

代数系入門
第3章 環と多項式

今村勇輝

May 12, 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

$R : \text{set}, R \neq \emptyset,$

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

1 $R : \text{加法について可換群}$

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

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

Def. 1.2

$R : \text{ring}$

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

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

Def. 1.3

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

Thm. 1.1

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

Def. 1.4

$$1 := e : R \text{ の単位元 (multiplicative identity)}$$

Exm. 1

$$\mathbb{Z} : \text{commutative ring} : \text{有理整数環 (ring of rational integers)}$$

Exm. 2

$$\mathbb{Q}, \mathbb{R}, \mathbb{C} : \text{commutative ring}$$

Exm. 3

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

Exm. 4

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

Def. 1.5

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

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

Def. 1.6

$\forall A : \text{additive group}, f : A \rightarrow A : \text{hom.} : \text{自己準同型 (endomorphism)}$
 $\text{End}(A) := \{f \mid f : A \rightarrow A : \text{hom.}\}$

Exm. 5

$\forall A : \text{additive group},$
 $f, g \in \text{End}(A), \forall x \in A, (f + g)(x) = f(x) + g(x), (fg)(x) = f(g(x)) \Rightarrow \text{End}(A) : \text{ring}$

Rem. $\text{End}(A) : \text{自己準同型環 (endomorphism ring)}$

Thm. 1.2

 R : ring

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

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

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

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

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

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

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

Def. 2.1

 $R : \text{ring}, 0, 1 \in R, 1 = 0 \stackrel{\text{def}}{\Leftrightarrow} R : \text{零環 (zero ring)}$

Rem. 今後, R は零環ではないとする.

Def. 2.2

 $R : \text{ring}, \exists a, b \in R \text{ s.t. } a \neq 0, b \neq 0, ab = 0 \stackrel{\text{def}}{\Leftrightarrow} a, b : R \text{ の零因子 (zero divisor)}$ $a : \text{左零因子 (left zero divisor)}, b : \text{右零因子 (right zero divisor)}$

Def. 2.3

 $R : \text{commutative ring}, \forall a, b \in R, a \neq 0, b \neq 0 \Rightarrow ab \neq 0 \stackrel{\text{def}}{\Leftrightarrow} R : \text{整域 (integral domain)}$

Exm. 1

 \mathbb{Z} : integral domain

Exm. 2

§1 Exm. 3 は整域ではない

Def. 2.4

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

Thm. 2.2

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

Lem. A

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

Exm. 3

$A : \text{additive group}, A \neq \{0\}$

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

Def. 2.5

$R : \text{ring}$

- $\forall a \in R, a \neq 0 \Rightarrow a : \text{unit} \stackrel{\text{def}}{\Leftrightarrow} R : \text{斜体 (skew field)}$
- $R : \text{skew field}, R : \text{commutative} \stackrel{\text{def}}{\Leftrightarrow} R : \text{体 (field)}$

Thm. 2.3

 R : ring

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

Exm. 4

- \mathbb{Z} : ring $\Rightarrow \mathbb{Z}$: field
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$: ring $\Rightarrow \mathbb{Q}, \mathbb{R}, \mathbb{C}$: field
 - \mathbb{Q} : 有理数体 (the field of rational numbers)
 - \mathbb{R} : 実数体 (the field of real numbers)
 - \mathbb{C} : 複素数体 (the field of complex numbers)

Thm. 2.4

 $\forall R : \text{field} \Rightarrow R : \text{integral domain}$

Lem. B

 $R : \text{integral domain}, |R| < \infty \Rightarrow R : \text{field}$

Def. 2.6

 $R : \text{ring}, R' \subset R, R' \neq \emptyset$ $R' : R$ 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 (subring)**

Thm. 2.5

 $R : \text{ring}, R' \subset R$ $R' : \text{subring of } R \Leftrightarrow 1_R \in R', \forall a, b \in R' \Rightarrow -a, a + b, ab \in R'$

Def. 2.7

 R' : subring of R

- R' : skew field $\stackrel{\text{def}}{\Leftrightarrow} R$ の部分斜体
- R' : field $\stackrel{\text{def}}{\Leftrightarrow} R$ の部分体 (subfield)

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)

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

Def. 2.8

R : skew field, $\forall a, b \in R \Rightarrow ab \neq ba \stackrel{\text{def}}{\Leftrightarrow} R$: 非可換体 (noncommutative field)

