最低限の環論

高瀬 幸一

ver.2022.9.20

目 次

1 環に関する基本的な定義と例 **3**

1.1 環の定義と例 3
1.2 部分環 7
1.3 環の乗法群（単数群） 7
1.4 整域，体 8

2 イデアル **9**

2.1 イデアルの定義と例 9
2.2 整数環のイデアル 11
2.3 Euclid の互除法 15

3 剰余類環 **18**

3.1 イデアルを法とする合同式 18
3.2 剰余類と剰余類環 20
3.3 素イデアルと極大イデアル 21

4 単項イデアル整域 **23**

4.1 多項式環のイデアル 23
4.2 Gauss の整数環のイデアル 24
4.3 単項イデアル整域の定義と基本的な性質 25
4.4 単項イデアル整域の素元 26
4.5 単項イデアル整域における素因子分解 29
4.6 多項式の最大公約数 31

5 環の準同型定理 **34**

5.1 環の準同型写像 34
5.2 環の準同型定理 35
5.3 中国剰余定理 37
5.4 代数的数の最小多項式 39

6 有理数体上の一変数多項式環 **40**

6.1 原始的多項式 41
6.2 整数係数の既約多項式 43
6.3 Eisenstein の判定法 44
6.4 整数係数多項式の素因子分解 46

7 Gauss の整数環 **50**

1　環に関する基本的な定義と例

1.1　環の定義と例

整数の全体

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$$

を考えると，そこでは加法（足し算）と乗法（掛け算）があって，分配法則

$$a(b+c) = ab + ac$$

が成り立っている．同様に係数が有理数である変数 X の多項式の全体を $\mathbb{Q}[X]$ と書くと，ここでも多項式の加法，乗法があって，分配法則

$$f(X)(g(X) + h(X)) = f(X)g(X) + f(X)h(X)$$

が成り立っている．このように，ある集合 A で**加法**と**乗法**が定義されていて，**分配法則**が成り立つとき，集合 A を**環 (ring)** と呼ぶ．

整数全体 $\mathbb{Z}$ や有理数係数一変数多項式全体 $\mathbb{Q}[X]$ の場合には「加法」や「乗法」は直感的に明らかであるが，これを抽象化して考えるためには，「加法」とは何か，「乗法」とは何かを正確に定義しなくてはならない．そこで，環の正確な定義は次のとおりである：

定義 1.1.1 集合 A に対して

1) 加法が定義されている，即ち，任意の $a, b \in A$ に対して，その**和** $a+b \in A$ が定義されていて

   i) 任意の $a, b, c \in A$ に対して $(a+b)+c = a+(b+c)$ となる（加法の結合法則），

   ii) 特別な $0_A \in A$ があって，任意の $a \in A$ に対して $a+0_A = 0_A+a = a$ となる（この特別な $0_A \in A$ を A の加法単位元と呼ぶ），

   iii) 任意の $a \in A$ に対して $a + a' = a' + a = 0_A$ となる $a' \in A$ が存在する（この $a' \in A$ を a の加法逆元と呼び $-a \in A$ と表す），

   iv) 任意の $a, b \in A$ に対して $a+b = b+a$ である（加法の交換法則）．

2) 乗法が定義されている，即ち，任意の $a, b \in A$ に対して，その**積** $a \cdot b \in A$ が定義されていて

   i) 任意の $a, b, c \in A$ に対して $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ となる（乗法の結合法則），

   ii) 特別な $1_A \in A$ があって，任意の $a \in A$ に対して $a \cdot 1_A = 1_A \cdot a = a$ となる（この特別な $1_A \in A$ を A の**乗法単位元**と呼ぶ），

   iii) 任意の $a, b \in A$ に対して $a \cdot b = b \cdot a$ である（乗法の交換法則）．

3) 任意の $a, b, c \in A$ に対して

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

である．

このとき集合 A はこれらの加法と乗法に関して**環**をなす，という．

注意 1.1.2 環 A に対して

1) A の加法単位元と乗法単位元は唯一存在する．

[**証明**] $0, 0' \in A$ が A の加法単位元とすると

$$0 = 0 + 0' = 0'$$

となる．$1, 1' \in A$ が A の乗法単位元とすると

$$1 = 1 \cdot 1' = 1'$$

となる．■

2) $a \in A$ の加法逆元は唯一存在する．

[**証明**] $x, y \in A$ が $a \in A$ の加法逆元とすると，$a + x = a + y = 0_A$ だから

$$x = x + 0_A = x + (a + y) = (x + a) + y = 0_A + y = y$$

となる．■

注意 1.1.3 環 A で $x, y \in A$ に対して $x + (-y)$ を $x - y$ と表す．

注意 1.1.4 環 A の元 $a, b \in A$ に対して，$a = bc$ となる $c \in A$ が存在するとき，a は b **を割り切る**といい，記号で $a|b$ と書く．

例 1.1.5 整数の全体

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$$

た通常の整数の加法と乗法に関して環である．

例 1.1.6 環 A に対して，A の元を係数とする変数 X の多項式の全体を $A[X]$ と書く．即ち $A[X]$ は形式的な有限和

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \quad (a_0, a_1, a_2, \cdots, a_n \in A, n = 0, 1, 2, 3, \cdots)$$

の全体で，

$$f(X) = \sum_{k=0}^{n} a_k X^k,\ g(X) = \sum_{k=0}^{n} b_k X^k \in A[X]$$

の和 $f(X)+g(X)$ と積 $f(X)\cdot g(X)$ をそれぞれ

$$f(X)+g(X)=\sum_{k=0}^{n}(a_k+b_k)X^k,\quad f(X)\cdot g(X)=\sum_{k=0}^{2n}\left(\sum_{i+j=k}a_ib_j\right)X^k$$

により定義すると，$A[X]$ は環となる．$A[X]$ の加法単位元は A の加法単位元 $0_A\in A$ であり，$A[X]$ の乗法単位元は A の乗法単位元 $1_A\in A$ である．

$A[X]$ を環 A 上の一変数多項式環と呼ぶ．

例 1.1.7 二つの環 A,B に対して，その直積集合

$$A\times B=\{(x,y)\mid x\in A,y\in B\}$$

は，加法，乗法を

$$(x,y)+(x',y')=(x+x',y+y'),\qquad (x,y)\cdot(x',y')=(xx',yy')$$

と定義することにより環となる．

$$0_{A\times B}=(0_A,0_B,\qquad 1_{A\times B}=(1_A,1_B)$$

である．環 $A\times B$ を環 A,B の**直積環**と呼ぶ．

同様に有限個の環 $A_1,A_2,\cdots,A_r$ の直積集合

$$A=A_1\times A_2\times^c dots\times A_r$$

は

$$\begin{aligned}&\text{加法}:(x_1,\cdots,x_r)+(y_1,\cdots,y_r)=(x_1+y_1,\cdots,x_r+y_r),\\&\text{乗法}:(x_1,\cdots,x_r)\cdot(y_1,\cdots,y_r)=(x_1\cdots y_1,\cdots,x_r\cdot y_r)\end{aligned}$$

により環となる．

$$0_A=(0_{A_1},\cdots,0_{A_r}),\quad 1_A=(1_{A_1},\cdots,1_{A_r})$$

である．環 A を $A_1,A_2,\cdots,A_r$ の直積環と呼ぶ．

例 1.1.8 同じ集合でも，異なる演算により環になることがある．例えば直積集合 $A=\mathbb{Z}\times\mathbb{Z}$ に対して

1) 直積環としての加法，乗法

$$(x,y)+(z,w)=(x+z,y+w),\qquad (x,y)\cdot(z,w)=(xz,yw)$$

により，A は環となる．$0_A=(0,0),1_A=(1,1)$ である．これとは別に

2) A 上の加法，乗法を

$$(x,y)+(z,w)=(x+z,y+w), \qquad (x,y)\cdot(z,w)=(xz-yw,xw+yz)$$

により定義すると，A は環となる．$0_A=(0,0), 1_A=(1,0)$ である．

例 1.1.9 環 A の元を成分とする $n>1$ 次正方行列の全体を $M_n(A)$ と書く．n 次正方行列 $X\in M_n(A)$ の (i,j)-成分を X_{ij} と書くことにする．このとき $X,Y\in M_n(A)$ の「和」$X+Y$ と「積」$X\cdot Y$ をそれぞれ

$$(X+Y)_{ij}=X_{ij}+Y_{ij}, \quad (X\cdot Y)_{ij}=\sum_{k=1}^{n}X_{ik}Y_{kj} \quad (1\le i,j\le n)$$

