Contents

1 環の定義

Definition 1.1. 環
$R \neq \emptyset$ とする．R は環である $\iff$ R にそれぞれ和と積と呼ばれる演算，$+ : R \times R \to R, \cdot : R \times R \to R$ が定義されていて，以下の条件をみたす．ただし，$a \cdot b = ab$ とかく

$(R1)$ R は和について可換群である．すなわち以下の条件をみたす

- $(G1)$ $\forall a, b, c \in R, (a + b) + c = a + (b + c)$
- $(G2)$ $\exists 0 \in R, \forall a \in R, a + 0 = 0 + a = a$
- $(G3)$ $\forall a \in R, \exists x \in R, a + x = x + a = 0$
- $(G4)$ $\forall a, b \in R, a + b = b + a$

$(R2)$ $\forall a, b, c \in R, (ab)\, c = a\, (bc)$

$(R3)$ $\forall a, b, c \in R, a\, (b + c) = ab + ac, (b + c)\, a = ba + ca$

$(R4)$ $\forall a, b \in R, a + b = b + a$

Remark 1.2. R を環とする．このとき，単位元 $e = 0$ なら $R = \{0\}$ となり，零環または自明な環と呼ばれる．一般の場合では，環は自明な環でないとする

Example 1.3. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は通常の和と積について環になる

Definition 1.4. 可換環・単元
R を環とする

1. R：可換環 $\iff$ $\forall a, b \in R, ab = ba$
2. $a \in R$：単元もしくは可逆元 $\iff$ $\exists b \in R, ab = ba = 1$．このとき b を a の逆元といい，a^{-1} で表す

Definition 1.5. 体
R を可換環とする $\iff$ $\forall a \in R \backslash \{0\}$ に対して a は単元

2　部分環・多項式環

Definition 2.1. 零因子・整域
R を可換環とする

1. $a \in R$ は零因子 $\iff \exists b \in \mathbb{R}\setminus\{0\}, s.t. ab = 0$
2. R は整域 $\iff \forall a, b \in R, ab = 0$ ならば $a = 0$ または $b = 0$（零因子は 0 のみ）

Example 2.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は整域である

Definition 2.3. 部分環
R を環とし，R' を R の空でない部分集合とする．R' は R の部分環 $\iff$ R' は以下の条件をみたす

1. R' は R の和と積について環である
2. R の単位元 $e_R \in R'$

Example 2.4. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ は全て部分環である

Proposition 2.5. R を環とし，R' を R の部分集合とする．R' は R の部分環 $\iff$ R' は以下の条件をみたす

1. $a, b \in R' \Longrightarrow a - b \in R'$
2. $a, b \in R' \Longrightarrow ab \in R'$
3. $e_R \in R'$

Definition 2.6. 多項式・多項式環・次数・根
R を可換環とする．R の元を係数とする文字 x の式

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, (a_i \in R) \tag{1}$$

を R を係数とする x の多項式（または R 上の x の多項式）という．x は変数（または不定元）と呼ばれる．R を係数とする x の多項式全体の集合を $R[x]$ とかく．$R[x]$ の元

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad g(x) = \sum_{j=0}^{m} b_j x^j \tag{2}$$

に対して，和と積を

$$f(x) + g(x) = \sum_{i=0}^{l} (a_i + b_i) x^i \qquad f(x) g(x) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k \tag{3}$$

と定める．ただし，$l := \max\{m, n\}$ とする．また，例えば $n > m$ のときは $b_{m+1} = \cdots = b_l = 0$ とする．この和と積により $R[x]$ は環になる．$R[x]$ を R 上の多項式環という．多項式

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \qquad (a_i \in R) \tag{4}$$

に対して，$a_n \neq 0$ のとき，$\deg f(x) = n$ と定め f の次数という．$f(x) = 0$ のとき，$\deg f(x) = -\infty$ とし，任意の $m \in \mathbb{Z}_{\geq 0}$ に対し $-\infty < m$ であるとする．次数が 0 の多項式を定数という
$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x], c \in R$ に対し

$$f(c) = a_0 + a_1 c + \cdots + a_n c^n \tag{5}$$

と定め，$f(x)$ の x を代入した元とよび，$f(\alpha) = 0$ となるとき $\alpha \in R$ を $f(x)$ の根という

Proposition 2.7. R を整域とする．$0 \neq f(x), g(x) \in R[x]$ に対し，以下は成立する

- $\deg(f(x)+g(x)) \max\{\deg f(x), \deg g(x)\}$
- $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$

