

2011年7月12日

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。

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。

\mathbb{Z} から \mathbb{Q} を作る構成法を、「商体 (quotient field, field of fractions)」の構成という。同じ構成法は次に定義する整域にも適用できる。

整域とその商体

可換環 A が次の条件を満たすとき、整域 (integral domain) という。

$$(9) \forall a, b \in A - \{0\}, a \times b \neq 0$$

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は整域である。 p が素数のとき $\mathbb{Z}/p\mathbb{Z}$ は整域だが、 $m > 1$ が素数でない自然数のとき、 $\mathbb{Z}/m\mathbb{Z}$ は整域ではない。環 A が整域ならば、 $A[[x]], A[x]$ も整域である。

A を整域とすると、

$$X = \{(a, b) \mid a \in A, b \in A, b \neq 0\}$$

とおき、

$$R = \{((a, b), (c, d)) \mid ((a, b), (c, d)) \in X \times X, ad = bc\}$$

とおくと、 R は X 上の同値関係になる。 R による商集合

$$X/R = \{[a, b] \mid (a, b) \in X\}$$

に演算 $+, \times$ を次のように定義することができる。

$$+ : (X/R) \times (X/R) \rightarrow X/R, \quad +([a, b], [c, d]) = [ad + bc, bd]$$

$$\times : (X/R) \times (X/R) \rightarrow X/R, \quad \times([a, b], [c, d]) = [ac, bd].$$

これらの写像 $+, \times$ は well-defined であり、これらの演算により X/R は環になる。 X/R を整域 A の商体という。

\mathbb{Z} の商体が \mathbb{Q} であることは先週示した。 $\mathbb{R}[x]$ の商体は有理関数体 (field of rational functions, x の有理式=分数式の全体で、 $\mathbb{R}(x)$ と書く) ができる。 $\mathbb{R}[[x]]$ の商体はどんなものになるだろうか？

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、

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

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

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。

$$+ : A/I \times A/I \rightarrow A/I, \quad +([a], [b]) = [a + b],$$

$$\times : A/I \times A/I \rightarrow A/I, \quad \times([a], [b]) = [ab].$$

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。

$A = \mathbb{R}[x]$ のイデアル

$$(x^2 + 1) = \{f(x)(x^2 + 1) \mid f(x) \in \mathbb{R}[x]\}$$

を考えると、写像 $g : \mathbb{R}[x]/(x^2 + 1) \rightarrow \mathbb{C}$, $g([f(x)]) = f(\sqrt{-1})$ が定義できて、これは全単射であり、しかも $[f_1(x)], [f_2(x)] \in \mathbb{R}[x]/(x^2 + 1)$ に対して

$$g([f_1(x)] + [f_2(x)]) = g([f_1(x)]) + g([f_2(x)]),$$

$$g([f_1(x)] \times [f_2(x)]) = g([f_1(x)])g([f_2(x)])$$

ただし右辺は \mathbb{C} における和と積である。

一般に A, B を2つの環とするとき、ある全単射 $g : A \rightarrow B$ が存在して、 $\forall a, b \in A$,

$$g(a + b) = g(a) + g(b),$$

$$g(ab) = g(a)g(b)$$

となるとき、 A と B は同型であるといい、 $A \cong B$ と書く。上のことは $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ となることを示している。また、 $\mathbb{Q} \cong (\mathbb{Z} \text{ の商体})$ である。