により定義すると，環の公理のうち 2) の iii)（積の交換法則）以外は全て成り立つ．このように，積の交換法則以外が全て成り立つようなものを**非可換環**と呼ぶ．非可換環は数学で非常に重要な役割を果たすものであるが，この講義では扱わない．

例 1.1.10 i を虚数単位として，

$$\mathbb{Z}[i]=\{x+iy \mid x,y\in\mathbb{Z}\}$$

は複素数の加法，乗法に関して環となる．この環を **Gauss の整数環**と呼ぶ．

例 1.1.11 1 の虚数 3 乗根 $\omega=\dfrac{-1+\sqrt{3}i}{2}$ に対して

$$\mathbb{Z}[\omega]=\{x+\omega y \mid x,y\in\mathbb{Z}\}$$

は複素数の加法，乗法に関して環となる．この環を **1 の 3 乗根の環**と呼ぶ．

例 1.1.12
1) 有理数全体の集合 $\mathbb{Q}$ は有理数の加法と乗法に関して環となる．

2) 実数全体の集合 $\mathbb{R}$ は実数の加法と乗法に関して環となる．

3) 複素数全体の集合 $\mathbb{C}$ は複素数の加法と乗法に関して環となる．

課題 1.1 例 1.1.8 の 2) の場合が，実際に環の条件を満たしていることを示せ．

課題 1.2 環 A の元 $a\in A$ に対して，$0_A\cdot a=0_A$ および $-a=(-1_A)\cdot a$ であることを示せ．

課題 1.3 例 1.1.10 を確かめよ．

課題 1.4 例 1.1.11 を確かめよ．

1.2 部分環

Gauss の整数環 $\mathbb{Z}[i]$ の中に整数全体 $\mathbb{Z}$ は部分集合として含まれている．このように大きな環 A の中に小さな環 B が部分集合として含まれる場合がよくある．このとき B は A の部分環であるという．正確には次のように定義する：

定義 1.2.1 環 A の部分集合 $B \subset A$ に対して

1) $0_A \in B$ かつ $1_A \in B$

2) 任意の $x, y \in B$ に対して $x + y \in B$ かつ $xy \in B$,

3) 任意の $x \in B$ に対して $-x \in B$,

が成り立つとき，B は A の**部分環**であるという．

例 1.2.2 環 A 上の一変数多項式環 $A[X]$ (例 1.1.6) の中に A 自身は部分環として含まれる．

1.3 環の乗法群（単数群）

定義 1.3.1 環 A に対して

$$A^\times = \{a \in A \mid ab = 1_A \text{ となる } b \in A \text{ が存在する } \}$$

を A の**乗法群**，あるいは**単数群**と呼ぶ．$A^\times$ の元を A の単数と呼ぶ．

注意 1.3.2 環 A に対して $1_A \in A^\times$ である．

例 1.3.3 $\mathbb{Z}^\times = \{\pm 1\}$ である．

定理 1.3.4 Gauss の整数環 $\mathbb{Z}[i]$ に対して $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ である．

[**証明**] まず $\alpha = x + iy \in \mathbb{Z}[i]$ に対して

$$N(\alpha) = \alpha \cdot \overline{\alpha} = x^2 + y^2 \in \mathbb{Z}$$

であり，$\alpha, \beta \in \mathbb{Z}[i]$ に対して $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$ である．さて $\varepsilon = x + yi \in \mathbb{Z}[i]^\times$ とすると，$\varepsilon \cdot \gamma = 1$ なる $\gamma \in \mathbb{Z}[i]$ が存在する．従って

$$N(\varepsilon) \cdot N(\gamma) = N(\varepsilon \cdot \gamma) = N(1) = 1$$

かつ $N(\varepsilon), N(\gamma)$ は正の整数だから，$N(\varepsilon) = 1$ である．よって $x^2 + y^2 = 1$ となり

$$(x, y) = (\pm 1, 0) \text{ または } (0, \pm 1)$$

となる．即ち $\varepsilon = \pm 1$ または $\varepsilon = \pm i$ である．■

課題 1.5 環 A の乗法群 $A^\times$ に対して，次を示せ：

1) $a, b \in A^\times$ ならば $ab \in A^\times$ である．

2) $a, b \in A$ に対して，$a|b$ かつ $b \in A^\times$ ならば $a \in A^\times$ である．

課題 1.6 1 の 3 乗根の環 $\mathbb{Z}[\omega]$ (例 1.1.11) について

$$\mathbb{Z}[\omega]^\times = \left\{\pm 1, \pm\omega, \pm\omega^2\right\}$$

であることを示せ．

1.4 整域，体

整数環 $\mathbb{Z}$ においては，任意の二つの整数 $a, b \in \mathbb{Z}$ に対して $ab = 0$ ならば $a = 0$ 又は $b = 0$ である．しかし，このような性質は一般の環では成り立たない．例えば，例 1.1.8 の 1) で定義した環では，$(1,0), (0,1) \in A = \mathbb{Z} \times \mathbb{Z}$ はどちらも 0 でないが，その積は

$$(1,0) \cdot (0,1) = (0,0)$$

となり，これは例 1.1.8 で定義した環 $A = \mathbb{Z} \times \mathbb{Z}$ の 0 である．そこで次のように定義する：

定義 1.4.1 環 A において，任意の二つの元 $a, b \in A$ に対して $ab = 0$ ならば $a = 0$ 又は $b = 0$ が成り立つとき，A を**整域**と呼ぶ．

例 1.4.2 整数環 $\mathbb{Z}$ は整域である．

例 1.4.3 Gauss の整数環 $\mathbb{Z}[i]$ (例 1.1.10) は整域である．

例 1.4.4 1 の 3 乗根の環 $\mathbb{Z}[\omega]$ (例 1.1.11) は整域である．

定理 1.4.5 整域 A 上の一変数多項式環 $A[X]$ は整域である．

[**証明**] $f(X), g(X) \in A[X]$ に対して，$f(x) \neq 0, g(X) \neq 0$ ならば $f(X)g(X) \neq 0$ を示せば良い．$f(X) \neq 0, g(X) \neq 0$ とすると

$$\begin{aligned} f(X) &= a_0X^m + a_1X^{m-1} + \cdots + a_{m-1}X + a_m \quad (a_i \in A, a_0 \neq 0), \\ g(X) &= b_0X^n + b_1X^{n-1} + \cdots + b_{n-1}X + b_n \quad (b_j \in A, b_0 \neq 0) \end{aligned}$$

とおける．A は整域だから $a_0b_0 \neq 0$ で

$$f(X)g(X) = a_0b_0X^{m+n} + (a_0b_1 + a_1b_0)X^{m+n-1} + \cdots + a_mb_n$$

となるから，$f(X)g(X) \neq 0$ である．■

定義 1.4.6 環 F において，0 でない任意の $a \in F$ に対して $ab = 1$ となる $b \in F$ が存在するとき，F は**体**であるという．言い換えれば，

$$F^\times = \{0 \neq a \in F\}$$

のとき，つまり F の乗法群が F の 0 以外の元全体であるとき，F を体と呼ぶ．

例 1.4.7 1) 有理数全体の集合 $\mathbb{Q}$ は有理数の加法と乗法に関して体となる．これを**有理数体**と呼ぶ．

2) 実数全体の集合 $\mathbb{R}$ は実数の加法と乗法に関して体となる．これを**実数体**と呼ぶ．

3) 複素数全体の集合 $\mathbb{C}$ は複素数の加法と乗法に関して体となる．これを**複素数体**と呼ぶ．

課題 1.7 整域 A 上の一変数多項式環 $A[X]$ に対して，$A[X]^\times = A^\times$ であることを示せ．

2 イデアル

2.1 イデアルの定義と例

定義 2.1.1 環 A の空でない部分集合 $\mathfrak{a} \subset A$ に対して[1]

1) 任意の $x, y \in \mathfrak{a}$ に対して $x + y \in \mathfrak{a}$,

2) 任意の $a \in A$ と任意の $x \in \mathfrak{a}$ に対して $ax \in \mathfrak{a}$

が成り立つとき，$\mathfrak{a}$ を環 A の**イデアル**と呼ぶ．

注意 2.1.2 環 A のイデアル $\mathfrak{a} \subset A$ について

1) $x, y \in A$ に対して $x - y = x + (-y)$, $-y = (-1_A) \cdot y$ である．よって $x, y \in \mathfrak{a}$ ならば $x - y \in \mathfrak{a}$ である．

2) $\mathfrak{a} \neq \emptyset$ で $x \in \mathfrak{a}$ に対して $0_A \cdot x = 0_A$ だから，$0_A \in \mathfrak{a}$ である．

例 2.1.3 環 A において，A 自身と $\{0\}$ は A のイデアルである．これらを環 A の**自明なイデアル**と呼ぶ．

[1] $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ はドイツ文字の小文字の $a, b, c, \cdots$ である．

命題 2.1.4 環 A の有限個の元 $\{a_1, a_2, \cdots, a_r\} \subset A$ をとって

$$(a_1, a_2, \cdots, a_r) = \{a_1x_1 + a_2x_2 + \cdots + a_rx_r \mid x_i \in A\}$$

とおくと，$(a_1, a_2, \cdots, a_r)$ は A のイデアルである．これを $\{a_1, a_2, \cdots, a_r\}$ **で生成されたイデアル**と呼ぶ.

