代数系入門

第 3 章 環と多項式

今村勇輝

February 6, 2022

Def. 1.1

R : 集合, $R \neq \emptyset$,
$R \times R \to R, (a,b) \mapsto a+b, (a,b) \mapsto ab$

1. R : 加法について可換群
2. $\forall a,b,c \in R \Rightarrow (ab)c = a(bc)$
3. $\forall a,b,c \in R \Rightarrow a(b+c) = ab+ac, (b+c)a = ba+ca$
4. $\exists e \in R$ s.t. $\forall a \in R, ea = ae = a$

$\overset{\text{def}}{\Leftrightarrow} R$: **環** (ring)

Def. 1.2

R: 環

- $\exists! e_+ \in R$ s.t. $\forall a \in R, e_+ + a = a \overset{\text{def}}{\Leftrightarrow} 0 := e_+$: R の**零元**
- $\forall a \in R, \exists! a' \in R$ s.t. $a + a' = 0 \overset{\text{def}}{\Leftrightarrow} -a := a'$

Def. 1.3

R : 環, $\forall a,b \in R \Rightarrow ab = ba \overset{\text{def}}{\Leftrightarrow} R$: **可換環**

Thm. 1.1

R : 環, $\exists ! e \in R$ s.t. $\forall a \in R, ea = ae = e \overset{\text{def}}{\Leftrightarrow} 1 := e : R$ の単位元

Exm. 1

$\mathbb{Z}$: 可換環 : 有理整数環

Exm. 2

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$: 可換環

Exm. 3

$[0,1] \subset \mathbb{R}, R = \{f \mid f\colon [0,1] \to [0,1]\}$,
$f, g \in R, \forall t \in [0,1], (f+g)(t) = f(t) + g(t), (fg)(t) = f(t)g(t) \Rightarrow R$: 可換環

Exm. 4

$\forall R$: 環, $\forall S$: 集合, $S \neq \emptyset, M(S,R) = \{f \mid f : S \to R\}$,
$f, g \in M(S,R), \forall x \in S, (f+g)(x) = f(x) + g(x), (fg)(x) = f(x)g(x) \Rightarrow M(S,R)$: 環

Def. 1.4

- $0 \in M(S,R)$: S から R の**零写像**
- $-f \in R, \forall x \in S, (-f)(x) = -f(x)$

Rem. $\forall x \in S, 0(x) = 0_R$

Def. 1.5

$\forall A$: 加法群, $f : A \to A$: hom. : **自己準同型写像, 自己準同型** (endomorphism)
$\mathrm{End}(A) := \{f \mid f : A \to A : \text{hom.}\}$

Exm. 5

$\forall A$: 加法群,
$f, g \in \mathrm{End}(A), \forall x \in A, (f+g)(x) = f(x) + g(x), (fg)(x) = f(g(x)) \Rightarrow \mathrm{End}(A)$: 環

Rem. $\mathrm{End}(A)$: **自己準同型環**

Thm. 1.2

R : 環

1. $0 \in R, \forall a \in R \Rightarrow a0 = 0a = 0$
2. $\forall a, b \in R \Rightarrow a(-b) = (-a)b = -ab$
3. $\forall a, b \in R \Rightarrow (-a)(-b) = ab$
4. $\forall a, b, c \in R, b - c := b + (-c) \Rightarrow a(b - c) = ab - ac, (b - c)a = ba - ca$
5. $a_1, \cdots, a_m, b_1, \cdots, b_n \in R \Rightarrow (a_1 + \cdots + a_m)(b_1 + \cdots + b_m) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j$

Thm. 2.1

R : 環, $0, 1 \in R$
$1 = 0 \Rightarrow R = \{0\}$ $(\because \forall a \in R, a = 1a = 0a = 0)$

Def. 2.1

R : 環, $0, 1 \in R, 1 = 0 \overset{\text{def}}{\Leftrightarrow} R$: **零環**

Rem. 今後, R は零環ではないとする.