Exm. 7

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

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

$$2 \quad Q = \{f_{\alpha, \beta} \mid \text{上記 } f_{\alpha, \beta}\} \Rightarrow Q : \text{subring of } \text{End}(A)$$

$$3 \quad Q : \text{noncommutative ring}$$

Rem. $Q : \mathbb{R}$ 上の四元数環 (quaternion ring)

Thm. 2.6

R : integral domain or field $\Rightarrow \exists 0, 1 \in R$ 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

 $R : \text{ring}, J \subset R, J \neq \emptyset$

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

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

$\stackrel{\text{def}}{\Leftrightarrow} J \trianglelefteq_l R, J : R \text{ の左イデアル (left ideal)}$

Thm. 3.1

 $R : \text{ring}, J \subset R, J \neq \emptyset$ $J \trianglelefteq_l R \Leftrightarrow J \leq R : \text{additive subgroup}, \forall r \in R, \forall a \in J \Rightarrow ra \in J$

Def. 3.2

 $R : \text{ring}, J \leq R : \text{additive subgroup}, \forall r \in R, \forall a \in J \Rightarrow ar \in J$

$\stackrel{\text{def}}{\Leftrightarrow} J \trianglelefteq_r R, J : R \text{ の右イデアル (right ideal)}$

Def. 3.3

$$J \trianglelefteq_l R, J \trianglelefteq_r R$$

$\stackrel{\text{def}}{\Leftrightarrow} J \trianglelefteq R, J : R$ の **イデアル (ideal)** または **両側イデアル (two-sided ideal)**

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

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

$$c \in [0, 1], J_c = \{f \in R \mid f(c) = 0\} \Rightarrow J_c \trianglelefteq R$$

Exm. 2

$$n \in \mathbb{Z}, n \geq 0 \Rightarrow n\mathbb{Z} \trianglelefteq \mathbb{Z}$$

Exm. 3

 R : ring

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

Def. 3.4

 R : ring

- $a \in R, Ra(\text{または } (a)) := \{xa \mid x \in R\}$
 $: a$ によって生成される単項左イデアル (left principal ideal)
- $a_1, \dots, a_n \in R, (a_1, \dots, a_n) := \{x_1a_1 + \dots + x_na_n \mid x_1, \dots, x_n \in R\}$
 $: a_1, \dots, a_n$ によって生成される左イデアル

Thm. 3.2

$$\forall J \trianglelefteq_l R, a_1, \dots, a_n \in J \Rightarrow (a_1, \dots, a_n) \subset J$$

Thm. 3.3

 R : ring

- $1 \in R \Rightarrow (1) = R$
- $0 \in R \Rightarrow (0) = \{0\}$
- $R \trianglelefteq R, (0) \trianglelefteq R$

Def. 3.5

 $J \trianglelefteq R, J = \{0\} \stackrel{\text{def}}{\Leftrightarrow} 0 := J$: 零イデアル (zero ideal)

Thm. 1

 R : ring, $R \neq \emptyset$ R : skew field $\Leftrightarrow \forall J \trianglelefteq_l R \Rightarrow J = R \text{ or } 0$

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

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

Thm. 2

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

Def. 3.6

 $R/J : R$ の J による剰余環 (factor ring) または商環 (quotient ring)

Thm. 3.4

- 1 $R/J : \text{zero ring} \Leftrightarrow J = R$
- 2 $J = (0) \Rightarrow R/J \cong R$
- 3 $R : \text{commutative ring} \Rightarrow \forall R/J : \text{commutative}$

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

$n \geq 0, (n) := n\mathbb{Z}, (n) \trianglelefteq \mathbb{Z} (\because \text{\S 3 Exm. 2})$

$\forall J \trianglelefteq \mathbb{Z} \Leftrightarrow \exists n \in \mathbb{Z} \text{ s.t. } n \geq 0, J = (n)$

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

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

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

Thm. 3

$$n \geq 2$$

- $n = p : \text{prime} \Rightarrow \mathbb{Z}_p : \text{field}$
- $n : \text{not prime} \Rightarrow \exists \bar{a} \in \mathbb{Z}_n \text{ s.t. } \bar{a} : \text{zero divisor}$

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

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 : prime

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

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.