Theorem 2.8. 除法の定理
R を整域とする．$f(x), g(x) \in R[x]$ に対し，$g(x)$ の最高次の係数が単元なら

$$f(x) = g(x)q(x) + r(x) \qquad \deg r(x) < \deg g(x) \tag{6}$$

となる多項式の組 $q(x), r(x) \in R[x]$

Proposition 2.9. 剰余の定理
R を整域とする．$f(x) \in R[x], \alpha \in R$ に対し，$q(x) \in R[x]$ が存在して

$$f(x) = (x-\alpha)q(x) + f(\alpha) \tag{7}$$

となる．特に，$f(x)$ が $x-\alpha$ で割り切れることの必要十分条件は $f(\alpha) = 0$ である

Corollary 2.10. R を整域とする．$0 \neq f(x) \in R[x]$ に対し，$n = \deg f(x)$ とする．このとき，$f(x)$ の異なる根の個数は n 以下である

3　剰余群の復習

自然数 n に対し，$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$ とおく．$\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ に対して，和と積を

$$\overline{a} + \overline{b} = \overline{x} \tag{8}$$

$$\overline{a}\overline{b} = y \tag{9}$$

と定義すると，$\mathbb{Z}/n\mathbb{Z}$ は環になる
$n\mathbb{Z}$ は加法に関して $\mathbb{Z}$ の正規部分群である．したがって，剰余群 $\mathbb{Z}/n\mathbb{Z}$ を考えることができ

$$\mathbb{Z}/\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \cdots, (n-1) + n\mathbb{Z}\} \tag{10}$$

である，和は

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} \tag{11}$$

であり，積を

$$(a + n\mathbb{Z})\,(b + n\mathbb{Z}) = ab + n\mathbb{Z} \tag{12}$$

と定義することができる．この和と積により $\mathbb{Z}/n\mathbb{Z}$ は環になる．$a + n\mathbb{Z} = \overline{a}$ と書くことがある

Proposition 3.1. $a, b \in \mathbb{Z}$ に対し，$au + bv = (a, b)$ となる $u, v \in \mathbb{Z}$ が存在する

Proposition 3.2. $(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$

Proposition 3.3. p を素数とすると，$\mathbb{Z}/p\mathbb{Z}$ は体である

4 イデアル

Definition 4.1. イデアル
R を環，I を R の空でない部分集合とする

- I が左イデアル $\iff$ I は以下の条件をみたす
  1. $a, b \in I \Longrightarrow a+b \in I$
  2. $a \in I, r \in R \Longrightarrow ra \in I$
- I が右イデアル $\iff$ I は以下の条件をみたす
  1. $a, b \in I \Longrightarrow a+b \in I$
  2. $a \in I, r \in R \Longrightarrow ar \in I$
- I が両側イデアル $\iff$ I は左イデアルかつ右イデアル

Proposition 4.2. R を環，I, J を左（右，両側）イデアルとする．$I \cap J$ は左（右，両側）イデアルになる

Definition 4.3. R を環，I, J を左（右，両側）イデアルとする

- $I+J = \{x+y : x \in I, y \in J\}$ と定める．$I+J$ は左（右，両側）イデアルになる
- $IJ = \left\{ \sum_{i=1}^{n} x_i y_i \middle| x_i \in I, y_i \in J, n \in \mathbb{N} \right\}$ と定める．IJ は左（右，両側）イデアルになる

Definition 4.4. 生成された R の左イデアル・単項左イデアル
R を環，$x_1, x_2, \cdots, x_n \in R$ とする

$$(x_1, \cdots, x_n) = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : a_i \in R\} \tag{13}$$

と定めると，$(x_1, \cdots, x_n)$ は $x_1, \cdots, x_n$ を含む最小の R の左イデアルとなる．これを $x_1, \cdots, x_n$ で生成された R の左イデアルという
$x \in R$ に対し，x で生成された R の左イデアル $Rx = \{ax : a \in R\}$ を x で生成された単項左イデアルという．$Rx = (x)$ と書くこともある

Definition 4.5. 単項イデアル環・単項イデアル整域
単位元を持つ可換環 R の全てのイデアルが単項イデアルであるとき，R を単項イデアル環という．整域 R の全てのイデアルが単項イデアルであるとき，R を単項イデアル整域という