Def. 2.2

$\exists a, b \in R$ s.t. $a \neq 0, b \neq 0, ab = 0 \overset{\text{def}}{\Leftrightarrow} a, b : R$ の**零因子** (a : 左零因子, b : 右零因子)

Def. 2.3

$\forall a, b \in R, a \neq 0, b \neq 0 \Rightarrow ab \neq 0, R$: 可換 $\overset{\text{def}}{\Leftrightarrow} R$: **整域**

Exm. 1

$\mathbb{Z}$: 整域

Exm. 2

§1 Exm. 3 は整域ではない

Def. 2.4

$a \in R, \exists b \in R$ s.t. $ba = ab = 1 \overset{\text{def}}{\Leftrightarrow} a : R$ の**可逆元**または**単元**, $a^{-1} := b : a$ の**逆元**

Thm. 2.2

- $a \in R$: 単元 $\Rightarrow a \neq 0$
- $a \in R$: 単元 $\Rightarrow \exists! a^{-1} \in R$ s.t. $a^{-1}a = aa^{-1} = 1$

Lem. A

R : 環, $G = \{a \in R \mid a : R$ の単元 $\} \Rightarrow G$: 乗法に関して群

Exm. 3

A : 加法群, $A \neq \{0\}$

- $f \in \mathrm{End}(A), f$: 単元 $\Rightarrow f$: iso.
- $G = \{f \in \mathrm{End}(A) \mid f$: 単元 $\} \Rightarrow G = \mathrm{Aut}(A)$

Def. 2.5

R : 環

- $\forall a \in R, a \neq 0 \Rightarrow a$: 単元 $\overset{\text{def}}{\Leftrightarrow} R$: **斜体**
- R : 斜体, $\forall a, b \in R, ab = ba \overset{\text{def}}{\Leftrightarrow} R$: **体**

Thm. 2.3

R: 環

- R : 斜体 $\Leftrightarrow G = \{a \in R \mid a \neq 0\}$: 乗法に関して群
- R : 体 $\Leftrightarrow G = \{a \in R \mid a \neq 0\}$: 乗法に関して可換群

Exm. 4

- $\mathbb{Z}$: 環 $\not\Rightarrow \mathbb{Z}$: 体
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$: 環 $\Rightarrow \mathbb{Q}, \mathbb{R}, \mathbb{C}$: 体

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

Thm. 2.4

$\forall R$: 体 $\Rightarrow R$: 整域

Lem. B

R : 整域, $|R| < \infty \Rightarrow R$: 体

Def. 2.6

R : 環, $R' \subset R, R' \neq \emptyset$

R' : R で定義されている加法, 乗法に関して環, $1_R \in R' \overset{\text{def}}{\Leftrightarrow} R'$: R の**部分環**

Thm. 2.5

R : 環, $R' \subset R$

R' : R の部分環 $\Leftrightarrow 1_R \in R', \forall a, b \in R' \Rightarrow -a, a+b, ab \in R'$

Def. 2.7

R' : R の部分環

- R' : 斜体 $\overset{\text{def}}{\Leftrightarrow}$ R の部分斜体
- R' : 体 $\overset{\text{def}}{\Leftrightarrow}$ R の部分体

Exm. 5

- 環 $\mathbb{Z}$: 体 $\mathbb{Q}$ の部分環
- 体 $\mathbb{Q}$: 体 $\mathbb{R}$ の部分体

Exm. 6

$R = \{f \mid f\colon [0,1] \to [0,1]\}$ (§1 Exm. 3 の環)

- $R' = \{f \mid f\colon [0,1] \to [0,1]$: 連続関数 $\} \Rightarrow R'$: R の部分環
- $R'' = \{f \mid f\colon [0,1] \to [0,1]$: 微分可能関数 $\} \Rightarrow R''$: R' の部分環

Def. 2.8

R : 斜体, $\forall a, b \in R \Rightarrow ab \neq ba \overset{\text{def}}{\Leftrightarrow} R$: **非可換体**

Exm. 7

$\mathbb{C}$: 複素数の加法群, $A = \mathbb{C} \times \mathbb{C}$

1. $\alpha, \beta \in \mathbb{C}, f_{\alpha,\beta} : A \to A, (x, y) \mapsto (\alpha x - \beta y, \bar{\beta} x + \bar{\alpha} y) \Rightarrow f_{\alpha,\beta} \in \mathrm{End}(A)$
2. $Q = \{f_{\alpha,\beta} \mid$ 上記 $f_{\alpha,\beta}\} \Rightarrow Q : \mathrm{End}(A)$ の部分環
3. Q : 非可換体

Rem. Q : $\mathbb{R}$ 上の**四元数環**

Thm. 2.6

R : 整域または斜体 $\Rightarrow \exists 0, 1 \in R$ s.t. $0 \neq 1$

Def. 3.1

R : 環, $J \subset R, J \neq \emptyset$

1. $\forall a, b \in J \Rightarrow a + b \in J$
2. $\forall r \in R, \forall a \in J \Rightarrow ra \in J$