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

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

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

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

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

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

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

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

Exm. 4

 $R : \text{ring}, J \trianglelefteq R$ $\varphi : R \rightarrow R/J; a \mapsto \bar{a} \Rightarrow \varphi : \text{hom.}$

Def. 5.3

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

Thm. 5.2

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

Thm. 5.3

 $R, R' : \text{ring}$ $f : R \rightarrow R' : \text{hom.} \Rightarrow R' \supset f(R) : \text{ring}$

Def. 5.4

 $R, R' : \text{ring}, f : R \rightarrow R' : \text{hom.}$ $\text{Ker} f := f^{-1}(0) : f \text{ の核 (kernel)}$

Rem. $\text{Ker} f$ 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

 $R, R' : \text{ring}$ $f : R \rightarrow R' : \text{hom.} \Rightarrow \text{Ker} f \trianglelefteq R$

Thm. 5.5

 $R, R' : \text{ring}, f : R \rightarrow R' : \text{hom.}$ $R' \neq \{0\} \Rightarrow \text{Ker} f \neq R$

Exm. 5

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

Exm. 6

 $R : \text{ring}$ $\forall J \trianglelefteq R, f: R \rightarrow R/J : \text{hom.} \Rightarrow \text{Ker } f = J$

Thm. 5.6

$R : \text{skew field}, R' \neq \emptyset : \text{ring}, f : R \rightarrow R' : \text{hom.} \Rightarrow f : \text{mon.}$

Thm. 4 (環の準同型定理)

$R, R' : \text{ring}$

$f : R \rightarrow R' : \text{hom.}, \text{Ker } f = J \Rightarrow R/J \cong f(R)$

Thm. 5

$R, R' : \text{ring}, f : R \rightarrow R' : \text{epi.}, \text{Ker } f = J$

- $\Omega = \{M \mid M \trianglelefteq_l (\trianglelefteq_r) R, J \subset M\}, \Omega' = \{M' \mid M' \trianglelefteq_l (\trianglelefteq_r) R'\}$
 $\phi : \Omega \rightarrow \Omega'; M \mapsto f(M), \psi : \Omega' \rightarrow \Omega; M' \mapsto f^{-1}(M') \Rightarrow \phi, \psi : \text{bij.}, \phi^{-1} = \psi$
- $M \trianglelefteq R, M' \trianglelefteq R' \Rightarrow R/M \cong R'/M'$

Def. 5.5

$R : \text{ring}, J_L \trianglelefteq_l R, J_R \trianglelefteq_r R, J_L, J_R \neq R$

$\forall M \trianglelefteq_l (\trianglelefteq_r) R, J_L(J_R) \subset M \Rightarrow M = R \text{ or } J_L(J_R)$

$\stackrel{\text{def}}{\Leftrightarrow} J_L(J_R) : R \text{ の極大左 (右) イデアル (maximal left (right) ideal)}$

Thm. 5.7

$R : \text{ring}, J_L \trianglelefteq_l R : \text{maximal}, J_R \trianglelefteq_r R : \text{maximal}, J_L, J_R \neq R$

$R : \text{commutative} \Rightarrow J_L = J_R$

Def. 5.6

$R : \text{commutative ring}, J \trianglelefteq R, J \neq R$

$\forall M \trianglelefteq R, J \subset M \Rightarrow M = R \text{ or } J \stackrel{\text{def}}{\Leftrightarrow} J : R \text{ の極大イデアル (maximal ideal)}$

Thm. 6

 $R : \text{ring}, J \trianglelefteq R, J \neq R$ $R/J : \text{skew field} \Leftrightarrow J \trianglelefteq_l R : \text{maximal} \Leftrightarrow J \trianglelefteq_r R : \text{maximal}$

Cor. 6.1

 $R : \text{commutative ring}, J \trianglelefteq R, J \neq R$ $R/J : \text{field} \Leftrightarrow J \trianglelefteq R : \text{maximal}$

Lem. E

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

Thm. 5.8

$$R : \text{ring}, \mu : \mathbb{Z} \rightarrow R; n \mapsto n1_R$$

$$\forall R' \subset R : \text{subring} \Rightarrow \mu(\mathbb{Z}) \subset R'$$

Def. 5.7

$$\mu : \mathbb{Z} \rightarrow R; n \mapsto n1_R, \exists ! m \geq 0 \text{ s.t. } \text{Ker } \mu = (m)$$

$$\stackrel{\text{def}}{\Leftrightarrow} \text{Char}(R) := m : R \text{ の標数 (characteristic)}$$

Thm. 5.9

$$R : \text{ring}, \text{Char}(R) = m$$

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

Thm. 5.10

$R : \text{ring}, \text{Char}(R) = m$

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

Lem. F

$R : \text{integral domain}, \text{Char}(R) = m \Rightarrow m = 0 \text{ or } m : \text{prime}$

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. 6.1

$$R : \text{ring}, R \neq \{0\}, F : \text{field}, \exists f : R \rightarrow F : \text{mon.} \Rightarrow R : \text{integral domain}$$

Thm. 6.2

$$R, R' : \text{ring}, f : R \rightarrow R' : \text{mon.} \Rightarrow R \cong f(R)$$

これより, R を R' の部分環として考えることができる.

