

Def. 集合 R が2つの演算

加法 $R \times R \rightarrow R, (a, b) \mapsto a + b,$

乗法 $R \times R \rightarrow R, (a, b) \mapsto ab,$

で次を満たすものをもつとき R を環 (ring) という.

(R1) R は加法について Abel 群 (可換群) をなす. すなわち

(加法交換律) $\forall a, b \in R$ に対して $a + b = b + a.$

(加法結合律) $\forall a, b, c \in R$ に対して $(a + b) + c = a + (b + c).$

(加法単位元の存在) $\exists 0 \in R$ が存在して $\forall a \in R$ に対して $a + 0 = 0 + a = a.$
0 のことを零元と呼ぶ.

(加法逆元の存在) $\forall a \in R$ に対して, $\exists b \in R$ が存在して, $a + b = b + a = 0.$
この b のことを $-a$ と表す. また $c + (-a)$ のことを $c - a$ と表す.

(R2) (乗法結合律) $\forall a, b, c \in R$ に対して $(ab)c = a(bc).$

(R3) (分配律) $\forall a, b, c \in R$ に対して, $a(b + c) = ab + ac, (a + b)c = ac + bc.$

更に次の条件を入れることもある.

(R4) (乗法単位元の存在) $\exists 1 \in R$ が存在して, $a1 = 1a = a$

乗法単位元 1 のことを単に単位元と呼ぶ.

(R5) (乗法交換律) $\forall a, b \in R$ に対して $ab = ba.$

特に (R5) を満たす環を可換環 (commutative ring) と呼ぶ.

更に単位元を持つ可換環が

(R6) (乗法逆元の存在) $\forall a \in R, a \neq 0$ に対して, $\exists b \in R$ が存在して $ab = ba = 1.$

この b のことを a^{-1} や $1/a$ などで表す. また $c(1/a)$ を c/a で表す.

を満たすとき R を体 (field) と呼ぶ.

Def. 集合 M が環 R 上の加群 (module over R), R -加群 (R -module) であるとは,

加法 $M \times M \rightarrow M, (m, n) \mapsto m + n,$

スカラー倍 $R \times M \rightarrow M, (a, m) \mapsto am,$

が定義され

(M1) M は加法について Abel 群をなす.

(M2) $\forall a \in R, \forall m, n \in M$ に対して, $a(m + n) = am + an.$

(M3) $\forall a, b \in R, \forall m \in M$ に対して, $(a + b)m = am + bm.$

(M4) $\forall a, b \in R, \forall m \in M$ に対して, $(ab)m = a(bm).$

(M5) $\forall m \in M$ に対して, $1m = m.$

を満たすときを言う.