Definition 4.6. R を環，I を R の両側イデアルとする．加法に関して I は R の正規部分群なので，剰余群 R/I を考えることができる．$a+I, b+I \in R/I$ に対して，和と積を

$$(a+I)+(b+I) = (a+b)+I \tag{14}$$
$$(a+I)(b+I) = ab+I \tag{15}$$

と定義すると，R/I は環になる．これを R の I による剰余環という．また，R/I の単位元は $1+I$ で，零元は $0+I$ である

5　準同型写像

Definition 5.1. 準同型写像
R, R' を環，$f : R \to R'$ を写像とする．$f : R \to R'$：（環）準同型写像 $\iff$ f は以下の条件をみたす

1. $f(a+b) = f(a) + f(b), \forall a, b \in R$
2. $f(ab) = f(a) f(b), \forall a, b \in R$
3. $f(1_R) = 1_{R'}$

環準同型 $f : R \to R'$ は同型 $\iff$ f : 全単射
R から R' への同型が存在するとき，R と R' は同型であるといい，$R \cong R'$ と書く

Definition 5.2. 核・像
$f : R \to R'$ を環準同型写像とすると，f の核と像は次のように定める

1. $\mathrm{Ker} f = \{a \in R : f(a) = 0\}$
2. $\mathrm{Im} f = \{f(a) : a \in R\}$

Proposition 5.3. $f : R \to R'$ を環準同型写像とする．このとき，$\mathrm{Ker} f$ は R イデアルである

Proof. $\forall x, y \in \mathrm{Ker} f, f(x+y) = f(x) + f(y) = 0 + 0 = 0$ なので，$x + y \in \mathrm{Ker} f$ である．また，$\forall r \in R, x \in \mathrm{Ker} f, f(rx) = f(r) f(x) = f(r) 0 = 0$ であり，$f(xr) = f(x) f(r) = 0 f(r) = 0$ である．よって，$\mathrm{Ker} f$ は R のイデアルである □

Proposition 5.4. $f : R \to R'$ が環準同型写像であるとき，以下は成立する

$$f \text{ 単射} \iff \mathrm{Ker} f = \{0\}$$

Theorem 5.5. 準同型定理
$f : R \to R'$ を環準同型写像とする．このとき，$R/\mathrm{Ker} f \cong \mathrm{Im} f$

6 剰余環

Definition 6.1. I を環 R のイデアルとする

$$R/I := \{x + I : x \in R\} \tag{16}$$
$$= R/\equiv_I \tag{17}$$

剰余環 R/I では，剰余群と同じように以下のように定義できる

- $(a + I) + (b + I) = (a + b) + I$
- $(a + I)(b + I) = ab + I$
- $0_{R/I} = 0_R + I$
- $1_{R/I} = 1_R + I$

このように得られた環 R/I は R の I による剰余環と呼ばれる. また, $q : R \to R/I, x \mapsto x+I$ を商写像といい, q は準同型写像であるから, q は商準同型写像とも呼ばれる. $x+I = I \iff x \in I$ から，$\mathrm{Ker} q = I$ である

7　直積

Definition 7.1. 直積
$R_1, R_2, \cdots, R_n$ を環とする

$$R = R_1 \times R_2 \times \cdots \times R_n = \{(a_1, a_2, \cdots, a_n) : a_i \in R_i\} \tag{18}$$

に対して，和と積を

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n) \tag{19}$$
$$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n) \tag{20}$$

と定めると，R は環になる．R を $R_1, R_2, \cdots, R_n$ の直積という．この環の単位元 1_R，零元 0_R は

$$1_R = (1_{R_1}, 1_{R_2}, \cdots, 1_{R_n}) \tag{21}$$
$$0_R = (0_{R_1}, 0_{R_2}, \cdots, 0_{R_n}) \tag{22}$$

である

Theorem 7.2. R を環として，$I_1, I_2, \cdots, I_n$ をどの二つも互いに素な R の両側イデアルとする．このとき，環同型

$$R/\bigcap_{i=1}^{n} I_i \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n \tag{23}$$

が存在する

8 素イデアル・極大イデアル

Definition 8.1. 素イデアル
R を可換環，P を R のイデアルで，$P \neq R$ とする

$$P : \text{素イデアル} \overset{def}{\iff} ab \in P \Longrightarrow a \in P \text{ または } b \in P$$

