# 代数系入門 第3章環と多項式

## 今村勇輝

February 2, 2022

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- §5 準同型写像
- §6 商の体
- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性
- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 Z または © の上の多項式
- §13 多変数の多項式

## Def. 1.1

R:集合,  $R\neq\emptyset$ ,

 $R \times R \to R, (a, b) \mapsto a + b, (a, b) \mapsto ab$ 

■ R:加法について可換群

 $\forall a, b, c \in R \Rightarrow (ab)c = a(bc)$ 

 $\exists \ \forall a,b,c \in R \Rightarrow a(b+c) = ab + ac, (b+c)a = ba + ca$ 

 $\exists e \in R \text{ s.t. } \forall a \in R, ea = ae = a$ 

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

## Def. 1.2

R: 環

■  $\exists ! e_+ \in R \text{ s.t. } \forall a \in R, e_+ + a = a \stackrel{\text{def}}{\Leftrightarrow} 0 := e_+ : R$ の零元

 $\blacksquare \ \forall a \in R, \exists ! a' \in R \text{ s.t. } a + a' = 0 \stackrel{\text{def}}{\Leftrightarrow} -a := a'$ 

## Def. 1.3

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

└─§1 環とその例

## Thm. 1.1

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

## Exm. 1

Z:可換環:有理整数環

## Exm. 2

ℚ, ℝ, ℂ: 可換環

#### Exm. 3

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

#### Exm. 4

 $\forall R:$ 環 $, \forall S:$  集合 $, S \neq \emptyset, M(S,R) = \{f \mid f: S \rightarrow R\},$ 

 $f, g \in M(S, R), \forall x \in S, (f + g)(x) = f(x) + g(x), (fg)(x) = f(x)g(x) \Rightarrow M(S, R)$ : 環

### Def. 1.4

- $0 \in M(S,R) : S$  から R の零写像
- $-f \in R, \forall x \in S, (-f)(x) = -f(x)$

 $\underline{\mathsf{Rem.}}\ \forall x\in S, 0(x)=0_R$ 

#### 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)

 $\operatorname{End}(A) := \{ f \mid f : A \to A : \text{hom.} \}$ 

#### Exm. 5

∀A:加法群,

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

Rem. End(A): **自己準同型環** 

#### Thm. 1.2

R:環

$$0 \in R, \forall a \in R \Rightarrow a0 = 0a = 0$$

$$\forall a, b \in R \Rightarrow a(-b) = (-a)b = -ab$$

$$\forall a, b \in R \Rightarrow (-a)(-b) = ab$$

$$4 \forall a, b, c \in R, b-c := b + (-c) \Rightarrow a(b-c) = ab - ac, (b-c)a = ba - ca$$

$$a_1, \dots, a_m, b_1, \dots, b_n \in R \Rightarrow (a_1 + \dots + a_m)(b_1 + \dots + b_m) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j$$

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- §5 準同型写像
- §6 商の体
- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性
- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 ℤ または ℚ の上の多項式
- §13 多変数の多項式

## 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 $, 0, 1 \in R, 1 = 0 \stackrel{\text{def}}{\Leftrightarrow} R:$ 零環

Rem. 今後, R は零環ではないとする.

## Def. 2.2

 $\exists a,b \in R \text{ s.t. } a \neq 0, b \neq 0, ab = 0 \stackrel{\text{def}}{\Leftrightarrow} a,b : R$  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  $\stackrel{\text{def}}{\Leftrightarrow} R$ : 整域

└-- §2 整域, 体

## Exm. 1

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.  $ba = ab = 1 \stackrel{\text{def}}{\Leftrightarrow} a : R$  の可逆元または単元,  $a^{-1} \coloneqq b : a$  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.  $a^{-1}a = aa^{-1} = 1$

└─ §2 整域, 体

## Lem. A

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

## Exm. 3

A: 加法群,  $A \neq \{0\}$ 

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

## Def. 2.5

R:環

- $\forall a \in R, a \neq 0 \Rightarrow a :$  単元  $\stackrel{\text{def}}{\Leftrightarrow} R :$  斜体
- R: 斜体,  $\forall a, b \in R, ab = ba \stackrel{\text{def}}{\Leftrightarrow} R:$  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⇔ G = {a∈R | a≠0}: 乗法に関して可換群

## Exm. 4

■ Z:環 ⇒ Z:体

■  $\mathbb{Q}, \mathbb{R}, \mathbb{C} : \mathbb{Q} \to \mathbb{Q}, \mathbb{R}, \mathbb{C} : \mathbf{\Phi}$ 