Def. 6.1

$$R, R' : \text{ring}$$

- $f : R \rightarrow R' : \text{mon.} : R$ から R' への埋め込み (embedding)
- $\exists f : R \rightarrow R' : \text{mon.} : R$ は R' (の中) に埋め込み可能

Def. 6.2

$$F : \text{field}, R \subset F : \text{subring}$$
$$a, b \in R, b \neq 0, ab^{-1} = b^{-1}a \stackrel{\text{def}}{\Leftrightarrow} a/b : a, b \text{ から作られる商または分数}$$

Thm. 6.3

 F : field, $R \subset F$: subring

$$\forall a, b, a', b' \in R, a/b = a'/b' \Leftrightarrow ab' = a'b$$

Lem. G

 F : field, $R \subset F$: subring

- $L := \{a/b \mid a, b \in R, b \neq 0\} \Rightarrow L \subset F$: subfield
- $\forall L' \subset F$: subfield, $R \subset L' \Rightarrow L \subset L'$

Def. 6.3

 F : field, $R \subset F$: subring L : R の (F における) 商の体 (field of quotients) または分数体 (fraction field)

Rem. 商体 (quotient field) と呼ばれることもあるが, §3 の商環と概念上まぎらわしいため, 本書では上記のような語を用いる.

Def. 6.4

R : integral domain, $R^* = \{a \in R \mid a \neq 0\}$

$(a, b), (a', b') \in R \times R^*, ab' = a'b \stackrel{\text{def}}{\Leftrightarrow} (a, b) \sim (a', b')$

Thm. 6.4

$\sim : R \times R^*$ における同値関係

Def. 6.5

$[a, b] := \{(a', b') \in R \times R^* \mid (a, b) \sim (a', b')\}$

$K := \{[a, b] \mid a \in R, b \in R^*\}$

Thm. 6.5

$\forall [a, b], [a', b'] \in K, [a, b] = [a', b'] \Leftrightarrow ab' = a'b$

Thm. 6.6

$\forall [a, b], [c, d] \in K, [a, b] + [c, d] = [ad + bc, bd], [a, b][c, d] = [ac, bd] \Rightarrow K : \text{field}$

Thm. 7

R : integral domain $\Rightarrow \exists K$: field, $\varphi : R \rightarrow K$: hom. s.t.

1 φ : embedding

2 $\forall k \in K, \exists a, b \in R$ s.t. $b \neq 0, k = \varphi(a)/\varphi(b)$

Def. 6.6

K : ($\varphi : R \rightarrow K$ と合わせて) R の商の体または分数体

Thm. 6.7

F : field, $R \subset F$: subring $\Rightarrow L \cong K$ (ただし L : Def.6.3, K : Def.6.6)

Rem. 以後, $a \in R$ と $\varphi(a) \in K$ とを同一視することにする.

そうすれば, $R \subset K, \forall k \in K, \exists a, b \in R, b \neq 0, k = a/b$

Def. 6.7

 R : integral domain

$$\text{Frac}(R) := \{a/b \mid a, b \in R, b \neq 0\}$$

Exm. 6.1

$$\mathbb{Q} := \text{Frac}(\mathbb{Z})$$

Lem. H

 R : integral domain, E : field, $f: R \rightarrow E$: embedding, $K = \text{Frac}(R)$ $\Rightarrow \exists ! f^*$ s.t. $f^*: K \rightarrow E$: embedding, $f = f^*|_R$ Rem. Lem. H は Lem. G をより精密にしたもの.

