

$$(x+1)^3 = x^3 + 3x^2 + 3x + 1 = (x-1) + 3x^2 + 3x + 1 = 3x^2 + 4x = x(3x+4).$$

ゆえに

$$f(x) = (x+1)^9 = ((x+1)^3)^3 = (x(3x+4))^3 = x^3(3x+4)^3.$$

ここで

$$(3x+4)^3 = 27x^3 + 108x^2 + 144x + 64 = 27(x-1) + 108x^2 + 144x + 64 = 108x^2 + 171x + 37.$$

よつて

$$f(x) = x^3(3x+4)^3 = (x-1)(108x^2+171x+37) = 108x^3+63x^2-134x-37.$$

 $x^3 = x - 1$  を代入して

$$f(x) = 108(x - 1) + 63x^2 - 134x - 37 = 63x^2 - 26x - 145.$$

<sup>1</sup>※この講義に関する情報はホームページを参照. <https://hirokazunasu.github.io/2025/alg2.html>