[**証明**] 簡単のために $\mathfrak{a} = (a_1, a_2, \cdots, a_r)$ とおく．$x, y \in \mathfrak{a}$ とすると

$$x = \sum_{i=1}^{r} a_ix_i, \qquad y = \sum_{i=1}^{r} a_iy_i \qquad (x_i, y_i \in A)$$

とおける．よって

$$x + y = \sum_{i=1}^{r} a_i(x_i + y_i) \in \mathfrak{a}$$

である．また $a \in A$ に対して

$$ax = \sum_{i=1}^{r} a_i(ax_i) \in \mathfrak{a}$$

である．■

上の定理で $r = 1$ とすれば次の系が成り立つ：

系 2.1.5 環 A の元 $a \in A$ に対して

$$(a) = \{ax \mid x \in A\}$$

は A のイデアルである．これを a **で生成された単項イデアル**と呼ぶ.

命題 2.1.6 環 A のイデアル $\mathfrak{a} \subset A$ に対して，次は同値である：

1) $\mathfrak{a} = A$,

2) $1_A \in \mathfrak{a}$,

3) $\mathfrak{a} \cap A^\times \neq \emptyset$.

[**証明**] 1) $\Rightarrow$ 2) 明らか.

2) $\Rightarrow$ 3) $1_A \in A^\times$ だから明らか.

3) $\Rightarrow$ 2) $\mathfrak{a} \cap A^\times \neq \emptyset$ だから $\varepsilon \in \mathfrak{a}$ なる $\varepsilon \in A \times$ がとれる．$\varepsilon \in A^\times$ だから $\varepsilon\eta = 1_A$ なる $\eta \in A$ が存在する．$\varepsilon \in \mathfrak{a}$ で $\mathfrak{a}$ は A のイデアルだから，$1_A = \eta\varepsilon \in \mathfrak{a}$ となる.

2) $\Rightarrow$ 1) $\mathfrak{a}$ は A のイデアルだから，$1_A \in \mathfrak{a}$ ならば，任意の $a \in A$ に対して $a = a \cdot 1_A \in \mathfrak{a}$ となる．よって $\mathfrak{a} = A$ となる．■

命題 2.1.7 整域 A において，0 でない $a, b \in A$ に対して

$$(a) = (b) \quad \Leftrightarrow \quad a = \varepsilon \cdot b \text{ なる } \varepsilon \in A^\times \text{ が存在する}$$

である．

[証明] $\Leftarrow$) まず

$$(a) = \{ax \mid x \in A\} = \{b(\varepsilon x) \mid x \in A\} \subset \{by \mid y \in A\} = (b)$$

である．$\varepsilon \in A^\times$ だから $\varepsilon \cdot \eta = 1$ なる $\eta \in A^\times$ がとれる．よって $\eta a = \eta \varepsilon b = b$ となるから，上と同様にして $(b) \subset (a)$ である．よって $(a) = (b)$ となる．

$\Rightarrow$) $a \in (a) = (b)$ だから $a = bx$ なる $x \in A$ が存在する．$b \in (b) = (a)$ だから $b = ay$ なる $y \in A$ が存在する．よって

$$a = bx = axy \qquad \therefore \ a(xy - 1) = 0$$

となる．$a \neq 0$ で A は整域だから $xy - 1 = 0$ つまり $xy = 1$ となり，$x \in A^\times$ である．■

課題 2.1 環 A の単項イデアル $(a) \subset A$ $(a \in A)$ に対して

$$(a) = A \quad \Leftrightarrow \quad a \in A^\times$$

であることを示せ．

課題 2.2 環 A のイデアル $\mathfrak{a} \subset A, \mathfrak{b} \subset A$ に対して

1) $\mathfrak{a} \cap \mathfrak{b}$ は A のイデアルであることを示せ．

2) $\mathfrak{a} + \mathfrak{b} = \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}$ は A のイデアルであることを示せ．

課題 2.3 有理数体 $\mathbb{Q}$ 上の一変数多項式環 $\mathbb{Q}[X]$ を考える．任意の複素数 $\alpha \in \mathbb{C}$ に対して

$$\mathfrak{a} = \{f(X) \in \mathbb{Q}[X] \mid f(\alpha) = 0\}$$

は $\mathbb{Q}[X]$ のイデアルとなることを示せ．

2.2 整数環のイデアル

整数環 $\mathbb{Z}$ のイデアルについて詳しく見てみよう．その際に，次の**整数の剰余の定理**が出発点となる：

定理 2.2.1 (整数の剰余の定理) 整数 $a, b \in \mathbb{Z}$, $b > 0$ に対して

$$a = qb + r, \qquad 0 \leq r < b$$

なる整数 $q, r \in \mathbb{Z}$ が唯一存在する．

[**証明**] 有理数 $\dfrac{a}{b} \in \mathbb{Q}$ に対して，

$$q \leq \frac{a}{b} < q+1$$

なる整数 $q \in \mathbb{Z}$ が存在する．このとき $r = a - qb \in \mathbb{Z}$ は整数となり $a = qb + r$ である．更に

$$qb \leq a < bq + b \qquad \therefore \ \ 0 \leq r = a - qb < b$$

となる．逆に

$$a = q'b + r' \qquad 0 \leq r' < b$$

なる整数 $q', r' \in \mathbb{Z}$ があれば

$$q'b + r' = qb + r \quad \therefore \ \ |r' - r| = |q' - q|b$$

となる．ここで $0 \leq r, r' < b$ だから $|r' - r| < b$，従って $|q' = q| < 1$ となる．よって $q' - q = 0$，従って $r' - r = 0$，つなり

$$q' = q, \qquad r' = r$$

となる．■

さて $\mathbb{Z}$ のイデアルについて次の定理が基本的である：

定理 2.2.2 整数環 $\mathbb{Z}$ のイデアル $\mathfrak{a} \subset \mathbb{Z}$ に対して，$\mathfrak{a} \gneqq \{0\}$ ならば

$$d = \mathrm{Min}\left\{0 < n \in \mathfrak{a}\right\}$$

とおくと $\mathfrak{a} = (d)$ である．

[**証明**] まず初めに $\mathfrak{a}$ が正の整数を含むことを示そう．$\mathfrak{a} \gneqq \{0\}$ だから $0 \neq x \in \mathfrak{a}$ がとれる．$x < 0$ とすると，$-1 \in \mathbb{Z}$ で $\mathfrak{a}$ は $\mathbb{Z}$ のイデアルだから，$-x = (-1) \cdot x \in \mathfrak{a}$ となり，$-x > 0$ である．従って $\mathfrak{a}$ は正の整数を含くことになるから，$\mathfrak{a}$ に含まれる最小の正の整数 d が定義できる．$d \in \mathfrak{a}$ だから

$$(d) = \{dn \mid n \in \mathbb{Z}\} \subset \mathfrak{a}$$

は明らか．任意の $x \in \mathfrak{a}$ をとる．整数の剰余の定理 2.2.1 から

$$x = qd + r, \qquad 0 \leq r < d$$

なる整数 $q, r \in \mathbb{Z}$ がとれる．ここで $x \in \mathfrak{a}$ であり，$qd \in (d) \subset \mathfrak{a}$ だから，$r = x - qd \in \mathfrak{a}$ である．ここで $r \neq 0$ とすると

$$r \in \mathfrak{a} \qquad 0 < r < d$$

となり d の定義に反する．よって $r = 0$，従って $x = qd \in (d)$ となる．よって $\mathfrak{a} \subset (d)$ となるから，$\mathfrak{a} = (d)$ である．■

