

代数系入門
第 3 章 環と多項式

今村勇輝

January 27, 2022

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 \mathbb{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 $\mathbb{Z}[i]$ の素元

■ §11 多項式の根, 代数的閉体

■ §12 \mathbb{Z} または \mathbb{Q} の上の多項式

■ §13 多変数の多項式

Def. 1.1

R : 集合, $R \neq \emptyset$,

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

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. $\forall a \in R, ea = ae = a$

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

Def. 1.2

R : 環

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

■ $\forall a \in R, \exists! a' \in R$ 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

Thm. 1.1

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

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

Exm. 4

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

Def. 1.4

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

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

Def. 1.5

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

Exm. 5

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

Rem. $\text{End}(A) : \text{自己準同型環}$

Thm. 1.2

 R : 環

$$\boxed{1} \quad 0 \in R, \forall a \in R \Rightarrow a0 = 0a = 0$$

$$\boxed{2} \quad \forall a, b \in R \Rightarrow a(-b) = (-a)b = -ab$$

$$\boxed{3} \quad \forall a, b \in R \Rightarrow (-a)(-b) = ab$$

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

$$\boxed{5} \quad a_1, \dots, a_m, b_1, \dots, b_n \in R \Rightarrow (a_1 + \dots + a_m)(b_1 + \dots + b_n) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j$$

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

Thm. 2.1

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

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

 $\exists a, b \in R$ 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

Exm. 1

 \mathbb{Z} : 整域

Exm. 2

§1 Exm. 3 は整域ではない

Def. 2.4

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

Thm. 2.2

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

Lem. A

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

Exm. 3

A : 加法群, $A \neq \{0\}$

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

Def. 2.5

R : 環

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

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 $\Rightarrow \mathbb{Z}$: 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

 $\forall R : \text{体} \Rightarrow R : \text{整域}$

Lem. B

 $R : \text{整域}, |R| < \infty \Rightarrow R : \text{体}$

Def. 2.6

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

Thm. 2.5

 $R : \text{環}, R' \subset R$ $R' : R$ 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

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

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

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

Def. 2.8

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

Exm. 7

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

1 $\alpha, \beta \in \mathbb{C}, f_{\alpha, \beta}: A \rightarrow A, (x, y) \mapsto (\alpha x - \beta y, \bar{\beta}x + \bar{\alpha}y) \Rightarrow f_{\alpha, \beta} \in \text{End}(A)$

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

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 $\Rightarrow \exists 0, 1 \in R \text{ s.t. } 0 \neq 1$

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

Def. 3.1

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

$$1 \quad \forall a, b \in J \Rightarrow a + b \in J$$

$$2 \quad \forall r \in R, \forall a \in J \Rightarrow ra \in J$$

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

Thm. 3.1

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

Def. 3.3

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

$R = \{f \mid f: [0, 1] \rightarrow [0, 1] : \text{実数値連続関数}\}$

$c \in [0, 1], J_c = \{f \in R \mid f(c) = 0\} \Rightarrow J_c: R$ の左イデアル

Exm. 2

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

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 によって生成される単項左イデアル
- $a_1, \dots, a_n \in R, (a_1, \dots, a_n) := \{x_1a_1 + \dots + x_na_n \mid x_1, \dots, x_n \in R\}$
: 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

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

Def. 3.5

 $J : R$ のイデアル, $J = \{0\} \stackrel{\text{def}}{\Leftrightarrow} 0 := J$: 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 の左イデアル

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

Thm. 2

R : 環, J : R の左イデアル, $R/J \ni \bar{a} := a + J$

$$\bar{a}, \bar{b} \in R/J, \bar{a} + \bar{b} = \overline{a + b}, \bar{a}\bar{b} = \overline{ab} \Rightarrow R/J: \text{環}$$

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 $J = (0) \Rightarrow R/J = R$
- 3 R : 可換環 $\Rightarrow \forall R/J$: 可換

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 \mathbb{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 $\mathbb{Z}[i]$ の素元
- §11 多項式の根, 代数的閉体
- §12 \mathbb{Z} または \mathbb{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 \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

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

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

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

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

Lem. D

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

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

Thm. 3

$$n \geq 2$$

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

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

Def. 4.3

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

Def. 4.4

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

Thm. 4.3

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

Thm. 4.4 (Euler)

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

Thm. 4.5

p : 素数

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

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

Def. 5.1

$R, R' : \text{環}, f : R \rightarrow R'$

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

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

$R, R', R'' : \text{環}$

$f : R \rightarrow R' : \text{hom.}, g : R' \rightarrow R'' : \text{hom.} \Rightarrow g \circ f : R \rightarrow R'' : \text{hom.}$

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

$R, R' : \text{環}$

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

Exm. 1

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

Exm. 2

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

Exm. 3

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

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

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

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

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

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

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

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

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