代数系入門

第 3 章 環と多項式

今村勇輝

March 1, 2022

Def. 1.1

R : set, $R \neq \emptyset$,
$R \times R \longrightarrow R, (a,b) \mapsto a+b, (a,b) \mapsto ab$

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: ring

- $\exists! e_+ \in R$ s.t. $\forall a \in R, e_+ + a = a \overset{\text{def}}{\Leftrightarrow} 0 := e_+$: R の零元 (additive identity)
- $\forall a \in R, \exists! a' \in R$ s.t. $a + a' = 0 \overset{\text{def}}{\Leftrightarrow} -a := a'$

Def. 1.3

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

Thm. 1.1

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

Def. 1.4

$1 := e : R$ の**単位元** (multiplcative identity)

Exm. 1

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

Exm. 2

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

Exm. 3

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

Exm. 4

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

Def. 1.5

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

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

Def. 1.6

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

Exm. 5

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

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

Thm. 1.2

R : ring

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

Def. 2.1

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

Rem. 今後, R は零環ではないとする.

Def. 2.2

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

Def. 2.3

R : commutative ring, $\forall a, b \in R, a \neq 0, b \neq 0 \Rightarrow ab \neq 0 \overset{\text{def}}{\Leftrightarrow} R$: 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. $ba = ab = 1$
$\overset{\text{def}}{\Leftrightarrow}$ $a : R$ の**可逆元**または**単元** (unit), $a^{-1} := b : a$ の**逆元** (inverse)

Thm. 2.2

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

Lem. A

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

Exm. 3

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

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

Def. 2.5

R : ring

- $\forall a \in R, a \neq 0 \Rightarrow a : \text{unit} \overset{\text{def}}{\Leftrightarrow} R$: **斜体 (skew field)**
- R : skew field, R : commutative $\overset{\text{def}}{\Leftrightarrow} R$: **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 $\not\Rightarrow \mathbb{Z}$: 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

$\forall R$: field $\Rightarrow R$: integral domain

Lem. B

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

Def. 2.6

R : 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, $1_R \in R'$
$\overset{\text{def}}{\Leftrightarrow} R'$: R の**部分環 (subring)**

Thm. 2.5

R : ring, $R' \subset R$
R' : 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 $\overset{\text{def}}{\Leftrightarrow}$ R の**部分斜体**
- R' : field $\overset{\text{def}}{\Leftrightarrow}$ 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

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

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

Def. 2.8

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

Exm. 7

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

1. $\alpha, \beta \in \mathbb{C}, f_{\alpha,\beta} : A \to A; (x, y) \mapsto (\alpha x - \beta y, \bar{\beta} x + \bar{\alpha} y) \Rightarrow f_{\alpha,\beta} \in \mathrm{End}(A)$
2. $Q = \{f_{\alpha,\beta} \mid$ 上記 $f_{\alpha,\beta}\} \Rightarrow Q$: subring of $\mathrm{End}(A)$
3. Q : 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. $0 \neq 1$

Def. 3.1

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

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

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

Thm. 3.1

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

$J \trianglelefteq_l R \Leftrightarrow J \leq R$: additive subgroup, $\forall r \in R, \forall a \in J \Rightarrow ra \in J$

Def. 3.2

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

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

Def. 3.3

$J \trianglelefteq_l R, J \trianglelefteq_r R$
$\overset{\text{def}}{\Leftrightarrow} J \trianglelefteq R, J : R$ の**イデアル** (ideal) または**両側イデアル** (tow-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

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

Exm. 2

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

Exm. 3

R : ring

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

Def. 3.4

R : ring

- $a \in R, Ra$(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 (left principal ideal)
- $a_1, \cdots, a_n \in R, (a_1, \cdots, a_n) := \{x_1a_1 + \cdots + x_na_n \mid x_1, \cdots, x_n \in R\}$
  : $a_1, \cdots, a_n$ によって生成される左イデアル

Thm. 3.2

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

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

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

Thm. 1

R : ring, $R \neq \emptyset$

R : skew field $\Leftrightarrow \forall J \trianglelefteq_l R \Rightarrow J = R$ 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 : 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 : ring, $J \trianglelefteq R, R/J \ni \bar{a} := a + J$
$\bar{a}, \bar{b} \in R/J, \bar{a} + \bar{b} = \overline{a+b},\ \bar{a}\bar{b} = \overline{ab} \Rightarrow R/J$: 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 : zero ring $\Leftrightarrow J = R$
2. $J = (0) \Rightarrow R/J \cong R$
3. R : commutative ring $\Rightarrow \forall R/J$: commutative

本節では特に有理数環 $\mathbb{Z}$ について考える.

Thm. 4.1

$n \geq 0, (n) := n\mathbb{Z}, (n) \trianglelefteq \mathbb{Z}$ ($\because$ §3 Exm. 2)
$\forall J \trianglelefteq \mathbb{Z} \Leftrightarrow \exists n \in \mathbb{Z}$ 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
- $(a, n) \neq 1 \Rightarrow \bar{a}$: zero divisor

Thm. 3

$n \geq 2$

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

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

Def. 5.1

R, R' : ring, $f : R \to R'$

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

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

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

Exm. 1

$R = \{f \mid f\colon [0,1] \to [0,1]$: 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

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

Exm. 4

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

Def. 5.3

$\varphi\colon R \longrightarrow R/J; a \mapsto \bar{a}$: 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' : ring
$f\colon R \longrightarrow R'$: hom. $\Rightarrow f(0_R) = 0_{R'}, f(-x) = -f(x)$

Thm. 5.3

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

Def. 5.4

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

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' : ring
$f : R \longrightarrow R'$: hom. $\Rightarrow \mathrm{Ker} f \trianglelefteq R$

Thm. 5.5

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

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) $\Rightarrow \operatorname{Ker} F = J_c$

Exm. 6

R : ring
$\forall J \trianglelefteq R, f\colon R \to R/J$: hom. $\Rightarrow \operatorname{Ker} f = J$

Thm. 5.6

R : skew field, $R' \neq \emptyset$: ring, $f\colon R \to R'$: hom. $\Rightarrow f$: mon.