整数環のイデアルの意味を理解するのに，次の定理が有用であろう：

定理 2.2.3 0 でない整数 $\{a_1, a_2, \cdots, a_r\} \subset \mathbb{Z}$ の最大公約数を

$$d = \mathrm{GCD}\{a_1, a_2, \cdots, a_r\}$$

とすると $(a_1, a_2, \cdots, a_r) = (d)$ である．

[**証明**] 定理 2.2.2 より $(a_1, a_2, \cdots, a_r) = (D)$ なる正の整数 $0 < D \in \mathbb{Z}$ が存在する．このとき

$$a_i \in (a_1, a_2, \cdots, a_r) = (D) \qquad (i = 1, 2, \cdots, r)$$

だから，a_i $(i = 1, 2, \cdots, r)$ は全て D の倍数となる．即ち D は $\{a_1, a_2, \cdots, a_r\}$ の公約数だから $D \leq d$ である．一方，a_i $(i = 1, 2, \cdots, r)$ は全て d の倍数だから $a_i \in (d)$ である．従って

$$(D) = (a_1, a_2, \cdots, a_r) = \left\{ \sum_{i=1}^{r} a_i x_i \;\middle|\; x_i \in \mathbb{Z} \right\} \subset (d)$$

である．よって $D \in (D) \subset (d)$ だから D は d の倍数となり $D \geq d$ である．よって $D = d$ となる．■

系 2.2.4 0 でない整数 $\{a_1, a_2, \cdots, a_r\} \subset \mathbb{Z}$ に対して

$$a_1 A_1 + a_2 A_2 + \cdots + a_r A_r = \mathrm{GCD}\{a_1, a_2, \cdots, a_r\}$$

なる整数 $A_i \in \mathbb{Z}$ $(i = 1, 2, \cdots, r)$ が存在する．

[**証明**] $\mathrm{GCD}\{a_1, a_2, \cdots, a_r\} = d$ とおくと，定理 2.2.3 より $(a_1, a_2, \cdots, a_r) = (d)$ である．よって

$$d \in (d) = (a_1, a_2, \cdots, a_r) = \left\{ \sum_{i=1}^{r} a_i x_i \;\middle|\; x_i \in \mathbb{Z} \right\}$$

となるから，$d = \sum_{i=1}^{r} a_i A_i$ なる $A_i \in \mathbb{Z}$ が存在する．■

この定理から，最大公約数の次のような性質が導かれる：

定理 2.2.5 正数 a, b と整数 d に対して

$$d \text{ は } a, b \text{ の公約数} \;\Leftrightarrow\; d \text{ は } \mathrm{GCD}\{a, b\} \text{ の約数}$$

である．

[**証明**] $\Leftarrow$) d が $\mathrm{GCD}\{a, b\}$ の約数であると仮定する．このとき $\mathrm{GCD}\{a, b\}$ は a の約数だから，d は a の約数である．同様に d は b の約数となるから，d は a, b の公約数である．

$\Rightarrow$) d が a, b の公約数であるとすると

$$a = da', \quad b = db' \quad (a', b' : \text{整数})$$

と書ける．系 2.2.4 より

$$Aa + Bb = \mathrm{GCD}\{a, b\}$$

なる整数 A, B が存在する．よって

$$\begin{aligned} \mathrm{GCD}\{a, b\} &= Aa + Bb = Ada' + Bdb' \\ &= d(Aa' + Bb') \quad (Aa' + Bb' : \text{整数}) \end{aligned}$$

となり， d は $\mathrm{GCD}(a, b)$ の約数となる．■

系 2.2.4 から次の重要な定理が導かれる：

定理 2.2.6 正の整数 a, b, c に対して $\mathrm{GCD}\{a, b\} = 1$ のとき，a が積 bc を割り切るならば a は c を割り切る．

[**証明**] 系 2.2.4 より $aA + bB = 1$ なる整数 A, B が存在する．両辺に c を掛けると

$$c = acA + bcB$$

となるが，a は bc を割り切るから，a は c を割り切る．■

系 2.2.7 素数 p が整数の積 ab を割り切るならば，p は a 又は b を割り切る．従って，素数 p が整数の積 $a_1 a_2 \cdots a_r$ を割り切るならば，p は $a_1, a_2, \cdots, a_r$ の少なくとも一つを割り切る．

[**証明**] $\mathrm{GCD}\{p, a\} = d$ とおく．正の整数 d は素数 p の約数だから $d = 1$ または $d = p$ である．$d = p$ ならば a が p で割り切れる．$d = 1$ ならば，定理 2.2.6 より p は b を割り切る．■

この系を用いて，整数の素因数分解の一意性を示すことができる：整数 $N > 1$ が素数の積として

$$N = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

と書けたとしよう．ここで p_i, q_j $(i = 1, 2, \cdots, r,\ j = 1, 2, \cdots, s)$ は素数である．このとき p_1 は $q_1 q_2 \cdots q_s$ を割り切るから，系 2.2.7 より $q_1, q_2, \cdots, q_s$ のいずれかを割り切る．番号を付け替えて p_1 は q_1 を割り切るとしよう．ここで q_1 は素数で $p_1 > 1$ だから $p_1 = q_1$ となり

$$p_2 \cdots p_r = q_2 \cdots q_s$$

となる．これを繰り返せば，$r = s$ かつ，番号を付け直せば

$$p_1 = q_1,\ p_2 = q_2, \cdots, p_r = q_r$$

となる．

2.3 Euclid の互除法

整数の最大公約数を求める効率的な方法として **Euclid (ユークリッド) の互除法**がある．その基礎となるのは次の定理である：

定理 2.3.1 整数 a, b $(b > 0)$ に対して

$$a = qb + r, \qquad 0 \leqq r < b$$

なる整数 q, r をとると

$$\mathrm{GCD}\{a, b\} = \mathrm{GCD}\{b, r\}$$

である．

[**証明**] 整数 d $(d \neq 0)$ をとる．d が a, b の公約数とすると

$$a = da', \qquad b = db'$$

なる整数 a', b' が存在するが，このとき

$$r = a - qb = d(a' - qb')$$

となり，$a' - qb'$ は整数だから， d は r の約数となる．即ち d は b, r の公約数である．逆に d が b, r の公約数とすると

$$b = db', \qquad r = dr'$$

なる整数 b', r' が存在するが，このとき

$$a = qb + r = d(qb' + r')$$

となり，$qb' + r'$ は整数だから，d は a の約数となる．即ち d は a, b の公約数である．以上の事から，集合として

$$\{a, b \text{ の公約数 }\} = \{b, r \text{ の公約数 }\}$$

となるから，この中の最大の整数は等しい．即ち $\mathrm{GCD}\{a, b\} = \mathrm{GCD}\{b, r\}$ となる．■

Euclid の互除法
整数 a, b $(b > 0)$ をとる．a を b で割った商を q_1, 余りを r_1 として

$$a = q_1 b + r_1, \qquad 0 < r_1 < b$$

とする．b を r_1 で割った商を q_2，余りを r_2 として

$$b = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1$$

とする．r_1 を r_2 で割った商を q_3, 余りを r_3 として，以下同様に

$$\begin{aligned}
r_1 &= q_3 r_2 + r_3, \qquad 0 < r_3 < r_2 \\
r_2 &= q_4 r_3 + r_4, \qquad 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, \qquad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

とする．余りは

$$b > r_1 > r_2 > r_3 > \cdots \geqq 0$$

という具合に，次々と小さくなるが，全体としては正またはゼロだから，いつかは余りがゼロとなる，即ち，割り切れることになる．

ここで定理 2.3.1 を用いると

$$\begin{aligned}
\mathrm{GCD}\{a, b\} &= \mathrm{GCD}\{b, r_1\} \\
&= \mathrm{GCD}\{r_1, r2\} \\
&= \mathrm{GCD}\{r_2, r_3\} \\
&= \cdots \\
&= \mathrm{GCD}\{r_{n-1}, r_n\} = r_n
\end{aligned}$$

となる．即ち，最後の余り r_n が a, b の最大公約数となる．これを **Euclid の互除法**と呼ぶ．

注意 2.3.2 Euclid の互除法をほかの問題に応用するときに便利に使うために，上の形の計算結果を残しておくと良い．特に最初に与えられる整数 a, b は文字で残すようにすること．

例 2.3.3 $a = 4389, b = 1014$ として，Euclid の互除法を適用してみよう．

$$\begin{aligned}
a &= 4 \cdot b + 333 \\
b &= 3 \cdot 333 + 15 \\
333 &= 22 \cdot 15 + 3 \\
15 &= 5 \cdot 3
\end{aligned}$$

より $\mathrm{GCD}\{4389, 1014\} = 3$ である．

整数 a, b $(b > 0)$ に Euclid の互除法を用いて最大公約数 $\mathrm{GCD}\{a, b\}$ が求

められる：

$$\begin{aligned}
a &= q_1 b + r_1, \qquad 0 < r_1 < b \\
b &= q_2 r_1 + r_2, \qquad 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, \qquad 0 < r_3 < r_2 \\
r_2 &= q_4 r_3 + r_4, \qquad 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, \qquad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n \qquad r_n = \mathrm{GCD}\{a, b\}.
\end{aligned}$$