Rem. Q: 有理数体, R: 実数体, C: 複素数体

└- §2 整域, 体

## Thm. 2.4

 $\forall R: \mathbf{\Phi} \Rightarrow R: 整域$ 

## Lem. B

R:整域,  $|R|<\infty\Rightarrow R:$ 体

## Def. 2.6

 $R: \overline{\mathfrak{P}}, R' \subset R, R' \neq \emptyset$ 

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

#### Thm. 2.5

 $R: 環, R' \subset R$ 

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

└ §2 整域, 体

#### Def. 2.7

R': R の部分環

■ R': 斜体 ⇔ R の部分斜体

■ R': 体 ⇔ R の部分体

#### Exm. 5

■ 環 ℤ:体 ℚ の部分環

■ 体 ②: 体 ℝ の部分体

## Exm. 6

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

■ R' = {f | f: [0,1] → [0,1]:連続関数 } ⇒ R': R の部分環

■ R'' = {f | f: [0,1] → [0,1]: 微分可能関数 } ⇒ R'': R' の部分環

└ §2 整域, 体

#### Def. 2.8

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

#### Exm. 7

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

 $\bullet \alpha, \beta \in \mathbb{C}, f_{\alpha,\beta} \colon A \to A, (x,y) \mapsto (\alpha x - \beta y, \bar{\beta} x + \bar{\alpha} y) \Rightarrow f_{\alpha,\beta} \in \operatorname{End}(A)$ 

②  $Q = \{f_{\alpha,\beta} \mid \textbf{上記} f_{\alpha,\beta}\} \Rightarrow Q : \operatorname{End}(A)$  の部分環

**3** Q: 非可換体

Rem. Q: R 上の四元数環

#### Thm. 2.6

R: 整域または斜体 ⇒ ∃0,1 ∈ R s.t. 0 ≠ 1

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- §5 準同型写像
- §6 商の体
- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性
- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 Z または Q の上の多項式
- §13 多変数の多項式

#### - 第 3 章 環と多項式

└─§3 イデアルと商環

## Def. 3.1

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

- $\forall a, b \in J \Rightarrow a + b \in J$
- $\forall r \in R, \forall a \in J \Rightarrow ra \in J$

 $\stackrel{\text{def}}{\Leftrightarrow} J: R$  の左イデアル

#### Thm. 3.1

 $R: \overline{\mathfrak{P}}, J \subset R, J \neq \emptyset$ 

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

 $J \le R$ : 加法部分群,  $\forall r \in R, \forall a \in J \Rightarrow ar \in J \stackrel{\text{def}}{\Leftrightarrow} J$ : R の右イデアル

└─§3 イテアルと商塚

## Def. 3.3

J: R の左イデアルかつ右イデアル  $\stackrel{\text{def}}{\Leftrightarrow} J: R$  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  $\}$   $c \in [0,1], J_c = \{f \in R \mid f(c) = 0\} \Rightarrow J_c : R$  の左イデアル

### Exm. 2

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

#### Exm. 3

## R:環

- $a \in R, J_a = \{xa \mid x \in R\} \Rightarrow J_a : 左イデアル$
- $a_1, \dots, a_n \in R, J = \{x_1a_1 + \dots + x_na_n \mid x_1, \dots x_n \in R\} \Rightarrow J : 左イデアル$

#### Def. 3.4

## R:環

- $a \in R, Ra($ または  $(a)) := \{xa \mid x \in R\} : a$  によって<mark>生成</mark>される単項左イデアル
- **■**  $a_1, \dots, a_n \in R, (a_1, \dots, a_n) \coloneqq \{x_1 a_1 + \dots + x_n a_n \mid x_1, \dots, x_n \in R\}$ :  $a_1, \dots, a_n$  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,  $a_1, \dots, a_n \in J \Rightarrow (a_1, \dots, a_n) \subset J$ 

## Thm. 3.3

R:環

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

#### Def. 3.5

J: R のイデアル,  $J = \{0\} \stackrel{\text{def}}{\Leftrightarrow} 0 \coloneqq J:$ 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.  $\pi$ 右イデアルも同様に成り立つが、両側イデアルの場合  $\pi$  は必ずしも成り立たない.

└─<sub>§3</sub> イデアルと商環

## Lem. C

$$\forall a, a', b, b' \in R, a \equiv a' \pmod{J}, b \equiv b' \pmod{J} \Rightarrow ab \equiv a'b' \pmod{J}$$

#### Thm. 2

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

#### Def. 3.6

R/J: R の J による剰余環または商環

### Thm. 3.4

- $\mathbf{I}$  R/J: 零環  $\Leftrightarrow J = R$
- $J = (0) \Rightarrow R/J = R$
- 3 R: 可換環 ⇒ ∀R/J: 可換

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 ℤ の商環
- §5 準同型写像
- §6 商の体
- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性
- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 ℤ または ℚ の上の多項式
- §13 多変数の多項式

## 本節では特に有理数環 ℤ について考える.

#### Thm. 4.1

 $n \ge 0, (n) := n\mathbb{Z} : \mathbb{Z} \ \mathcal{O} \ \mathsf{TTV} \ (\because \S 3 \ \mathsf{Exm.} \ 2)$   $\forall J : \mathbb{Z} \ \mathcal{O} \ \mathsf{TTV} \ \Leftrightarrow \exists n \in \mathbb{Z} \ \mathsf{s.t.} \ n \ge 0, J = (n)$ 

## Def. 4.1

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

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

#### Def. 4.2

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

## Thm. 4.2

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

Rem. ā: 第1章 §8の「法nに関する既約剰余類」のこと

## Lem. D

$$n \ge 2, \bar{a} \in \mathbb{Z}_n, \bar{a} \ne \bar{0}$$

- $\bullet$   $(a, n) = 1 \Rightarrow \bar{a} : \text{unit}$
- (a,n) ≠ 1 ⇒ ā: 零因子