Thm. 4 (環の準同型定理)

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

Thm. 5

R, R' : ring, $f\colon R \to R'$: epi., $\mathrm{Ker} f = J$

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

Def. 5.5

R : ring, $J_L \trianglelefteq_l R, J_R \trianglelefteq_r R,\ J_L, J_R \neq R$
$\forall M \trianglelefteq_l (\trianglelefteq_r)R,\ J_L(J_R) \subset M \Rightarrow M = R$ or $J_L(J_R)$
$\overset{\text{def}}{\Leftrightarrow} J_L(J_R)$: R の**極大左 (右) イデアル (maximal left (right) ideal)**

Thm. 5.7

R : ring, $J_L \trianglelefteq_l R$: maximal, $J_R \trianglelefteq_r R$: maximal, $J_L, J_R \neq R$
R : commutative $\Rightarrow J_L = J_R$

Def. 5.6

R : commutative ring, $J \trianglelefteq R,\ J \neq R$
$\forall M \trianglelefteq R,\ J \subset M \Rightarrow M = R$ or $J \overset{\text{def}}{\Leftrightarrow} J$: R の**極大イデアル (maximal ideal)**

Thm. 6

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

Cor. 6.1

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

Lem. E

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

Thm. 5.8

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

Def. 5.7

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

Thm. 5.9

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

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

Thm. 5.10

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

- $R = \{0\} \Leftrightarrow m = 1$
- $R \neq \{0\} \Rightarrow m = 0$ 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, $\mathrm{Char}(R) = m \Rightarrow m = 0$ or m : prime

Thm. 6.1

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

Thm. 6.2

R, R' : ring, $f : R \to R'$: mon. $\Rightarrow R \cong f(R)$

Def. 6.1

R, R' : ring

- $f : R \to R'$: mon. : R から R' への**埋め込み (embedding)**
- $\exists f : R \to R'$: mon. : R は R'(の中) に**埋め込み可能**

Def. 6.2

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

$a, b \in R, b \neq 0, ab^{-1} = b^{-1}a \overset{\text{def}}{\Leftrightarrow} a/b$: a, b 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

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

Def. 6.3

F : field, $R \subset F$: subring
$\mathrm{Frac}(R)$: 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, $R^* = \{a \in R \mid a \neq 0\}$

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

Thm. 6.4

$\sim : R \times R^*$ における同値関係

Def. 6.5

$[a,b] \coloneqq \{(a',b') \in R \times R' \mid (a,b) \sim (a',b')\}$

$K \coloneqq \{[a,b] \mid a,b \in R\}$

Thm. 6.5

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

Thm. 6.6

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

Thm. 7

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

1. φ : R の K への埋め込み
2. $\forall k \in K, \exists a, b \in R$ s.t. $b \neq 0, k = \varphi(a)/\varphi(b)$

Def. 6.6

K : ($\varphi\colon R \to K$ と合わせて)R の**商の体**または**分数体**

Thm. 6.7

F : field, K : fraction field
$R \subset F$: subring $\Rightarrow \mathrm{Frac}(R) \cong K$

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

Exm. 6.1

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

Lem. H

R : integral domain, E : field, $f : R \longrightarrow E$: embedding, $K = \mathrm{Frac}(R)$
$\Rightarrow \exists! f^*$ s.t. $f^* : K \longrightarrow E$: embedding, $f = f^*|_R$

Rem. Lem. H は Lem. G をより精密にしたもの.

Def. 7.1

$a_0, \cdots, a_m \in \mathbb{R}, x \in \mathbb{R}$: variable
$x \mapsto a_0 + a_1 x + \cdots + a_m x^m$: 多項式写像または多項式関数 (polynomial function)

Def. 7.2

R : commutative ring, $R \neq 0$, $\tilde{P} := \{f \mid f : \mathbb{N} \to R\}$
$f \in \tilde{P}, f\{n\} = a_n, f = (a_0, a_1, a_2, \cdots) = (a_n)_{n \geq 0} = (a_n)$

Rem. 後に用いる $f(x)$ などの表記と区別するため $f\{n\}$ とかく.

Thm. 7.1

$\forall f, g \in \tilde{P}, f = (a_n), g = (b_n)$

$$f + g = (a_n + b_n),\ fg = \sum_{i=0}^{n} a_i b_{n-i} \Rightarrow \tilde{P} : \text{commutative ring}$$

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. 7.3

- $\forall a \in R,\ \bar{a} \colon \mathbb{N} \longrightarrow R, \bar{a}\{0\} = n, \bar{a}\{n\} = 0\ (n \neq 0), \bar{a} = (a, 0, 0, 0, \cdots)$
- $x \colon \mathbb{N} \longrightarrow R, x\{1\} = 1, x\{n\} = 0\ (n \neq 1), x = (0, 1, 0, 0, \cdots)$

Thm. 7.2

- $x^i\{i\} = 1, x^i\{n\} = 0\ (n \neq i)$
- $\bar{a}x^i\{i\} = a, \bar{a}x^i\{n\} = 0\ (n \neq i)$

Def. 7.4

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

Thm. 7.3

- $P \subset \tilde{P}$: subring
- $\forall f \in P, f = (a_0, \cdots, a_m, 0, \cdots) \Rightarrow f = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_m x^m$