

4 第4回

4.1 環の例

(例1) 整数の集合 $\mathbb{Z}$ は通常の加法、乗法に関して可換環をなす。また乗法に関して単位元 1 をもつ。これを整数環という。

(例2) 整数係数の x の多項式 $a(x)$ の集合は、通常の加法、乗法に関して可換環をなす。乗法に関しての単位元は $a(x) = 1$ である。これを多項式環という。

(例3) $\{0, 1\}$ は次の演算に関して環をなす。

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

または

$\cdot$	0	1
0	0	0
1	0	0

環 R の加法における単位元： 0 ^{ゼロ} で表す。

乗法における単位元 (もしあれば)： 1 ^{イチ} で表す。

乗法単位元を有する環 R において、ある元 $a \in R$ に対し

$a \cdot b = 1$ となる元 b があれば、 b を a の右逆元という。

$b \cdot a = 1$ となる元 b があれば、 b を a の左逆元という。

定理 6 乗法の単位元をもつ環 R について

1. 単位元 1 は唯一である。
2. a が右逆元 b と左逆元 c をもてば、 $b = c$ であり、 a は逆元をもつといい、 a の逆元を a^{-1} で表す。また、逆元は唯一である。
3. $(a^{-1})^{-1} = a$

(証明)

1. 1 と $1'$ を2つの異なる乗法単位元とすると、 $1 \cdot 1' = 1'$ より $1 = 1'$ である。
2. $1 = a \cdot b$ であるので、左から c を乗ずると

$$c \cdot 1 = c \cdot a \cdot b$$

すなわち $c = b$ が得られる。また、

$$a^{-1} = a^{-1} \cdot (a \cdot a'^{-1}) = (a^{-1} \cdot a) \cdot a'^{-1} = a'^{-1}$$

3. $a^{-1} \cdot a = a \cdot a^{-1} = 1$ だから、 a は a^{-1} の逆元である。逆元は唯一なので

$$\frac{(a^{-1})^{-1}}{a^{-1} \text{の逆元}} = a$$

□

逆元をもつ元を単元あるいはユニット (unit) という。 a, b が単元ならば、 $c = a \cdot b$ もまた単元である。なぜなら、 c の逆元は $c^{-1} = b^{-1} \cdot a^{-1}$ であるからである。従って、全ての単元の集合は乗法のもとで閉じている。

定理 7 環 R の乗法のもとで、単元の集合は群をなす。

(証明) $G1$ と $G2$ は $R2$ と $R3$ から自明。 $G3$ は R が乗法の単位元を持たねばならないことから自明。 $G4$ は単元の定義から明らか。□

(例 1) 整数環において ± 1 のみが単元である。

(例 2) 多項式環において $a(x) = \pm 1$ のみが単元である。

(例 3) 実数を要素とする 2×2 行列は、行列の加法、乗法について環をなす。乗法に関する単位元は単位行列である。また、正則行列は単元である。

4.2 イデアル (ideal)

環 R の部分集合 I で、次の 2 つの性質を有するものを (左) イデアルと呼ぶ。

I1 I は R の加法に関して部分群である。

I2 $\forall a \in I, \forall r \in R$ について、 $ra \in I$ である。

(例 1) m を正の整数とする。整数環 $\mathbb{Z}$ において m の倍数全体の集合

$$\{0, \pm m, \pm 2m, \pm 3m, \dots\}$$

はイデアルである。

(例 2) 多項式環において定数項が 0 であるような多項式全体の集合 I はイデアルである。(x の倍数項式全体の集合はイデアルである。)

4.3 整数環とその性質

定理 8 $\forall a, b \in \mathbb{Z}$ に対し

$$b = aq + r, \quad 0 \leq r < |a|$$

となる $\exists q, r \in \mathbb{Z}$ が一意的に定まる。特に、 q を商、 r を剰余という。

(証明)

$$b = aq_1 + r_1, \quad 0 \leq r_1 < |a|$$

$$b = aq_2 + r_2, \quad 0 \leq r_2 < |a|$$

と 2 通りに定まるとすれば、

$$aq_1 + r_1 = aq_2 + r_2$$

$$a(q_1 - q_2) = r_2 - r_1$$

が得られる。ここで、もし $r_2 - r_1 \neq 0$ ならば、 $|r_2 - r_1| < |a|$ から $q_1 - q_2 = 0$ でなければならず、これは $r_2 - r_1 \neq 0$ に矛盾する。従って、 $r_1 = r_2$ かつ $q_1 = q_2$ である。□

以下では、 $b = aq + r$ と書くかわりに、 $r = R_a[b]$ と書くことにする。すなわち、 b を a で割った余りを $R_a[b]$ で表す。

定理 9 (素因数分解の一意性) a を正の整数とし、 $a \neq 1$ とする。このとき、 a は有限個の正の素数の積に一意的に分解される。すなわち

1. a は有限個の素数の積である。
2. m 個の素数 $p_1, p_2, \dots, p_m$ と n 個の素数 $q_1, q_2, \dots, q_n$ について、 $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ ならば $m = n$ であり、しかも $q_1, q_2, \dots, q_m$ の順序を適当に入れ換えれば、 $p_i = q_i$ ($i = 1, 2, \dots, m$) である。

(証明)

1. 帰納法による。 $a = 2$ ならば、2 は素数なので 1 が成り立つ。 $a < n$ のときに 1 が成り立つとし、 $a = n$ のときの成立を示す。 n が素数ならば明らかに 1 が成り立つ。 n が合成数ならば、ある素数 p が存在して、 $n = pn'$ と書ける。このとき、 $n' < n$ なので、帰納法の仮定から n' は有限個の素数の積で書ける。従って 1 がいえた。

2. $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ ($n \geq m$) と2通りに分解されたとする。 p_1 は素数なので p_1 は $q_1 \sim q_n$ のどれかを割り切る。適当に順序を変えて q_1 を割り切るとすると、 p_1 と q_1 は素数なので $p_1 = q_1$ 。

$$a' = p_2 p_3 \cdots p_m = q_2 q_3 \cdots q_n$$

とすると同様にして、適当に順序を変えて、 p_2 は q_2 を割り切り、 p_2 と q_2 は素数なので、 $p_2 = q_2$ 。以下、同様にして、 $p_3 = q_3, \cdots, p_m = q_n$ となり

$$1 = q_{m+1} q_{m+2} \cdots q_n$$

となるので、 $n = m$ でなければならない。

□