Proposition 8.2. R を可換環，P を R のイデアルで，$P \neq R$ とする

$$P : \text{素イデアル} \iff R/P \text{ は整域}$$

Proof.
P を素イデアルとすると，$\forall a+P, b+P \in R/P, (a+P)(b+P) = 0$ ならば，$(a+P)(b+P) = ab+P = P$ で，P は素イデアルであるから，$a \in P$ または $b \in P$．逆に，R/P が整域であるとすると，$a \cdot b \in P \iff (a+P)(b+P) = 0$ となる．$a+p=0$ と仮定すると，$a \in P$．よって，P は素イデアルである □

Definition 8.3. 極大イデアル
R を可換環，I を R のイデアルで $I \neq R$ とする

$$I : \text{極大イデアル} \overset{def}{\iff} I \text{ を含むイデアルは } I \text{ と } R \text{ のみ}$$

Theorem 8.4. R を可換環，I を R のイデアルで $I \neq R$ とする

$$I : \text{極大イデアル} \iff R/I \text{ は体}$$

Corollary 8.5. R を可換環，I を R のイデアルで $I \neq R$ とする

$$I : \text{極大イデアル} \Longrightarrow I : \text{素イデアル}$$

Theorem 8.6. R を可換環，I を R のイデアルで $I \neq R$ とする．このとき，I を含む R の極大イデアルが存在する

Proof.
$\mathcal{J} = \{J \supset I, J : ideal, J \neq R\}$ とし，$J_1 \preccurlyeq J_2 \overset{def}{\iff} J_1 \subset J_2$ とする．このとき，$\forall S \subset \mathcal{J}, J_* = \bigcup_{J \in S} J$ とする．$\forall x, y \in J_*, \exists J_1, J_2 \in S, s.t. x \in J_1, y \in J_2$．すると，$J_1 \supset J_2$ とおくと，$x, y \in J_1$ で，$x \pm y \in J_1 \subset J$ から，J_* は R の部分群である．また，$\forall r \in R, rx \in J_1 \subset J_*$ から，J_* はイデアルである．$\forall J \in S, 1 \notin J$ から，$1 \notin J_*$ で，$J_* \neq R$ となる．従って，$J_* \in \mathcal{J}$ で，定義より，J_* は S の上界であり，Zorn の補題より，$\mathcal{J}$ には極大元が存在する．これが I を含む極大イデアルである □

R を交換環とし，$I_1, I_2, \cdots, I_n \subset R$ をイデアルとする．このとき

$$\pi : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n \tag{24}$$
$$x \mapsto (\pi_1(x), \pi_2(x), \cdots, \pi_n(x)) \tag{25}$$

は自然に環の準同型になり，$\pi_i : A \to A/I_i$ は商写像であり，$\mathrm{Ker}\pi = \bigcap_{i=1}^{n} I_i$ である

Definition 8.7. 互いに素なイデアル
R を交換環とし，$I, J \subset R$ をイデアルとする．$I+J=R$ であれば，I と J は互いに素であるという．言い換えれば，I と J は互いに素である $\iff 1 \in I+J$

Lemma 8.8. R を交換環とし，$n \geq 2, I_1, \cdots, I_n \subset R$ をイデアルとする．このとき，$\bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i$ である．さらに，$\pi : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$ が全射で，次の同型が成り立つ

$$R/(I_1 \cdot I_2 \cdot \cdots \cdot I_n) \cong R/(I_1 \cap I_2 \cap \cdots \cap I_n) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n \tag{26}$$

Corollary 8.9. $n_1, \cdots, n_k$ を互いに素な自然数とし，$n = n_1 \cdots n_k$ とする．このとき，以下の同型が成り立つ

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \tag{27}$$

Proposition 8.10. $\phi : A \to B$ を環の準同型とする．$Q \subset B$ を素イデアル，$P = \phi^{-1}(Q)$ とするとき，以下は成り立つ

1. A/P は B/Q の部分環とみなせる
2. $P = \phi^{-1}(Q) \subset A$ は素イデアルである

Proof. 1. $\pi : B \to B/Q$ を自然な準同型とすると，$\pi \circ \phi : A \to B/Q$ の核は $\phi^{-1}(\mathrm{Ker}(\pi)) = \phi^{-1}(Q) = P$ である．従って，準同型定理より，A/P は $\mathrm{Im}(\pi \circ \phi) \subset B/Q$ と同型である