## Thm. 3

 $n \ge 2$ 

- $n = p : 素数 \Rightarrow \mathbb{Z}_p :$ 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

L<sub>§4ℤ の商環</sub>

## Def. 4.3

$$n\geq 2, G=\{ar{a}\in\mathbb{Z}_n\mid (a,n)=1\}\Rightarrow G:$$
群  $(\because$  Lem. D)  $(\mathbb{Z}/n\mathbb{Z})^{ imes}\coloneqq G:$ 法  $n$  に関する  $\mathbb{Z}$  の既約剰余類群

#### Def. 4.4

$$\varphi(n) \coloneqq |\{a \mid 1 \le a \le n, (n, a) = 1\}|$$
: Euler の関数

## Thm. 4.3

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

## Thm. 4.4 (Euler)

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

## Thm. 4.5

## p:素数

$$|(\mathbb{Z}/p\mathbb{Z})^{\times}| = p - 1$$

$$(\mathbb{Z}/p\mathbb{Z})^{\times} = \{ \bar{a} \in \mathbb{Z}_p \mid \bar{a} \neq \bar{0} \}$$

■ (Z/pZ)×: 巡回群

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環

#### ■ §5 準同型写像

- §6 商の体
- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性
- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 Z または Q の上の多項式
- §13 多変数の多項式

## Def. 5.1

R, R': 環,  $f: R \to R'$ 

$$f(1_R) = 1_{R'}, \forall x, y \in R, f(x+y) = f(x) + f(y), f(xy) = f(x)f(y) \stackrel{\text{def}}{\Leftrightarrow} f$$
: 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

 $f\colon R\to R': \mathsf{hom.}, g\colon R'\to R'': \mathsf{hom.} \Rightarrow g\circ f\colon R\to R'': \mathsf{hom.}$ 

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

 $\exists f: R \to R' : \text{iso.} \stackrel{\text{def}}{\Leftrightarrow} R \cong R' : R \succeq R'$  は同型

└─§5 準同型写像

## Exm. 1

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

#### Exm. 2

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

## Exm. 3

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

└─<sub>§5</sub> 準同型写像

## Exm. 4

R:環,J:Rのイデアル

 $\varphi: R \to R/J, a \mapsto \bar{a} \Rightarrow \varphi: \text{hom.}: 標準的準同型写像または自然な準同型写像$ 

## Thm. 5.2

R, R': 環

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

## Thm. 5.3

R, R': 環

 $f: R \to R' : \text{hom.} \Rightarrow R' \supset f(R) : 環$ 

## Def. 5.3

R, R': 環,  $f: R \rightarrow R'$ : hom.

$$f^{-1}(0) = \{x \in R \mid f(x) = 0\} \stackrel{\text{def}}{\Leftrightarrow} \ker f := f^{-1}(0) : f \mathcal{D}_{k}$$

 $\underline{\mathsf{Rem.}}\ \ker f$  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

 $f: R \to R': hom. \Rightarrow \ker f: R$  の両側イデアル

 $\underline{\mathsf{Rem.}}\,R'=\{0\} \Leftrightarrow \ker f=R$ 

└─§6 商の体

## 1 第3章環と多項式

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- §5 準同型写像

## ■ §6 商の体

- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性
- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 Z または © の上の多項式
- §13 多変数の多項式

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- §5 準同型写像
- §6 商の体

## ■ §7 多項式環

- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性
- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 ℤ または ℚ の上の多項式
- §13 多変数の多項式

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- §5 準同型写像
- §6 商の体
- §7 多項式環

## ■ §8 体の上の多項式, 単項イデアル整域

- §9 素元分解とその一意性
- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 Z または © の上の多項式
- §13 多変数の多項式

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- §5 準同型写像
- §6 商の体
- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域

## ■ §9 素元分解とその一意性

- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 ℤ または ℚ の上の多項式
- §13 多変数の多項式

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- §5 準同型写像
- §6 商の体
- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性

## ■ §10 ℤ[i] の素元

- §11 多項式の根, 代数的閉体
- §12 ℤ または ℚ の上の多項式
- §13 多変数の多項式

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- §5 準同型写像
- §6 商の体
- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性
- §10 ℤ[i] の素元

## ■ §11 多項式の根, 代数的閉体

- §12 ℤ または ℚ の上の多項式
- §13 多変数の多項式

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- 85 準同型写像
- §6 商の体
- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性
- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 ℤ または ℚ の上の多項式
- §13 多変数の多項式

- §1 環とその例
- §2 整域, 体
- §3 イデアルと商環
- §4 Z の商環
- §5 準同型写像
- §6 商の体
- §7 多項式環
- §8 体の上の多項式, 単項イデアル整域
- §9 素元分解とその一意性
- §10 ℤ[i] の素元
- §11 多項式の根, 代数的閉体
- §12 ℤ または ℚ の上の多項式
- §13 多変数の多項式