$\overset{\text{def}}{\Leftrightarrow} J : R$ の**左イデアル**

Thm. 3.1

R : 環, $J \subset R, J \neq \emptyset$
$J : R$ の左イデアル $\Leftrightarrow J \leq R$: 加法部分群, $\forall r \in R, \forall a \in J \Rightarrow ra \in J$

Def. 3.2

R : 環
$J \leq R$: 加法部分群, $\forall r \in R, \forall a \in J \Rightarrow ar \in J \overset{\text{def}}{\Leftrightarrow} J : R$ の**右イデアル**

Def. 3.3

$J:R$ の左イデアルかつ右イデアル $\overset{\text{def}}{\Leftrightarrow}$ $J:R$ の**イデアル**または**両側イデアル**

Rem. R が可換なら, 左イデアル, 右イデアル, 両側イデアルは一致する

Exm. 1

$R=\{f \mid f\colon [0,1]\to[0,1]$: 実数値連続関数 $\}$
$c\in[0,1], J_c=\{f\in R \mid f(c)=0\} \Rightarrow J_c:R$ のイデアル

Exm. 2

$n\in\mathbb{Z}, n\geq 0 \Rightarrow n\mathbb{Z}$: 環 $\mathbb{Z}$ のイデアル

Exm. 3

R : 環

- $a \in R, J_a = \{xa \mid x \in R\} \Rightarrow J_a$: 左イデアル
- $a_1, \cdots, a_n \in R, J = \{x_1 a_1 + \cdots + x_n a_n \mid x_1, \cdots x_n \in R\} \Rightarrow J$: 左イデアル

Def. 3.4

R : 環

- $a \in R, Ra$(または (a)) $:= \{xa \mid x \in R\}$: a によって生成される単項左イデアル
- $a_1, \cdots, a_n \in R, (a_1, \cdots, a_n) := \{x_1 a_1 + \cdots + x_n a_n \mid x_1, \cdots, x_n \in R\}$
  : $a_1, \cdots, a_n$ によって生成される左イデアル

Thm. 3.2

$\forall J$: R の左イデアル, $a_1, \cdots, a_n \in J \Rightarrow (a_1, \cdots, a_n) \subset J$

Thm. 3.3

R : 環

- $1 \in R \Rightarrow (1) = R$
- $0 \in R \Rightarrow (0) = \{0\}$
- $R, (0)$: R の両側イデアル

Def. 3.5

J : R のイデアル, $J = \{0\} \overset{\text{def}}{\Leftrightarrow} 0 := J$: 零イデアル

Thm. 1

R : 環, $R \neq \emptyset$
R : 斜体 $\Leftrightarrow \forall J$: R の左イデアル $\Rightarrow J = R$ or 0

Rem. 右イデアルも同様に成り立つが, 両側イデアルの場合 $\Leftarrow$ は必ずしも成り立たない.

Lem. C

R : 環, J : R のイデアル
$\forall a, a', b, b' \in R, a \equiv a' \pmod{J}, b \equiv b' \pmod{J} \Rightarrow ab \equiv a'b' \pmod{J}$

Thm. 2

R : 環, J : R のイデアル, $R/J \ni \bar{a} := a + J$
$\bar{a}, \bar{b} \in R/J, \bar{a} + \bar{b} = \overline{a+b},\ \bar{a}\bar{b} = \overline{ab} \Rightarrow R/J$: 環

Def. 3.6

R/J : R の J による**剰余環**または**商環**

Thm. 3.4

1. R/J : 零環 $\Leftrightarrow J = R$
2. $J = (0) \Rightarrow R/J \cong R$
3. R : 可換環 $\Rightarrow \forall R/J$: 可換

本節では特に有理数環 $\mathbb{Z}$ について考える.