2. Q が素イデアルなので，B/Q は整域である．よって，A/P も整域となり，P は素イデアルである

□

Proposition 8.11. R を環, $P \subset R$ を素イデアルとする. $R[X] = R[x_1, x_2, \cdots, x_n]$ を R 上の n 変数多項式環とするとき, $PR[X]$ は $R[X]$ の素イデアルであり, $R[X]/(PR[X]) \cong (R/P)[X]$ である

Proposition 8.12. $I \subset P$ を環 R のイデアルとする．このとき，P が R の素イデアルであることと，P/I が R/I の素イデアルであることは同値である

9　一意分解整域 UFD

Definition 9.1. 倍元・約元・同伴
R を整域とする．$a, b \in R$ に対し

1. $b|a \overset{def}{\iff} \exists c \in R, s.t. a = bc$ と定める，このとき a は b の倍元，b は a の約元，b は a を割り切るという

2. $a \approx b \overset{def}{\iff} \exists u \in R^{\times}, a = bu$ と定める，このとき a と b は同伴であるという

Lemma 9.2. R を整域とし，$x, y \in R$ とすると

1. $x|y \iff (x) \supset (y)$

2. $x \approx y \iff (x) = (y)$

Proof.　1. $x|y$ より，$y = dx$ とおき，$d \in R$ である．すると，$(y) = dxR \subset xR = (x)$ となる．逆に，$(y) \subset (x)$ とすると，$y \in (y) \subset (x)$ から，$\exists d \in R, s.t. y = dx$

2. $x \approx y$ とすると，$\exists r \in R^{\times}, s.t. y = rx$ であるから，$x|y$ となる．$\approx$ の対称性より，$y|x$ となる．したがって，(1) より，$(x) = (y)$ である．逆に，$(x) = (y)$ とすると，$x \in (x) = (y)$ より，$\exists r \in R, s.t. x = ry$ である．同様に，$y \in (y) = (x)$ より，$\exists s \in R, s.t. y = sx$ である．したがって，$x = rys$ となる．よって，$x \approx y$

□

Definition 9.3. 既約元
R を整域とする．$0 \neq p \in R$ は単元でないとする

$$p \in R : \text{既約元} \overset{def}{\iff} \forall a, b \in R, p = ab \text{ ならば } a \text{ または } b \text{ は単元}$$

Definition 9.4. 素元
R を整域とする．$0 \neq p \in R$ は単元でないとする

$$p \in R : \text{素元} \overset{def}{\iff} \forall a, b \in R, p \mid ab \text{ ならば } p \mid a \text{ または } p \mid b$$

ここで，もう一つの方法で素元と既約元を定義しよう

Definition 9.5. p を整域 R の零でない元とする，$p \notin R^{\times}$

- p が素元 $\overset{def}{\iff} p \mid ab \iff p \mid a$ または $p \mid b$

- p が既約元 $\overset{def}{\iff} a \mid p \iff a \approx p$ または $a \approx 1$

Lemma 9.6. p を整域 R の素元とすると，p は既約元である

Proof. $\forall a \in R, a \mid p$ が成り立つと，$p = ab$ とかけ，$p \mid ab$ となる．もし $p \mid a$ であると，$a \mid p$ かつ $p \mid a$．すると，$a \approx p$ となる．もし $p \nmid a$ なら，$p \mid b$ である．すると，$p \approx b$ となる．言い換えれば，$\exists r \in R^{\times}, s.t. ab = p = rb$．$p \neq 0$ から，$b \neq 0$ である．よって，$a = r \in R^{\times}$ で，$a \approx 1$ である　□

Definition 9.7. 一意分解整域 UFD
R を整域とする

$$R : \text{一意分解整域} \overset{def}{\iff} R \text{ は次の条件をみたす}$$

1. $a \in R$ が $a \neq 0$ で単元でないなら，$a = p_1 \cdots p_r \quad (p_i : \text{既約元}, i = 1, \cdots, r)$ とかけ，これを既約元分解という

2. $p_1 \cdots p_r = q_1 \cdots q_s \quad p_i, q_j$: 既約元, $i = 1, \cdots, r, j = 1, \cdots, s$ なら，$r = s$ であり，適当に番号を付け替えれば $p_i \approx q_i \quad (i = 1, \cdots, r)$