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. 7.1

 $a_0, \dots, a_m \in \mathbb{R}, x : \text{variable}$ $a_0 + a_1x + \dots + a_mx^m : \text{多項式 (polynomial)}$

Def. 7.2

 $a_0, \dots, a_m \in \mathbb{R}, x : \text{variable}$ $f: \mathbb{R} \rightarrow \mathbb{R}; x \mapsto a_0 + a_1x + \dots + a_mx^m : \text{多項式写像 or 多項式関数}$

Def. 7.3

 $R : \text{commutative ring}, R \neq 0$ $\tilde{P} := \{f \mid f: \mathbb{N} \rightarrow R\}, a_n := f\{n\}$

Thm. 7.1

 $f \in \tilde{P} \Rightarrow f = (a_0, a_1, a_2, \dots)$

Rem. $f = (a_0, a_1, a_2, \dots)$ は簡単に $(a_n)_{n \geq 0}$, 略して (a_n) とも表す.

Thm. 7.2

$$\begin{aligned} \forall f, g \in \tilde{P}, f &= (a_n), g = (b_n) \\ f + g &= (a_n + b_n), fg = \sum_{i+j=n} a_i b_j \Rightarrow \tilde{P} : \text{commutative ring} \end{aligned}$$

Rem. \tilde{P} と $M(\mathbb{N}, R)$ は集合として同じで加法の定義も同じだが, 乗法の定義は異なっている.

Def. 7.4

- $\forall a \in R, \bar{a} : \mathbb{N} \rightarrow R; \bar{a}\{0\} = a, \bar{a}\{n\} = 0 \ (n \neq 0)$
- $x : \mathbb{N} \rightarrow R; x\{1\} = 1, x\{n\} = 0 \ (n \neq 1)$

Rem. $\bar{a} = (a, 0, 0, 0, \dots), x = (0, 1, 0, 0, \dots)$

Thm. 7.3

- $x^i : \mathbb{N} \rightarrow R; x^i\{i\} = 1, x^i\{n\} = 0 \ (n \neq i)$
- $\bar{a}x^i : \mathbb{N} \rightarrow R; \bar{a}x^i\{i\} = a, \bar{a}x^i\{n\} = 0 \ (n \neq i)$

Def. 7.5

$$P := \{f \in \tilde{P} \mid \exists N \in \mathbb{N} \text{ s.t. } \forall k \in \mathbb{N}, k > N, a_k = 0\}$$

Thm. 7.4

- $P \subset \tilde{P}$: subring
- $\forall f \in P, f = (a_0, \dots, a_m, 0, \dots) \Rightarrow f = \bar{a}_0 + \bar{a}_1 x + \dots + \bar{a}_m x^m$
- $\phi: R \rightarrow P; a \mapsto \bar{a}$: embedding

Thm. 7.5

$$\forall f \in P \Rightarrow \exists! a_0, \dots, a_m \in R \text{ s.t. } f = a_0 + a_1 x + \dots + a_m x^m$$

Def. 7.6

- $R[x] := P : R$ 上の多項式環 (polynomial ring)
- $f \in R[x]$: 多項式, R : 係数環, x : 変数 or 不定元 (indeterminate)

Def. 7.7

 $f \in R[x]$

- $f(x) = a_0 + a_1x + \cdots + a_mx^m, a_m \neq 0 \stackrel{\text{def}}{\Leftrightarrow} \deg f := m : f \text{ の次数 (degree)}$
- $\deg 0 = -\infty, \forall m \in \mathbb{N}, -\infty < m$
- $\deg f = 0 \text{ or } -\infty \stackrel{\text{def}}{\Leftrightarrow} f : \text{定数 (constant)}$

Thm. 7.6

 $f \in R[x] : \text{constant} \Rightarrow f \in R$

Def. 7.8

 $f \in R[x], f(x) = a_0 + a_1x + \cdots + a_mx^m$

- $a_mx^m : \text{主項}, a_m : \text{主係数}$
- $a_m = 1 \stackrel{\text{def}}{\Leftrightarrow} f : \text{モニック (monic)}$

Thm. 7.7

$f, g \in R[x] \Rightarrow \deg(fg) \leq \deg f + \deg g$, R : integral domain のとき等号成立

Lem. 1

R : integral domain $\Rightarrow R[x]$: integral domain

Def. 7.9

R : 可換環, $R_1 \supset R$: 拡大可換環, $c \in R_1, R[x] \ni f(x) = a_0 + a_1x + \cdots + a_mx^m$
 $R_1 \ni f(c) := a_0 + a_1c + \cdots + a_mc^m$: x に c を代入 (substitute) した元

Thm. 7.8

$\Phi: R[x] \rightarrow R_1; f \mapsto f(c)$: hom.

Thm. 7.9

$\forall R' \subset R_1$: subring, $\forall r \in R, r \in R', c \in R' \Rightarrow R[c] \subset R'$

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