Thm. 4.1

$n \geq 0, (n) := n\mathbb{Z} : \mathbb{Z}$ **のイデアル** ($\because$ §3 Exm. 2)
$\forall J : \mathbb{Z}$ **のイデアル** $\Leftrightarrow \exists n \in \mathbb{Z}$ s.t. $n \geq 0, J = (n)$

Def. 4.1

$n \geq 1, \mathbb{Z}_n := \mathbb{Z}/(n)$: **法** n **に関する** $\mathbb{Z}$ **の商環**

Rem. $|\mathbb{Z}_n| = n, \mathbb{Z}_1 = \{0\}$

Def. 4.2

$n \geq 2, \mathbb{Z}_n \ni \bar{a} := a + (n)$

Thm. 4.2

$\bar{a} \in \mathbb{Z}_n, \bar{a} \neq \bar{0}, (a, n) = 1, \forall a' \in a + (n) \Rightarrow (a', n) = 1$

Rem. 上記 $\bar{a}$: 第 1 章 §8 の「法 n に関する既約剰余類」のこと

Lem. D

$n \geq 2, \bar{a} \in \mathbb{Z}_n, \bar{a} \neq \bar{0}$

- $(a, n) = 1 \Rightarrow \bar{a}$: unit
- $(a, n) \neq 1 \Rightarrow \bar{a}$: 零因子

Thm. 3

$n \geq 2$

- $n = p$: 素数 $\Rightarrow \mathbb{Z}_p$: 体
- n : 素数でない $\Rightarrow \exists \bar{a} \in \mathbb{Z}_n$ s.t. $\bar{a}$: 零因子

Rem. $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$: 体

Def. 4.3

$(\mathbb{Z}/n\mathbb{Z})^\times := \{\bar{a} \in \mathbb{Z}_n \mid (a,n) = 1\}$: 法 n に関する $\mathbb{Z}$ の既約剰余類群

Def. 4.4

$\varphi(n) := |\{a \in \mathbb{Z} \mid 1 \leq a < n, (n,a) = 1\}|$: Euler の関数

Thm. 4.3

$|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$

Thm. 4.4 (Euler)

$a, n \in \mathbb{Z}, n \geq 0, (a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Thm. 4.5

p : 素数

- $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$
- $(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}_p \mid \bar{a} \neq \bar{0}\}$
- $(\mathbb{Z}/p\mathbb{Z})^\times$: 巡回群

これらの証明は体論と関係させたほうが都合がよいので第 5 章 §2 で行う.

Def. 5.1

R, R' : 環, $f : R \longrightarrow R'$

$f(1_R) = 1_{R'}, \forall x, y \in R, f(x+y) = f(x) + f(y), f(xy) = f(x)f(y) \overset{\text{def}}{\Longleftrightarrow} f$: **準同型写像**

Rem. 加法群の準同型写像と区別する場合は**環準同型 (写像)** とよぶ

Thm. 5.1

R, R', R'' : 環

$f : R \longrightarrow R'$: hom., $g : R' \longrightarrow R''$: hom. $\Rightarrow g \circ f : R \longrightarrow R''$: hom.

Rem. **単射準同型**, **全射準同型**, **同型**, **自己同型**などの語の用法は群の場合と同様

Def. 5.2

R, R' : 環

$\exists f : R \longrightarrow R'$: iso. $\overset{\text{def}}{\Longleftrightarrow} R \cong R'$: R と R' は**同型**

Exm. 1

$R = \{f \mid f\colon [0,1] \to [0,1] : \text{連続関数}\}$
$c \in [0,1], F\colon R \to \mathbb{R}, f \mapsto f(c) \Rightarrow F$: hom.

Exm. 2

$f\colon \mathbb{C} \to \mathbb{C}, \alpha \mapsto \bar{\alpha} \Rightarrow f \in \mathrm{Aut}(\mathbb{C})$

Exm. 3

$R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$: 環
$f\colon R \to R, a + b\sqrt{2} \mapsto a - b\sqrt{2} \Rightarrow f \in \mathrm{Aut}(R)$

Exm. 4

R : 環, J : R のイデアル
$\varphi : R \longrightarrow R/J, a \mapsto \bar{a} \Rightarrow \varphi$: hom. : **標準的準同型写像**または**自然な準同型写像**

Thm. 5.2

R, R' : 環
$f : R \longrightarrow R'$: hom. $\Rightarrow f(0_R) = 0_{R'}, f(-x) = -f(x)$

Thm. 5.3

R, R' : 環
$f : R \longrightarrow R'$: hom. $\Rightarrow R' \supset f(R)$: 環

Def. 5.3

R, R' : 環, $f\colon R \longrightarrow R'$: hom.