Proposition 9.8. R を一意分解整域とし，$0 \neq p \in R$ とする

$$(p) : \text{素イデアル} \iff p : \text{既約元}$$

Definition 9.9. R を一意分解整域とし，$h \in \mathrm{Frac}(R) \setminus \{0\}$ とすると，$\exists f, g \in R, s.t. g \neq 0$ かつ f, g が互いに素であり，$h = \dfrac{f}{g}$ である．このとき，$\dfrac{f}{g}$ を既約分式という

もし，$f_1, g_1 \in R$ も $g_1 \neq 0$ かつ $h = \dfrac{f_1}{g_1}$ をみたしているなら，$f \mid f_1, g \mid g_1$ である

Lemma 9.10. 整域 $F[X]$ のすべてのイデアルは単項イデアルである

Proof.
$I = \{0\}$ の場合は自明であるから，以下は $I \neq \{0\}$ とする
$I \neq \{0\}$ より，$\exists h \in I$ かつ $h \neq 0$．ここで，$S := \{\deg(h) : h \in I, h \neq 0\} \subset \mathbb{N}$ とおくと，非空な自然数の部分集合であるから，最小元を持つ．よって，$\exists 0 \neq f \in I, s.t. \deg(f) = \min S$
$f \in I$ かつ I はイデアルであるから，$\forall a(X) \in F[X], a(X) f(X) \in I$ である．よって，$(f) \subset I$
逆に,$g \in I$ を任意に取り,剰余の定理より,$\exists d(X), r(X) \in F[X], s.t. g(X) = d(X) f(X) + r(X)$ かつ $r = 0$ または $\deg(r) < \deg(f)$ である．$f, g \in I$ かつ $d \in F[X]$ より $d(X) f(X) \in I$ で，イデアルは加法に関して閉じているから，$r = g - df \in I$ である．よって，$r \in I$ かつ $r = 0$ または $\deg(r) < \deg(f)$ である．$r \neq 0$ では，$r \in I$ かつ $\deg(r) < \deg(f)$ から，f の最小性と矛盾する．従って，$r = 0$ で，$g = df$ となり，$g \in (f)$ である．ここで，g は任意にとるから，$I \subset (f)$
以上より，$I = (f)$ である．よって，整域 $F[X]$ のすべてのイデアルは単項イデアルである　□

Lemma 9.11. 整域 $F[X]$ のすべての既約元は素元である

Proof.
$p \in F[X]$ を既約元とし，$p \mid ab$ とする．$a \in F[X]$ に対して，イデアル $\langle p, a \rangle$ を考えると，$(f) = \langle p, a \rangle$ をみたす $f \in F[X]$ を任意にとる．$(f) \supset (a)$ より，$f \mid a$ で，$(f) \supset (p)$ より，$f \mid p$ である．p は既約元であるから，$f \approx p$ または $f \approx 1$ である．

- $f \approx p$ なら $f \mid a$ で $p \mid a$ となる
- $f \approx 1$ なら $\langle p, a \rangle = F[X]$ で,$\exists x, y, s.t. px + ay = 1$ で,両辺に b をかけると,$p \mid pxb + aby = b$ となる

よって，p は素元である　□

Remark 9.12. 多項式 f, g が $f \mid g$ をみたしていると，f を g の約元といい，多項式環 $F[X]$ における既約元（もしくは素元）を既約多項式という

10　公約元・公倍元・単項イデアル整域 PID

Definition 10.1. 公約元・公倍元
$a_1, \cdots, a_n \in R$ とする

- $d \in R : a_1, \cdots, a_n$ の公約元 $\overset{def}{\iff} \forall i = 1, \cdots, n, d | a_i$
- $d \in R : a_1, \cdots, a_n$ の最大公約元 d は $a_1, \cdots, a_n$ の公約元であり，$a_1, \cdots, a_n$ の任意の公約元 c に対し $c|d$
- $m \in R : a_1, \cdots, a_n$ の公倍元 $\overset{def}{\iff} \forall i = 1, \cdots, n, a_i | m$
- $m \in R : a_1, \cdots, a_n$ の最小公倍元 m は $a_1, \cdots, a_n$ の公倍元であり，$a_1, \cdots, a_n$ の任意の公倍元 l に対し $m|l$