このとき，最初の式から順番に

$$\begin{aligned}
r_1 &= a - q_1 b \\
r_2 &= b - q_2 r_1 = b - q_2(a - q_1 b) \\
&= (-q_2)a + (1 + q_2 q_1)b \\
r_3 &= r_1 - q_3 r_2 = a - q_1 b - q_3\{(-q_2)a + (1 + q_2 q_1)b\} \\
&= (1 + q_3 q_2)a + \{-q_1 - q_3(1 + q_2 q_1)\}b \\
&\vdots
\end{aligned}$$

となって

$$r_n = A \cdot a + B \cdot b$$

なる整数 A, B が求められる．

例 2.3.4 $a = 4389, b = 1014$ とする．例 2.3.3 から

$$\begin{aligned}
333 &= a - 4b \\
15 &= b - 3 \cdot 333 = b - 3 \cdot (a - 4b) \\
&= (-3)a + 13b \\
3 &= 333 - 22 \cdot 15 = a - 4b - 22 \cdot (-3a + 13b) \\
&= 67 \cdot a - 290 \cdot b
\end{aligned}$$

ここで $\mathrm{GCD}\{a, b\} = 3$ だから

$$67 \cdot a + (-290) \cdot b = \mathrm{GCD}\{a, b\}$$

となる．

次の定理に注意すると，一般の $\{a_1, a_2, \cdots, a_r\} \subset \mathbb{Z}$ に対して，

$$a_1 A_1 + a_2 A_2 + \cdots + a_r A_r = \mathrm{GCD}\{a_1, a_2, \cdots, a_r\}$$

なる $A_i \in \mathbb{Z}$ $(i = 1, 2, \cdots, r)$ を求めることができる：

定理 2.3.5 正数 $a_1, a_2, \cdots, a_r$ $(r \geq 3)$ に対して

$$\mathrm{GCD}\{a_1, a_2, \cdots, a_r\} = \mathrm{GCD}\left\{\mathrm{GCD}\{a_1, a_2\}, a_3, \cdots, a_r\right\}.$$

[証明] 定理 2.2.5 から

$$\begin{aligned}
&\{a_1, a_2, \cdots, a_r \text{ の公約数 }\} \\
=&\{a_1, a_2 \text{ の公約数 }\} \cap \{a_3, \cdots, a_r \text{ の公約数 }\} \\
=&\{\mathrm{GCD}\{a_1, a_2\} \text{ の約数 }\} \cap \{a_3, \cdots, a_r \text{ の公約数 }\} \\
=&\{\mathrm{GCD}\{a_1, a_2\}, a_3 \cdots, a_r \text{ の公約数 }\}
\end{aligned}$$

よって $\{a_1, a_2, \cdots, a_r$ の公約数 $\}$ の最大の整数である $\mathrm{GCD}\{a_1, a_2, \cdots, a_r\}$ は $\{\mathrm{GCD}\{a_1, a_2\}, a_3 \cdots, a_r$ の公約数 $\}$ の最大の整数である

$$\mathrm{GCD}\left\{\mathrm{GCD}\{a_1, a_2\}, a_3, \cdots, a_r\right\}$$

に等しい．■

課題 2.4 $a = 19561222, b = 19560124$ として

1) 最大公約数 $\mathrm{GCD}\{a, b\}$ を Euclid の互除法を用いて求めよ．

2) $A \cdot a + B \cdot b = \mathrm{GCD}\{a, b\}$ となる整数 A, B を求めよ．

課題 2.5 $a = 1482, b = 3230, c = 4389$ とする．Euclid の互除法を用いて

1) $\mathrm{GCD}\{a, b, c\}$ を求めよ．

2) $Aa + Bb + Cc = \mathrm{GCD}\{a, b, c\}$ なる整数 A, B, C を一組求めよ．

課題 2.6 整数 $a_1, a_2, \cdots, a_r$ $(r \geq 3)$ に対して

$$\mathrm{GCD}\{a_1, a_2, \cdots, a_r\} = \mathrm{GCD}\left\{\mathrm{GCD}\{a_1, \cdots, a_k\}, a_{k+1}, \cdots, a_r\right\} \quad (1 < k < r)$$

であることを示せ．

3 剰余類環

3.1 イデアルを法とする合同式

環 A のイデアル $\mathfrak{a} \subset A$ を一つ固定して考える．

定義 3.1.1 $a, b \in A$ に対して，$a - b \in \mathfrak{a}$ のとき $\mathfrak{a}$ を法として a は B に合同といい

$$a \equiv b \pmod{\mathfrak{a}}$$

と書く．

合同に関して基本的なこと次の二つの定理である：

定理 3.1.2　1) 任意の $a \in A$ に対して $a \equiv a \pmod{\mathfrak{a}}$,

2) 任意の $a, b \in A$ に対して

$$a \equiv b \pmod{\mathfrak{a}} \;\Rightarrow\; b \equiv a \pmod{\mathfrak{a}},$$

3) 任意の $a, b, c \in A$ に対して

$$a \equiv b \pmod{\mathfrak{a}},\ b \equiv c \pmod{\mathfrak{a}} \;\Rightarrow\; a \equiv c \pmod{\mathfrak{a}}$$

が成り立つ.

[証明]

1) 注意 2.1.2 より $a - a = 0 \in \mathfrak{a}$ だから $a \equiv a \pmod{\mathfrak{a}}$ である.

2) $a - b \in \mathfrak{a}$ で $-1 \in A$ だから $b - a = (-1) \cdot (a - b) \in \mathfrak{a}$. よって $b \equiv a \pmod{\mathfrak{a}}$ となる.

3) $a - b = s \in \mathfrak{a}, b - c = t \in \mathfrak{a}$ だから $a - c = s = t \in \mathfrak{a}$, よって $a \equiv c \pmod{\mathfrak{a}}$ である.

■

定理 3.1.3 $a, a', b, b' \in A$ に対して

$$a \equiv a' \pmod{\mathfrak{a}}, \qquad b \equiv b' \pmod{\mathfrak{a}}$$

ならば

1) $a + b \equiv a' + b' \pmod{\mathfrak{a}}$, $a - b \equiv a' - b' \pmod{\mathfrak{a}}$,

2) $ab \equiv a'b' \pmod{\mathfrak{a}}$

である.

[証明] 仮定から $a - a' = s \in \mathfrak{a}, b - b' = t \in \mathfrak{a}$ である.

$$(a + b) - (a' + b') = s + t \in \mathfrak{a}, \qquad (a - b) - (a' - b') = s - t \in \mathfrak{a}$$

だから $a + b \equiv a' + b' \pmod{\mathfrak{a}}$, $a - b \equiv a' - b' \pmod{\mathfrak{a}}$ である. また

$$ab - a'b' = a(b - b') + (a - a')b' = as + b't \in \mathfrak{a}$$

だから $ab \equiv a'b' \pmod{\mathfrak{a}}$ である. ■

課題 3.1 $0 < N \in \mathbb{Z}$ としてイデアル $(N) \subset \mathbb{Z}$ を考える．任意の整数 $a, b \in \mathbb{Z}$ に対して，次は同値であることを示せ：

1) $a \equiv b (\mathrm{mod}\ (N))$,

2) $a - b$ が N で割り切れる，

3) a を N で割った余りと，b を N で割った余りが等しい．

このとき $a \equiv b (\mathrm{mod}\ N)$ と書いて，N を法として a は b に合同という．

課題 3.2 1) $10^n \equiv (-1)^n (\mathrm{mod}\ 11)$ $(n = 0, 1, 2, 3, \cdots)$ を示せ．

2) 12345678901234567 を 11 で割った余りは

$$7 - 6 + 5 - 4 + 3 - 2 + 1 - 0 + 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1$$

を 11 で割った余りと等しいことを，1) の結果を用いて説明せよ．

3.2 剰余類と剰余類環

環 A のイデアル $\mathfrak{a} \subset A$ を一つ固定して考える．

定義 3.2.1 $a \in A$ に対して

$$\overline{a} = \{x \in A \mid x \equiv a \pmod{\mathfrak{a}}\}$$

を $\mathfrak{a}$ **を法とした** a **の剰余類**と呼ぶ．$\mathfrak{a}$ を法とした剰余類の全体を $A/\mathfrak{a}$ と表す．

例 3.2.2 整数環 $\mathbb{Z}$ のイデアル (6) を法とした剰余類は，課題 3.1 より，6 で割った余りが同じ整数を集めたものだから

$$\mathbb{Z}/(6) = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\right\}$$

