§1.1. 体

Dfn. 1.1.1 1.1.4 1.1.6 体とは

$\left\{\begin{array}{lll} \text{集合 } \mathbb{K} & & \\ \text{二項演算 } + & & \text{(和/加法)} \\ \quad \text{〃} \quad \cdot & & \text{(積/乗法)} \end{array}\right.$

の組 $(\mathbb{K}, +, \cdot)$ であって

(1)-(9) をみたすもの.

(2) の $0 \in \mathbb{K}$：零元

(6) の $1 \in \mathbb{K}$：単位元

体 $(\mathbb{K}, +, \cdot)$ のことを $\mathbb{K}$ と略記する.

$(\mathbb{K}, +)$ は可換群：(1)-(4)

(1) $\forall a, b, c \in \mathbb{K}\quad (a+b)+c = a+(b+c)$.

(2) $\exists 0 \in \mathbb{K}.\ \forall a \in \mathbb{K}\quad a+0 = 0+a = a$

(3) $\forall a \in \mathbb{K}\ \exists -a \in \mathbb{K}\quad a+(-a) = (-a)+a = 0$

(4) $\forall a, b \in \mathbb{K},\quad a+b = b+a$

$(\mathbb{K}, \cdot)$ は　モノイド：(5), (6)

(5) $\forall a, b, c \in \mathbb{K}\quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(6) $\exists 1 \in \mathbb{K}\quad \forall a \in \mathbb{K}\quad a \cdot 1 = 1 \cdot a = a$

$(\mathbb{K}, +, \cdot)$ は環：(1)-(7)

(7) $\forall a, b, c \in \mathbb{K}\quad (a+b) \cdot c = ac + bc$,

$a \cdot (b+c) = ab + ac$

$(\mathbb{K}, +, \cdot)$ は可換環：(1)-(8)

(8) $\forall a, b \in \mathbb{K}\quad a \cdot b = b \cdot a$

$(\mathbb{K}, +, \cdot)$ は体：

(9) $\forall a \in \mathbb{K} \setminus \{0\},\ \exists a^{-1} \in \mathbb{K},\ a \cdot a^{-1} = 1$

↑ $\mathbb{K}$ から 0 を除いた集合 □

Rmk. 二項演算は写像 $\mathbb{K} \times \mathbb{K} \to \mathbb{K}$

とみなせる.　↑ $\{(a,b) \mid a, b \in \mathbb{K}\}$

積・は略す　集合 $\mathbb{K}$ とそれ自身の直積

Exm. 1.1.7 有理数体 $\mathbb{Q}$, 実数体 $\mathbb{R}$, 複素数体 $\mathbb{C}$.

$+$ と $\cdot$ は(通常の)数の和と積 □

Rmk. 整数環 $\mathbb{Z}$ ($+$ と $\cdot$ は通常の和と積) は体ではない.

$\because$ $2 \in \mathbb{Z} \setminus \{0\}\quad \nexists a \in \mathbb{Z}\quad 2 \cdot a = 1.$ より (9) は不成立 □

Exm. 1.1.7 p：素数.　$\mathbb{F}_p := \{0, 1, \ldots, p-1\}$

$\forall a, b \in \mathbb{F}_p\quad a \mathbin{+_p} b := a+b \bmod p,\quad a \mathbin{\cdot_p} b := a \cdot b \bmod p$

↑ $\mathbb{Z}$ での和　↑ $\mathbb{Z}$ での積

$(\mathbb{F}_p, +_p, \cdot_p)$ は体.　(問 1.1) □

§1.2. 線形空間

Dfn. 1.2.1 体$\mathbb{K}$上の線形空間とは、

- 集合 V
- 写像 $+ : V \times V \to V$ (和)
- 〃 $\cdot : \mathbb{K} \times V \to V$ (スカラー倍)

の組 $(V, +, \cdot)$ であって (1)-(7) をみたすもの。

$\mathbb{K}$線形空間とも呼ぶ。

$(V, +, \cdot)$ を V と略記する、$\mathbb{K}$: Vの係数体。

スカラー倍 $\cdot$ は略す。

$(V, +)$ は可換群:

(1) $\forall u, v, w \in V \quad (u+v)+w = u+(v+w)$

(2) $\exists 0 \in V \quad \forall v \in V \quad v+0 = 0+v = v$

(3) $\forall v \in V \quad \exists -v \in V \quad v+(-v) = (-v)+v = 0$

(4) $\forall u, v \in V \quad u+v = v+u$

和とスカラー倍の分配律:

(5) $\forall a, b \in \mathbb{K}, \ \forall v \in V \quad (a \cdot b) \cdot v = a \cdot (b \cdot v)$

(6) $\forall a \in \mathbb{K}, \ \forall v, w \in V \quad a \cdot (v+w) = a \cdot v + a \cdot w$

単位元 $1 \in \mathbb{K}$ のスカラー倍は恒等写像

(7) $\forall v \in V \quad 1 \cdot v = v$ $\square$

Exm. 1.2.5 1.2.6 (数ベクトル空間), n: 正整数

$$\mathbb{R}^n := \left\{ v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \middle| \ v_i \in \mathbb{R} \right\}, \quad \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} := \begin{pmatrix} v_1+w_1 \\ \vdots \\ v_n+w_n \end{pmatrix}, \quad \overset{a \in \mathbb{R}}{a} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} := \begin{pmatrix} av_1 \\ \vdots \\ av_n \end{pmatrix}$$