Definition 10.2. 単項イデアル整域 PID
R を整域とする

$$R：\text{単項イデアル整域} \overset{def}{\iff} R \text{ の任意のイデアルは単項イデアル}$$

Proposition 10.3. 整域 R が一意分解整域である必要十分条件は，次の二つの条件を満たすことである

- $\forall r \in R \setminus \{0\}$，$r$ は既約元の積に分解できる
- すべての既約元は素元である

Proposition 10.4. 単項イデアる整域の零でない素イデアルは極大イデアルである

Lemma 10.5. Noether 性質
R を単項イデアル整域とし，$(I_n)_{n=1}^{\infty}$ を R のイデアルの列であるとする．また，$I_1 \subset I_2 \subset I_3 \subset \cdots$ であれば，ある自然数 N が存在して，$\forall n \geq N, I_n = I_{n+1} = \cdots$

Proof.
$I := \bigcup_{n=1}^{\infty} I_n$ とし，$x \in I_a, y \in I_b$ とすると，$x + y \in I_{\max\{a,b\}}$ となり，$\forall r \in R, rx \in I_a$ である．すると，$I = (h)$ をみたす $h \in R$ を任意に取り，I は和集合であるから，$\exists n \in \mathbb{N}, s.t. h \in I_n$ で，$I \subset I_n$ となる．また，定義より，$I_n \subset I_{n+1} \subset \cdots \subset I$ である．よって，$I_n = I_{n+1} = \cdots = I$　□

Theorem 10.6. R を単項イデアル整域とすると，R は一意分解整域である

Proposition 10.7. R を単項イデアル整域，$t \in R \setminus \{0\}$ かつ $t \notin R^{\times}$ とする．このとき，以下同値

1. $R/(t)$ は体である
2. $R/(t)$ は整域である
3. t は素元である
4. t は既約元である

Definition 10.8. R を一意分解整域とし，$f(x) = a_n x^n + \cdots + a_0 \in R[x]$ で，$a_0, \cdots, a_n$ の最大公約元が単元であるとき，$f(x)$ を原始多項式という

Proposition 10.9. R を一意分解整域とし，$f(x) \in R[x]$ とする．このとき，以下同値

1. $f(x)$ は原始多項式である

2. $p \in A$ を任意の素元とするとき，$f(x)$ を p で法として考えた多項式 $\overline{f}(x) \in (R/(p))[x]$ は零でない

Definition 10.10. ユークリッド整域
R を整域とする

$$R：\text{ユークリッド整域} \overset{def}{\iff} \text{写像 } d : R\backslash\{0\} \to \mathbb{N} \cup \{0\} \text{ が存在し，} a, b \in R \text{ に対し，} b \neq 0 \text{ なら} \\ a = qb + r, \quad r = 0 \text{ または } d(r) < d(b) \text{ となる } q, r \in R \text{ が存在する}$$

Theorem 10.11. R を整域とする

$$R：\text{ユークリッド整域} \implies R：\text{単項イデアル整域} \implies R：\text{一意分解整域}$$

Theorem 10.12. R を単項イデアル整域，I を R のイデアルとする

$$I：\text{素イデアル} \iff I：\text{極大イデアル}$$

Proposition 10.13. R を単項イデアル整域，$0 \neq p \in R$ とする

$$p：\text{既約元} \iff (p)：\text{素イデアル}$$

Example 10.14. $\mathbb{Z}\left[\sqrt{-1}\right]$ はユークリッド整域

Proof.
$\mathbb{Z}\left[\sqrt{-1}\right] := \left\{a + b\sqrt{-1} : a, b \in \mathbb{Z}\right\}$ とおき，$\mathbb{Z}\left[\sqrt{-1}\right] \subset \mathbb{C}$ であるから，整域となる．ここで

$$N : \mathbb{Z}\left[\sqrt{-1}\right] \to \mathbb{Z}_{\geq 0} \tag{28}$$
$$N\left(x + y\sqrt{-1}\right) = x^2 + y^2 \tag{29}$$

と定義し，$N(a \cdot b) = N(a) N(b)$ がある．$\forall a = x + y\sqrt{-1}, b = z + w\sqrt{-1} \in \mathbb{Z}\left[\sqrt{-1}\right]$

$$\frac{a}{b} = \frac{(xz + yw) + (yz - xw)\sqrt{-1}}{N(b)} \tag{30}$$
$$= q_1 + q_2\sqrt{-1} + \frac{r_1 + r_2\sqrt{-1}}{N(b)} \tag{31}$$

