2. 体の定義

2–1. **群の定義.** 集合 G 上に演算 $*: G \times G \to G$ と元 $e = e_G \in G$ とがあって次を満たす時、$G = (G, *, e)$ は**群 (group)** を成すという。

(1) $\forall x, y, z \in G : (x * y) * z = x * (y * z)$ (結合律,associative law)
(2) $\forall x \in G : x * e = e * x = x$ (単位元,unit)
(3) $\forall x \in G : \exists y \in G : x * y = y * x = e$ (逆元,inverse)

通常は演算記号 $*$ を省略して、$x * y$ を単に xy と書く。単位元 e を 1 と書くことも多い。

- $e' \in G$ に対し、$(\forall x \in G : x * e' = e' * x = x) \Rightarrow e' = e$ (単位元の一意性)
- $x \in G$ に対し、上述の y は一意に定まり、この $y \in G$ を通常 x^{-1} と書く。

更に、群 G が次をも満たす時、**可換群 (commutative group)** という。

(4) $\forall x, y \in G : x * y = y * x$ (可換律,commutative law)

(**アーベル群 (abelian group)** ともいう。) 可換群では演算を $+$ で書くこともある (加法群 (additive group) という)。この時は、単位元を 0 、x の逆元を $-x$ と書く。

2–2. **環の定義.** 集合 R 上に 2 種の演算 $+ : R \times R \to R$ (**加法 (addition)** と呼ぶ), $\cdot : R \times R \to R$ (**乗法 (multiplication)** と呼ぶ) と元 $0 = 0_R, 1 = 1_R \in R$ とがあって次を満たす時、$R = (R, +, \cdot, 0, 1)$ は**環 (ring)**(単位元を持つ環) を成すという。

(1) $(R, +, 0)$ が可換群を成す。(R の**加法群 (additive group)** と呼ぶ。)
(2) $\forall x, y, z \in R : (x\cdot y)\cdot z = x\cdot(y\cdot z)$ (結合律,associative law)
(3) $\forall x \in R : x\cdot 1 = 1\cdot x = x$ (**単位元 (identity element, unit element)**)
(4) $\forall x, y, z \in R : x\cdot(y + z) = x\cdot y + x\cdot z, (x + y)\cdot z = x\cdot z + y\cdot z$ (分配律,distributive law)

更に、環 R が次をも満たす時、**可換環 (commutative ring)** という。

(5) $\forall x, y \in R : x\cdot y = y\cdot x$ (可換律,commutative law)

$x + y$ を**和 (sum)** と呼ぶ。通常 $x\cdot y$ を単に xy と書き**積 (product)** と呼ぶ。

- 環 R の元 $x \in R$ に対し、その加法逆元を $-x$ と書く (負元・反元)。
- 環 R の元 $x \in R$ に対し、$y \in R$ が x の**逆元 (inverse)** $\overset{\leftharpoonup}{\Longleftrightarrow} xy = yx = 1$
- $x \in R$ に対し、その逆元は存在すれば一意的。x の逆元を x^{-1} と書く。
- $x \in R$ が**単元, 単数 (unit), 可逆元 (invertible element)**
  $\overset{\leftharpoonup}{\Longleftrightarrow} \exists y \in R : xy = yx = 1$
- $R^\times := \{x \in R | \exists y \in R : xy = yx = 1\}$: 単元全体。乗法で群を成す。
  (R の**乗法群 (multiplicative group), 単元群 (unit group)**)
- 環 R の 0 でない元 $x \in R \setminus \{0\}$ が R の**零因子 (zero divisor)**
  $\overset{\leftharpoonup}{\Longleftrightarrow} \exists y \in R \setminus \{0\} : xy = 0$(または $yx = 0$)
- 零環でない可換環 R が**整域 (integral domain)**
  $\overset{\leftharpoonup}{\Longleftrightarrow}$ (0 以外の) 零因子を持たない
  $\Longleftrightarrow \forall x, y \in R : (xy = 0 \Rightarrow (x = 0$ 又は $y = 0))$

2–3. **体の定義.** 可換環 K が $K^\times = K \setminus \{0\}$ を満たす時、K は**(可換) 体 (field)** を成すという。即ち、$K = (K, +, \cdot, 0, 1)$ が次を満たす時、体という。

(1) $(K, +, 0)$ が可換群を成す。
(2) $(K \setminus \{0\}, \cdot, 1)$ が可換群を成す。
(3) $\forall x, y, z \in K : x(y + z) = xy + xz, (x + y)z = xz + yz$ (分配律,distributive law)

2–4. **体の例.**

- **有理数体 (field of rational numbers)** $\boldsymbol{Q}$、**実数体 (field of real numbers)** $\boldsymbol{R}$、**複素数体 (field of complex numbers)** $\boldsymbol{C}$
- 素数 p に対し $\boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$ (p 元体)
- 体 K 上の**有理関数体 (rational function field)** $K(X)$