$f^{-1}(0) = \{x \in R \mid f(x) = 0\} \overset{\text{def}}{\Leftrightarrow} \mathrm{Ker} f := f^{-1}(0)$: f の核

Rem. $\mathrm{Ker} f$ は加法群の準同型としての f の核にほかならない

Thm. 5.4

R, R' : 環

$f\colon R \longrightarrow R'$: hom. $\Rightarrow \mathrm{Ker} f$: R の両側イデアル

Thm. 5.5

R, R' : 環, $f\colon R \longrightarrow R'$: hom.

$R' = \{0\} \Leftrightarrow \mathrm{Ker} f = R$

Exm. 5

$R = \{f \mid f\colon [0,1] \to [0,1]$: 連続関数 $\}$
$F : f \mapsto f(c)$: hom. (Exm. 1), $J_c = \{f \in R \mid f(c) = 0\}$ (§3 Exm. 1) $\Rightarrow \mathrm{Ker}\, F = J_c$

Exm. 6

R : 環
$\forall J : R$ のイデアル, $f\colon R \to R/J \Rightarrow \mathrm{Ker} f = J$

Thm. 5.6

R : 斜体, $R' \neq \emptyset$: 環, $f\colon R \to R'$: hom. $\Rightarrow f$: injective hom.

Thm. 4 (環の準同型定理)

R, R' : 環
$f\colon R \to R'$: hom., $\mathrm{Ker} f = J \Rightarrow g\colon R/J \to f(R)$: iso. $(R/J \cong f(R))$

Thm. 5

R, R' : 環, $f\colon R \to R'$: surjective hom., $\mathrm{Ker} f = J$

- M : left ideal of R, M' : left ideal of R', $J \subset M \Rightarrow f(M) = M', f^{-1}(M') = M$
- M : right ideal of R, M' : right ideal of R', $J \subset M \Rightarrow f(M) = M', f^{-1}(M') = M$
- M : ideal of $R \Leftrightarrow M'$: ideal of R, $R/M \cong R'/M'$

Def. 5.4

R : ring, J_L, J_R : left (right) ideal of R, $J_L, J_R \neq R$

$\forall J$: left ideal of $R \Rightarrow J = R$ or $J_L \overset{\text{def}}{\Leftrightarrow} J_L : R$ の**極大左イデアル** (maximal left ideal)

$\forall J$: right ideal of $R \Rightarrow J = R$ or $J_R \overset{\text{def}}{\Leftrightarrow} J_R : R$ の**極大右イデアル** (maximal right ideal)

Def. 5.5

R : ring, J_L, J_R : maximal left (right) ideal of R, $J_L, J_R \neq R$

R : commutative $\Rightarrow J_L = J_R$: **極大イデアル** (maximal ideal)

Thm. 6

R : ring, J : tow-sided ideal of R, $J \neq R$

R/J : skew field $\Leftrightarrow J$: maximal left ideal of $R \Leftrightarrow J$: maximal right ideal of R

Cor. 6.1

R : commutative ring, J : ideal of R, $J \neq R$

R/J field $\Leftrightarrow J$: maximal ideal of R

Lem. E

$\forall R$: ring $\Rightarrow \exists ! \mu : \mathbb{Z} \to R$: hom. s.t. $\mu(n) = n1_R$

Thm. 5.7

R : ring, $\mu : \mathbb{Z} \to R, n \mapsto n1_R$
$\forall R' \subset R$: subring $\Rightarrow \mu(R) \subset R'$

Def. 5.6

$\mu : \mathbb{Z} \to R, n \mapsto n1_R, \exists ! m \geq 0$ s.t. $\operatorname{Ker}\mu = (m) \overset{\text{def}}{\Leftrightarrow} m : R$ の**標数** (characteristic)

Thm. 5.8

R : ring, m : characteristic of R

- $m = 0 \Rightarrow \mu(R) \cong \mathbb{Z}$
- $m > 0 \Rightarrow \mu(R) \cong \mathbb{Z}/(m) = \mathbb{Z}_m$

Thm. 5.9

R : ring, m : characteristic of R

- $R = \{0\} \Leftrightarrow m = 1$
- $R \neq \{0\} \Rightarrow m = 0$ or $m \geq 2$
- $m = 0 \Rightarrow 1_R \in R$: additive group, $o(1_R) = \infty$
- $m \geq 2 \Rightarrow 1_R \in R$: additive group, $o(1_R) = m$

Lem. F

R : integral domain, m : characteristic of $R \Rightarrow m = 0$ or m : prime number