から，$a = \left(q_1 + q_2\sqrt{-1}\right) b + \dfrac{r_1 + r_2\sqrt{-1}}{N(b)} b = qb + r$ で，$q \in \mathbb{Z}\left[\sqrt{-1}\right]$ より，$r \in \mathbb{Z}\left[\sqrt{-1}\right]$

$$N(r) = N\left(\frac{r_1 + r_2\sqrt{-1}}{N(b)} b\right) = \frac{N\left(r_1 + r_2\sqrt{-1}\right) N(b)}{N(b)^2} = \frac{r_1^2 + r_2^2}{N(b)} \tag{32}$$
$$\leq \frac{\frac{1}{4}N(b)^2 + \frac{1}{4}N(b)^2}{N(b)} < N(b) \tag{33}$$

よって，N はノルムであり，$\mathbb{Z}\left[\sqrt{-1}\right]$ がユークリッド整域である □

Proposition 10.15.
1. $x \in \mathbb{Z}\left[\sqrt{d}\right]$ なら，$N(x) \in \mathbb{Z}$
2. $\forall x, y \in \mathbb{Q}\left[\sqrt{d}\right], N(xy) = N(x) N(y)$
3. $x = a + b\sqrt{d} \in \mathbb{Q}\left[\sqrt{d}\right] \setminus \{0\}$ なら，$N(x) \neq 0, x^{-1} = \phi(x) N(x)^{-1}$
4. $x = a + b\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\right]$ が $\mathbb{Z}\left[\sqrt{d}\right]$ の単元であることと，$N(x) = \pm 1$ であることと同値である

11　可約・既約

Definition 11.1. 可約・既約
R を整域，$f(x) \in R[x], \deg f \geq 1$ とする

- $f(x)$：可約 $\overset{def}{\iff} \exists g(x), h(x) \in R[x], \deg g, \deg h \geq 1$ に対し $f(x) = g(x)h(x)$
- $f(x)$：既約 $\overset{def}{\iff} f(x)$：可約でない

Proposition 11.2. R を一意分解整域，K を R の商体，$f(x) \in R[x]$ とする

$$f(x)：R\text{ 上既約} \iff f(x)：K\text{ 上既約}$$

Definition 11.3. 容量
$P(X) \in R[X]$ を $P(X) = a_nX^n + \cdots + a_1X + a_0, a_n \neq 0$ とする．$c(P)$ を $\gcd(a_0, a_1, \cdots, a_n)$ とすると，$c(P)$ は同伴の意味で一意に定まる．これを $P(X)$ の容量という

Lemma 11.4. R を一意分解整域，$P, Q \in R[X]$ とすると，$c(P)c(Q)$ と $c(PQ)$ は同伴である

Theorem 11.5. Gauss の補題
R を一意分解整域，$K = \mathrm{Frac}(R)$ を商体とすると，$P(X) \in R[X]$ は $R[X]$ 上既約である $\iff$ $P(X)$ は $K[X]$ で既約である
さらに,$K[X]$ で $P(X) = P_1(X)P_2(X), \deg(P_i) \geq 1$ であれば,$\exists k \in K^\times, s.t. kP_1(x), kP_2(X) \in R[X]$

Theorem 11.6. Gauss の定理
R を一意分解整域，$R[X]$ も一意分解整域である

Proposition 11.7. K が体，$f(x) \in K[x]$ が既約なら，$K[x]/(f(x))$ は体である

Definition 11.8. 整・整拡大

- A を環 B の部分環とする．このとき，$x \in B$ が A 上**整**とは，$a_1, a_2, \cdots, a_n \in A$ があり $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ となることである
- A, B を環，$\phi : A \to B$ を準同型とする．$x \in B$ が $\phi(A)$ 上整なら，x は A 上整であるという．B の元がすべて A 上整なら，B は A 上整であるという
- B が A の拡大環で A 上整なら**整拡大**という

Definition 11.9. 整閉整域・正規環
R を整域とし，K をその商体とする．$a \in K$ が R 上整なら $a \in A$ をみたすとき，A を整閉整域，あるいは正規環という

Theorem 11.10. 一意分解整域は正規環である

Proposition 11.11. $f(x) = a_nx^n + \cdots + a_0 \in R[x]$ が原始多項式，$\overline{a_n} \neq 0$ で $\overline{f(x)}$ が $k[x]$ の既約元なら，$f(x)$ も $K[x]$ の既約元である．ただし，R を一意分解整域，$p \in R$ を素元，K と k はそれぞれ $R, R/(p)$ の商体であり，$r \in R, f(x) \in R[x]$ を p を法として考えるときには $\overline{a}, \overline{f(x)}$ である