である．

定理 3.2.3 環 A のイデアル $\mathfrak{a}|subset A$ を法とした剰余類の全体 $A/\mathfrak{a}$ に，加法と乗法を次のように定義して，$A/\mathfrak{a}$ を環にすることが出来る：

$$\text{加法：}\ \overline{a} + \overline{b} \overset{\text{def.}}{=} \overline{a + b},$$
$$\text{乗法：}\ \overline{a} \cdot \overline{b} \overset{\text{def.}}{=} \overline{a \cdot b}.$$

これを $\mathfrak{a}$ **を法とした剰余類環**と呼ぶ．

$A/\mathfrak{a}$ の 0 は $\overline{0_A}$ であり，$A/\mathfrak{a}$ の 1 は $\overline{1_A}$ である．

[証明] 定理 3.1.3 により，加法と乗法が well-defined であることに注意しよう．これらの演算により $A/\mathfrak{a}$ が環となることを確かめるのは演習課題とする．
■

例 3.2.4 例 3.2.2 の剰余類環 $\mathbb{Z}/(6)$ で

$$\overline{2}+\overline{3}=\overline{5},\quad \overline{2}\cdot\overline{3}=\overline{6}=\overline{0}$$

である．

課題 3.3 定理 3.2.3 で定義した加法と乗法により $A/\mathfrak{a}$ が環となることを確かめよ．

課題 3.4 例 1.1.8 の 1) で定義した環 $A=\mathbb{Z}\times\mathbb{Z}$ について

1) $\mathfrak{a}=\{(x,0)\mid x\in\mathbb{Z}\}$ は A のイデアルであることを示せ．

2) 剰余類環 $A/\mathfrak{a}$ は整域であることを示せ．

3) 剰余類環 $A/\mathfrak{a}$ は体ではないことを示せ．

3.3 素イデアルと極大イデアル

定義 3.3.1 環 A のイデアル $\mathfrak{a}\subsetneqq A$ に対して

1) 剰余類環 $A/\mathfrak{a}$ が整域となるとき，$\mathfrak{a}$ を A の**素イデアル**と呼ぶ．

2) 剰余類環 $A/\mathfrak{a}$ が体となるとき，$\mathfrak{a}$ を A の**極大イデアル**と呼ぶ．

注意 3.3.2 1) 体は整域だから，$\mathfrak{a}$ が A の極大イデアルならば $\mathfrak{a}$ は A の素イデアルとなる．

2) 課題 3.4 で見たように，一般には $\mathfrak{a}$ が A の素イデアルであっても，$\mathfrak{a}$ が A の極大イデアルになるとは限らない．

次の定理は極大イデアルという呼び名の由来を示している：

定理 3.3.3 環 A のイデアル $\mathfrak{a}\subsetneqq A$ に対して次は同値である：

1) $\mathfrak{a}$ は A の極大イデアルである．

2) $\mathfrak{a}\subset\mathfrak{b}\subset A$ なる A のイデアル $\mathfrak{b}$ は $\mathfrak{a}$ または A に限る（言い換えれば，$\mathfrak{a}$ は A のイデアルの集合で，包含関係に関する極大元である）．

[証明] 1) $\Rightarrow$ 2) $\mathfrak{a} \subsetneqq \mathfrak{b}$ とする．$\mathfrak{a}$ に含まれない $c \in \mathfrak{b}$ がとれる．$c \notin \mathfrak{a}$ だから，剰余類環 $A/\mathfrak{a}$ で $\overline{c} \neq 0$ である．仮定から $A/\mathfrak{a}$ は体だから $\overline{c} \cdot \overline{d} = 1$ なる $\overline{d} \in A/\mathfrak{a}$ が存在する．即ち $cd \equiv 1 (\mathrm{mod}\ \mathfrak{a})$ なる $d \in A$ がとれる．このとき $1 - cd = a \in \mathfrak{a} \subset \mathfrak{b}$ であり，$cd \in \mathfrak{b}$ だから $1 = a + cd \in \mathfrak{b}$ となり，$\mathfrak{b} = A$ となる．

2) $\Rightarrow$ 1) $0 \neq \overline{a} \in A/\mathfrak{a}$ とする．即ち $a \notin \mathfrak{a}$ なる $a \in A$ をとる．

$$\mathfrak{b} = \{x + ay \mid x \in \mathfrak{a}, y \in A\}$$

は A のイデアルで，$\mathfrak{a} \subset \mathfrak{b}$ かつ $a \in \mathfrak{b}$ だから $\mathfrak{a} \subsetneqq \mathfrak{b}$ となる．よって仮定から $\mathfrak{b} = A$ となる．よって $1 \in A = \mathfrak{b}$ となるから，$1 = x + ay$ なる $x \in \mathfrak{a}, y \in A$ が存在する．このとき

$$1 - ay = x \in \mathfrak{a}, \qquad \therefore\ ax \equiv 1 \pmod{\mathfrak{a}}$$

となるから，剰余類環 $A/\mathfrak{a}$ で $\overline{a} \cdot \overline{y} = 1$ となる．よって $A/\mathfrak{a}$ は体となり，$\mathfrak{a}$ は A の極大イデアルとなる．■

実際に極大イデアルが存在することは，次の定理によって保障される．一般の環で証明するためには **Zorn の補題**を用いる必要があるので，ここでは省略する（定理 4.3.6 参照）．

定理 3.3.4 $\mathfrak{a} \subsetneqq A$ なる A のイデアル $\mathfrak{a}$ に対して，$\mathfrak{a} \subset \mathfrak{p}$ なる A の極大イデアル $\mathfrak{p}$ が存在する．

次の定理は特殊な環における素イデアル，極大イデアルの重要性を示している：

定理 3.3.5 整数 $1 < p \in \mathbb{Z}$ に対して，次は同値である：

1) p は素数である．

2) 単項イデアル $(p) \subset \mathbb{Z}$ は素イデアルである．

3) 単項イデアル $(p) \subset \mathbb{Z}$ は極大イデアルである．

[証明] 1) $\Rightarrow$ 3) 剰余類環 $\mathbb{Z}/(p)$ が体であることを示せばよい．$0 \neq \overline{a} \in \mathbb{Z}/(p)$ をとる．$p \not\equiv 0 (\mathrm{mod}\ (p))$ だから $a \notin (p)$，即ち p は a の約数でない．p は素数だから $\mathrm{GCD}\{a, p\} = 1$ となる．よって系 2.2.4 より $aB + pB = 1$ なる整数 $A, B \in \mathbb{Z}$ が存在する．このとき

$$1 - aA = pB \in (p) \qquad \therefore\ aA \equiv a \pmod{(p)}$$

となるから，剰余類環 $\mathbb{Z}/(p)$ において $\overline{a} \cdot \overline{A} = 1$ となる．

3) $\Rightarrow$ 2) 注意 3.3.2 の 1) にあるように，これはいつでも成り立つ．

2) $\Rightarrow p = ab$ $(a, b \in \mathbb{Z})$ とすると，$ab = p \in (p)$ だから $ab \equiv 0 \pmod{(p)}$，即ち剰余類環 $\mathbb{Z}/(p)$ において $\overline{a} \cdot \overline{b} = 0$ となる．仮定から剰余類環 $\mathbb{Z}?(p)$ は整域だから，$\overline{a} = 0$ または $\overline{b} = 0$ である．$\overline{a} = 0$ とすると，$a \in (p)$，即ち $a = pc$ $(c \in \mathbb{Z})$ と書けるから

$$p = ab = pcb \qquad \therefore\ p(1 - cb) = 0 \qquad \therefore\ cb = 1$$

となる．$b, c \in \mathbb{Z}$ だから $b = \pm 1$ となる．よって p は素数である．■

注意 3.3.6 系 2.2.7 は，p が素数ならば，剰余類環 $\mathbb{Z}/(p)$ は整域であることを主張している．

4　単項イデアル整域

4.1　多項式環のイデアル

体 K 上の一変数多項式環 $K[X]$ のイデアルを詳しく見てみよう．まず次の命題が基本的である：

命題 4.1.1 (多項式の剰余の定理) $f(X), g(X) \in K[X]$ $(g(X) \neq 0)$ に対して

$$f(X) = h(X) \cdot g(X) + r(X), \quad r(X) = 0 \text{ または } \deg r(X) < \deg g(X)$$

なる $h(X), r(X) \in K[X]$ が唯一存在する．

この命題から次の定理が導かれる：

定理 4.1.2 $K[X]$ のイデアル $\mathfrak{a} \supsetneqq \{0\}$ に対して，$\mathfrak{a}$ に含まれる 0 でない多項式で次数最小のものを $d(X)$ とすると

$$\mathfrak{a} = (d(X)) = \{d(X) \cdot h(X) \mid h(X) \in K[X]\}$$

である．

[証明] $d(X) \in \mathfrak{a}$ だから $(d(X)) \subset \mathfrak{a}$ は明らかである．任意の $f(X) \in \mathfrak{a}$ をとる．命題 4.1.2 より

$$f(X) = h(X) \cdot d(X) + r(X), \quad r(X) = 0 \text{ または } \deg r(X) < \deg d(X)$$