$(\mathbb{R}^n, +, \cdot)$ は実数体$\mathbb{R}$上の線形空間。

任意の体 $\mathbb{K}$ に対し、同様に $\mathbb{K}$線形空間 $(\mathbb{K}^n, +, \cdot)$ が定まる。 $\square$

§1.3 線形空間の例

Exm. 1.3.1. (行列空間) m, n: 正整数, $\mathbb{K}$: 体

$$M(m,n;\mathbb{K}) := \left\{ X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix} \middle| \, x_{ij} \in \mathbb{K} \right\} \ni X, Y.$$

$X+Y := (x_{ij}+y_{ij})_{ij}$, $aX := (a x_{ij})_{ij}$ $a \in \mathbb{K}$

$(M(m,n;\mathbb{K}), +, \cdot)$ は $\mathbb{K}$ 線形空間 $\square$

Exm. 1.3.2 (函数空間) S: 空でない集合 $\quad f: S \to \mathbb{R}, \; s \mapsto f(s)$

$\mathbb{R}^S := \{$写像 $S \to \mathbb{R}\} \ni f, g$, $a \in \mathbb{R}$

$f+g \in \mathbb{R}^S$: $(f+g)(s) := f(s)+g(s)$. $af \in \mathbb{R}^S$: $(af)(s) := a \cdot f(s)$

$(\mathbb{R}^S, +, \cdot)$ は $\mathbb{R}$ 線形空間. (問1.2) 一般の体$\mathbb{K}$に対しても、$\mathbb{K}$線形空間$\mathbb{K}^S$が定義できる. $\square$

Exm. 1.3.6 $U \subset \mathbb{R}$: 空でない開区間. (例えば $\mathbb{R}$全体, $(0,1)$区間, $(0,+\infty)=\mathbb{R}_{>0}$)

$C^0(U) := \{f: U \to \mathbb{R} \mid U$上連続$\}$

$C^1(U) := \{ \quad 〃 \quad \mid 〃$ 微分可能で, f'は連続$\}$

$\vdots$

n: 正整数 $C^n(U) := \{ \quad 〃 \quad \mid U$上$n$回微分可能で, $f^{(n)}$は連続$\}$

$\vdots$

$C^\infty(U) := \{ \quad 〃 \quad \mid U$上 任意回微分可能$\}$

$$\mathbb{R}^U \supset C^0(U) \supset C^1(U) \supset \cdots \supset C^n(U) \supset \cdots C^\infty(U)$$

$\mathbb{R}^U$の$+$と$\cdot$について, これらは全て $\mathbb{R}$線形空間. $\square$

§1.4. 線形写像

Dfn. 1.4.1 $\mathbb{K}$：体．V, W：$\mathbb{K}$線形空間 $(V, \underset{V}{+}, \underset{V}{\cdot}),\ (W, \underset{W}{+}, \underset{W}{\cdot})$

$\mathbb{K}$線形写像 $f: V \to W$ とは，写像 $V \to W$ であって

$\forall v, v' \in V,\ \forall a \in \mathbb{K}\quad f(v \underset{V}{+} v') = f(v) \underset{W}{+} f(v'),\ f(a \underset{V}{\cdot} v) = a \underset{W}{\cdot} f(v)$ □

Exm. 1.4.2（行列の左掛算写像）$\mathbb{K}$：体，m, n：正整数，$X \in M(m, n; \mathbb{K})$

$l_X : \mathbb{K}^n \to \mathbb{K}^m,\ v \mapsto Xv$ は$\mathbb{K}$線形写像 □

Exm. 1.4.6（微分）$\phi \neq U \subset \mathbb{R}$：開区間．

$\frac{d}{dx} : C^\infty(U) \to C^\infty(U),\ f(x) \mapsto \frac{df}{dx}(x) = f'(x)$

は $\mathbb{R}$線形写像 （問1.3） □

Dfn. 1.4.7 全単射である$\mathbb{K}$線形写像を $\mathbb{K}$同型（写像）と呼ぶ． □

← 全射かつ単射 ⇔ 逆写像が存在．

Exm. 1.4.9. n：正整数．$[n] := \{1, 2, \ldots, n\}$ n点集合 $\mathbb{K}$：体

$\mathbb{K}^n$：数ベクトル空間 $\mathbb{K}^{[n]} = \{[n] \to \mathbb{K}\}$：関数空間

$\varphi : \mathbb{K}^{[n]} \to \mathbb{K}^n,\ f \mapsto \begin{pmatrix} f(1) \\ \vdots \\ f(n) \end{pmatrix}$ は$\mathbb{K}$同型

∵ $\forall f, g \in \mathbb{K}^{[n]}$．$\varphi(f+g) = {}^t(f(i) + g(i))_{i=1}^n = {}^t(f(i))_i + {}^t(g(i))_i = \varphi(f) + \varphi(g)$

$\forall a \in \mathbb{K}\quad \varphi(af) = {}^t(af(i))_i = a \cdot {}^t(f(i))_i = a \cdot \varphi(f)$

逆写像は $\psi : \mathbb{K}^n \to \mathbb{K}^{[n]},\ {}^t(v_i)_i \mapsto (f : i \mapsto v_i)$ □

Exm. 1.4.8 行列 $X \in M(m, n; \mathbb{R})$ の左掛算写像 $l_X : \mathbb{R}^n \to \mathbb{R}^m$ について，

l_X が同型 ⇔ $m = n$ かつ X は正則行列 （問1.4） □