2012年6月5日

$\mathbb{Z}/m\mathbb{Z}$ の構成

m を正の整数とし、$a \in \mathbb{Z}$ が m で割り切れるとき $m|a$ と書く。

$$R = \{(a, b) \mid (a, b) \in \mathbb{Z} \times \mathbb{Z},\ m|(a - b)\}$$

とおくと、R は $\mathbb{Z}$ 上の同値関係になる。R による商集合

$$\mathbb{Z}/R = \{[a] \mid a \in \mathbb{Z}\}$$

を $\mathbb{Z}/m\mathbb{Z}$ とも書く。$\mathbb{Z}/m\mathbb{Z}$ に演算 $+$ を次のように定義することができる。

$$+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ +([a], [b]) = [a + b].$$

この写像 $+$ は well-defined である。また、$\mathbb{Z}/m\mathbb{Z}$ に演算 $\times$ を次のように定義することができる。

$$\times : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ \times([a], [b]) = [ab].$$

この写像 $\times$ は well-defined である。

環の定義

集合 A に2つの演算 $+$（加法）, $\times$（乗法）が定義されていて、下記の性質が成り立つとき、A は環 (ring) であるという。

(1) $\forall a, b, c \in A,\ (a + b) + c = a + (b + c)$ （結合法則）

(2) $\forall a, b \in A,\ a + b = b + a$ （交換法則）

(3) $\exists 0 \in A,\ \forall a \in A,\ a + 0 = a$ （零元の存在）

(4) $\forall a \in A,\ \exists b \in A,\ a + b = 0$ （加法に関する逆元の存在）

(5) $\forall a, b, c \in A,\ (a \times b) \times c = a \times (b \times c)$ （結合法則）

(6) $\exists 1 \in A,\ \forall a \in A,\ a \times 1 = 1 \times a = a$ （単位元の存在）

(7) $\forall a, b, c \in A,\ a \times (b + c) = (a \times b) + (a \times c),\ (b + c) \times a = (b \times a) + (c \times a)$ （分配法則）

通常、「$\times$」は省略して書かない。また、a の加法に関する逆元（上記 (4) 参照）を $-a$ と書き、$a + (-b)$ を $a - b$ と書く（これで減法が定義されたことになる）。例えば、$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ などがそうである。$\mathbb{R}$ を成分とする n 次正方行列全体の集合も環になる。さらに、$\mathbb{Z}/m\mathbb{Z}$ も環になる。これらの例のうち、n 次正方行列全体の作る環 $(n \geq 2)$ を除いて、次の性質を持つ。

(8) $\forall a, b \in A,\ ab = ba$ （乗法に関する交換法則）

この性質を持つ環を可換環という。

多項式と形式的べき級数

A を可換環とし、

$$\mathbb{N}_0 = \{0, 1, 2, \dots\}$$

とすると、$A^{\mathbb{N}_0}$ に和と積を定義することができる。

$$(f+g)(n) = f(n) + g(n),$$
$$(fg)(n) = \sum_{k=0}^{n} f(k)g(n-k).$$

これらの演算により $A^{\mathbb{N}_0}$ は環になり、これを A 係数 1 変数形式的べき級数環 (univariate formal power series ring over A) という。通常 f のかわりに変数（ただの記号）x を用いて

$$\sum_{n=0}^{\infty} f(n)x^n$$

と書き、そのとき $A^{\mathbb{N}_0}$ を $A[[x]]$ と書く。

$f \in A^{\mathbb{N}_0}$ であって

$$\text{有限個の } n \in \mathbb{N}_0 \text{ を除いて } f(n) = 0$$

を満たすものを A 係数 1 変数多項式という。A 係数 1 変数多項式全体のつくる $A^{\mathbb{N}_0}$ の部分集合はそれ自身、$A^{\mathbb{N}_0}$ の演算に関して環になり、これを A 係数 1 変数多項式環 (univariate polynomial ring over A) という。変数に x を使うとき、A 係数 1 変数多項式環を $A[x]$ と書く。

剰余環の構成

$\mathbb{Z}$ から $\mathbb{Z}/m\mathbb{Z}$ を作る方法を、一般化する。A を、可換環とする。A の空でない部分集合 I がイデアルとは、

(i) $\forall a \in I, \forall b \in I, a + b \in I$

(ii) $\forall a \in A, \forall b \in I, ab \in I$

が成り立つときをいう。$A = \mathbb{Z}$ とし、$m \in \mathbb{Z}$ とすると

$$I = m\mathbb{Z} = (m) = \{am \mid a \in \mathbb{Z}\}$$

はイデアルになる。一般に、I が A のイデアルならば

$$R = \{(a, b) \mid a \in A,\ b \in A,\ a - b \in I\}.$$

は A 上の同値関係になる。商集合 A/R を A/I と書く。A/I に演算 $+, \times$ を次のように定義することができる。

$$\begin{aligned} + &: A/I \times A/I \to A/I, \quad + ([a], [b]) = [a + b], \\ \times &: A/I \times A/I \to A/I, \quad \times ([a], [b]) = [ab]. \end{aligned}$$

これらの写像 $+, \times$ は well-defined であり、これらの演算により A/I は環になる。