なる $h(X), r(X) \in K[X]$ が存在する．ここで $r(X) \neq 0$ と仮定する．$f(X) \in \mathfrak{a}$ かつ $h(X) \cdot d(X) \in (d(X)) \subset \mathfrak{a}$ だから

$$r(X) = f(X) - h(X) \cdot d(X) \in \mathfrak{a} \text{ かつ } \deg r(X) < \deg d(X)$$

である．これは $d(X)$ の定義に反する．よって $r(X) = 0$ である．よって $f(X) = h(X) \cdot d(X) \in (d(X))$ となる．よって $\mathfrak{a} \subset (d(X))$ となる．以上から $\mathfrak{a} = (d(X))$ である．■

課題 4.1 多項式環 $\mathbb{Q}[X]$ のイデアル

$$\mathfrak{a} = \{f(X) \in \mathbb{Q}[X] \mid f(\sqrt{2}) = 0\}$$

に対して，$\mathfrak{a} = (p(X))$ となる多項式 $p(X) \in \mathbb{Q}[X]$ で最高次の係数が 1 であるものを求めよ．

4.2 Gauss の整数環のイデアル

Gauss の整数環

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \qquad (i^2 = -1)$$

のイデアルを詳しく調べてみよう．まず次の命題から始める：

命題 4.2.1 $\alpha, \beta \in \mathbb{Z}[i]$ $(\beta \neq 0)$ に対して

$$\alpha = \gamma\beta + \delta \qquad |\delta| < |\beta|$$

なる $\gamma, \delta \in \mathbb{Z}[i]$ が存在する．

[証明] $\mathbb{Z}[i]$ の元の複素平面 $\mathbb{C}$ 上の位置関係を考えると，$\dfrac{\alpha}{\beta} \in \mathbb{C}$ に対して

$$\left|\frac{\alpha}{\beta} - \gamma\right| \leq \frac{\sqrt{2}}{2}$$

なる $\gamma \in \mathbb{Z}[i]$ が存在することが判る．$\delta = \alpha - \gamma\beta \in \mathbb{Z}[i]$ とおけば，$\alpha = \gamma\beta + \delta$ かつ

$$|\delta| = \left|\frac{\alpha}{\beta} - \gamma\right| \cdot |\beta| \leq \frac{\sqrt{2}}{2} \cdot |\beta| < |\beta|$$

となる．■

定理 4.2.2 $\mathbb{Z}[i]$ のイデアル $\mathfrak{a} \supsetneqq \{0\}$ に対して，$\mathfrak{a}$ に含まれる 0 でない元で絶対値が最小のものを $\beta \in \mathfrak{a}$ とすると

$$\mathfrak{a} = (\beta) = \{\beta \cdot \gamma \mid \gamma \in \mathbb{Z}[i]\}$$

である．

[証明] $\beta \in \mathfrak{a}$ だから $(\beta) \subset \mathfrak{a}$ は明らか．任意の $\alpha \in \mathfrak{a}$ をとる．命題 4.2.1 より

$$\alpha = \gamma \cdot \beta + \delta \qquad |\delta| < |\beta|$$

なる $\gamma, \delta \in \mathbb{Z}[i]$ が存在する．ここで $\delta \neq 0$ と仮定すると，$\alpha \in \mathfrak{a}, \gamma\beta \in (\beta) \subset \mathfrak{a}$ だから

$$\delta = \alpha - \gamma\beta \in \mathfrak{a}, \qquad 0 < |\delta| < |\beta|$$

となり，β の取り方に反する．よって $\delta = 0$ である．よって $\alpha = \gamma \cdot \beta \in (\beta)$ となる．従って $\mathfrak{a} \subset (\beta)$ となる．よって $\mathfrak{a} = (\beta)$ である．■

課題 4.2 Gauss の整数環 $\mathbb{Z}[i]$ の場合を参考にして，$\mathbb{Z}[\omega]$ (例 1.1.11 参照) に関して次の事を示せ：

1) $\alpha, \beta \in \mathbb{Z}[\omega]$ $(\beta \neq 0)$ に対して

$$\alpha = \gamma\beta + \delta \qquad |\delta| < |\beta|$$

なる $\gamma, \delta \in \mathbb{Z}[\omega]$ が存在する．

2) $\mathbb{Z}[\omega]$ は単項イデアル整域である．

4.3 単項イデアル整域の定義と基本的な性質

定義 4.3.1 環 A が整域でありかつ，A の任意のイデアルが単項イデアルであるとき，環 A を単項イデアル整域 (Principal Ideal Domain=P.I.D.) と呼ぶ．

例 4.3.2 定理 2.2.2 より整数環 $\mathbb{Z}$ は単項イデアル整域である．

例 4.3.3 定理 4.1.2 より，体 K 上の一変数多項式環 $K[X]$ は単項イデアル整域である．

例 4.3.4 定理 4.2.2 より，Gauss の整数環 $\mathbb{Z}[i]$ は単項イデアル整域である．

単項イデアル整域の最も基本的な性質は

定理 4.3.5 単項イデアル整域 A のイデアルの増加列

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n \subset \mathfrak{a}_{n+1} \subset \cdots$$

があれば，番号 N があって $\mathfrak{a}_{N+k} = \mathfrak{a}_N$ $(k = 1, 2, 3 \cdots)$ となる．

[証明] $\mathfrak{a} = \bigcup_{n=1}^{\infty} \mathfrak{a}_n$ は A のイデアルとなる：実際，$x, y \in \mathfrak{a}$ とすると $x \in \mathfrak{a}_l, y \in \mathfrak{a}_m$ なる番号 l, m がとれる．$n = \mathrm{Max}\{l, m\}$ とおくと，$x, y \in \mathfrak{a}_n$ だから $x + y \in \mathfrak{a}_n \subset \mathfrak{a}$．また任意の $a \in A$ に対して $ax \in \mathfrak{a}_n \subset \mathfrak{a}$ となる．A は単項イデアル整域だから $\mathfrak{a} = (a)$ なる $a \in A$ が存在する．$a \in \mathfrak{a}_N$ とすると，$k = 1, 2, 3, \cdots$ に対して

$$\mathfrak{a}_{N+k} \subset \mathfrak{a} = (a) \subset \mathfrak{a}_N \subset \mathfrak{a}_{N+k}$$

となるから $\mathfrak{a}_{N+k} = \mathfrak{a}_N$ となる．■

この定理から次の重要な結果が示される：

定理 4.3.6 単項イデアル整域 A の任意のイデアル $\mathfrak{a} \subsetneqq A$ に対して，$\mathfrak{a} \subset \mathfrak{p}$ なる A の極大イデアル $\mathfrak{p}$ が存在する．

[証明] A のイデアル $\mathfrak{a} \subsetneqq A$ を含む A の極大イデアルが存在しないと仮定する．$\mathfrak{a} \subsetneqq A$ は A の極大イデアルではないから，$\mathfrak{a} \subsetneqq \mathfrak{a}_1 \subsetneqq A$ なる A のイデアル $\mathfrak{a}_1$ がとれる．$\mathfrak{a}_1 \subsetneqq A$ は A の極大イデアルではないから，$\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq A$ なる A のイデアル $\mathfrak{a}_2$ がとれる．以下同様に繰り返すと

$$\mathfrak{a} \subsetneqq \mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \mathfrak{a}_3 \subsetneqq \cdots$$

なる A のイデアルの列 $\mathfrak{a}_n$ $(n = 1, 2, 3, \cdots)$ ができる．これは定理 4.3.5 に反する．■

4.4 単項イデアル整域の素元

この節では A は単項イデアル整域であるとする．整数環 $\mathbb{Z}$ を参考にして，次のように定義する：

定義 4.4.1 p が次の二つの条件を満たすとき，p は A の**素元**（または**既約元**）であるという：

1) $p \neq 0$ かつ $p \notin A^\times$,

2) $p = ab$ $(a, b \in A)$ ならば $a \in A^\times$ または $b \in A^\times$.

整数環の場合と同様に次の定理が成り立つ：

定理 4.4.2 $p \in A$ は $p \neq 0$ かつ $p \notin A^\times$ とする．このとき次は同値である：

1) p は A の素元である．

2) 単項イデアル (p) は A の素イデアルである．

3) 単項イデアル (p) は A の極大イデアルである．

[証明] 1) $\Rightarrow$ 3) $(p) \subset \mathfrak{a}$ なる A のイデアル $\mathfrak{a}$ を考える．A は単項イデアル整域だから $\mathfrak{a} = (a)$ なる $a \in A$ が存在する．

$$p \in (p) \subset \mathfrak{a} = (a) = \{ax \mid x \in A\}$$

だから $p = ab$ なる $b \in A$ がとれる．1) を仮定しているから，$a \in A\times$ または $b \in A\times$ である．$a \in A^\times$ ならば $\mathfrak{a} = (a) = A$ であり，$b \in A^\times$ ならば $(p) = (a) = \mathfrak{a}$ である．よって (p) は A の極大イデアルである．

3) $\Rightarrow$ 2) は明らか．

2) $\Rightarrow$ 1) $p = ab$ $(a, b \in A)$ とする．$ab = p \in (p)$ だから，剰余類環 $A/(p)$ で $\overline{a} \cdot \overline{b} = 0$ である．(p) は A の素イデアルと仮定しているから，$A/(p)$ は整

域だえる．よって $A/(p)$ で $\overline{a}=0$ または $\overline{b}=0$ となる．即ち $a\in(p)$ または $b\in(p)$ である．$a\in(p)$ とすると $a=pc$ なる $c\in A$ がとれる．よって

$$p=ab=pcb \qquad \therefore\ p(bc-1)=0$$

となる．A は整域で $p\neq 0$ だから $bc-1=0$，即ち $bc=1$ となり，$b\in A^{\times}$ である．■

上の定理を少し言い換えると次の定理が得られる：

定理 4.4.3 1) A の素元 p が積 $a_1a_2\cdots a_r$ $(a_i\in A)$ を割り切るならば，p は $a_1,a_2,\cdots,a_r$ の何れかを割り切る．

2) $0\neq a\in A$ に対して，$a\notin A^{\times}$ のとき，a が A の素元でなければ a を割り切る A の素元が存在する．

[証明] 1) p が積 $a_1a_2\cdots a_r$ を割り切るから，$a_1a_2\cdots a_r\in(p)$ となり，これは

$$\overline{a}_1\cdot\overline{a}_2\cdots\overline{a}_r=\overline{a_1a_2\cdots a_r}=0\in A/(p)$$

を意味する．p は A の素元だから，定理 4.4.2 より剰余類環 $A/(p)$ は整域である．よって $\overline{a}_i\in A/(p)$ $(i=1,2,\cdots,r)$ の何れかは 0 である．$\overline{a}_1=0\in A/(p)$ とすると，$a_1\in(p)$ となる，これは $p|a_1$ を意味する．

2) $a\notin A^{\times}$ だから $(a)\gneqq A$ である．a は A の素元ではないから，定理 4.4.2 より $(a)\gneqq A$ は A の極大イデアルではない．よって定理 4.3.6 より $(a)\subset\mathfrak{p}\subset A$ なる A の極大イデアル $\mathfrak{p}$ が存在する．$\mathfrak{p}=(p)$ とすると p は A の素元であり

$$a\in(a)\subset\mathfrak{p}=(p)$$

だから，p は a を割り切る．■

例 4.4.4 整数環 $\mathbb{Z}$ は単項イデアル整域だから（例 4.3.2），定理 4.4.2 を $\mathbb{Z}$ に適用してみると，$\mathbb{Z}^{\times}=\{\pm1\}$ だから

$$\mathbb{Z}\text{ における素元}=\pm1\times\text{正の素数}$$

であることがわかる．

例 4.4.5 体 K 上の一変数多項式環 $K[X]$ は単項イデアル整域だから（例 4.3.3），定理 4.4.2 を $K[X]$ に適用してみると

$$K[X]^{\times}=\{0\neq c\in K\}=\{f(x)\in K[X]\mid \deg f(X)=0\}$$

だから，$p(X)\in K[X]$ が $p(X)\neq 0$ かつ $\deg p(X)\geq 1$ に対して次は同値である：

1) $p(X)$ は $K[X]$ の素元（即ち，既約元）である．

2) $p(X) = f(X)g(X)$ $(f(X), g(X) \in K[X])$ ならば $\deg f(X) = 0$ または $\deg g(X) = 0$ である．

このとき $p(X)$ を K **上の既約多項式**とよぶ.

注意 4.4.6 一般に多項式の既約性は，係数を数のどのような体で考えるかによって変化する．例えば $X^2 - 2 \in \mathbb{Q}[X]$ を考えると

$$X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2}) \qquad (\pm\sqrt{2} \in \mathbb{R})$$

だから $X^2 - 2$ は $\mathbb{R}$ 上では既約でない．しかし $X^2 - 2$ は $\mathbb{Q}$ 上では既約多項式である；実際,

$$X^2 - 2 = f(X)g(X) \qquad (f(X), g(X) \in \mathbb{Q}[X])$$

とおくと

$$\deg f(X) + \deg g(X) = \deg(X^2 - 2) = 2$$

だから

$$\begin{cases} \deg f(X) = 2, \\ \deg g(X) = 0 \end{cases}, \text{ または } \begin{cases} \deg f(X) = 1, \\ \deg g(X) = 1 \end{cases}, \text{ または } \begin{cases} \deg f(X) = 0, \\ \deg g(X) = 2 \end{cases},$$

である．$\deg f(X) = \deg g(X) = 1$ とすると

$$f(X) = aX + b, \;\; g(X) = cX + d \;\; (a, b, c, d \in \mathbb{Q}, a \neq 0, c \neq 0)$$

となるから $X^2 - 2 = (aX + b)(cX + d)$ となる．よって $\pm\sqrt{2} = -\dfrac{a}{b}, -\dfrac{c}{d}$ となり，$\sqrt{2} \in \mathbb{Q}$ となるが，これは矛盾である．よって $\deg f(X) = 0$ または $\deg g(X) = 0$ となる．

このように係数を考える体を大きくすると，既約な多項式が既約でなくなる場合がある．

例 4.4.7 1) $1 + i$ は Gauss の整数環 $\mathbb{Z}[i]$ の素元である．

2) 3 は Gauss の整数環 $\mathbb{Z}[i]$ の素元である．

[**証明**] 定理 1.3.4 の証明でも利用したように，$\alpha \in \mathbb{Z}[i]$ に対して $N(\alpha) = \alpha \cdot \overline{\alpha} \in \mathbb{Z}$ であり，$\alpha, \beta \in \mathbb{Z}[i]$ に対して $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$ である．このことを利用して

1) $1 + i = \alpha \cdot \beta$ $(\alpha, \beta \in \mathbb{Z}[i])$ とする．

$$2 = N(1 + i) = N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$$

だから $N(\alpha) = 1$ または $N(\beta) = 1$ となる．よって $\alpha \in \mathbb{Z}[i]^\times$ または $\beta \in \mathbb{Z}[i]^\times$ となる．よって $1 + i$ は $\mathbb{Z}[i]$ の素元である．

2) $3 = \alpha \cdot \beta$ $(\alpha, \beta \in \mathbb{Z}[i])$ とすると，

$$9 = N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$$

だから，$N(\alpha) = 1, 3, 9$ である．$N(\alpha) = 3$ とすると，$\alpha = a + bi$ $(a, b \in \mathbb{Z})$ と書けるから，$3 = a^2 + b^2$ となる．すると

$$|a|, |b| \leq \sqrt{3} = 1.732\cdots \quad \therefore a, b = 0, \pm 1$$

となり，$a^2 + b^2 = 3$ とは成り得ないことが判る．よって $N(\alpha) = 1, 9$ であるが，$N(\alpha) = 9$ ならば $N(\beta) = 1$ だから，$N(\alpha) = 1$ または $N(\beta) = 1$ である．よって $\alpha \in \mathbb{Z}[i]^\times$ または $\beta \in \mathbb{Z}[i]^\times$ である．よって 3 は $\mathbb{Z}[i]$ の素元である．

■

課題 4.3 素数 $5, 7$ について次の問いに答えよ：

1) 5 は Gauss の整数環 $\mathbb{Z}[i]$ の素元ではないことを示せ．

2) 7 は Gauss の整数環 $\mathbb{Z}[i]$ の素元であることを示せ．

課題 4.4 $\pi \in \mathbb{Z}[i]$ に対して $N(\pi) = p$ が素数ならば，π は Gauss の整数環 $\mathbb{Z}[i]$ の素元であることを示せ．

課題 4.5 奇数の素数 p に対して $p \not\equiv 1 \pmod 4$ ならば，p は Gauss の整数環 $\mathbb{Z}[i]$ の素元であることを示せ．

4.5 単項イデアル整域における素因子分解

この節では A は単項イデアル整域であるとする．
定理 4.4.3 の 1) から次の定理が得られる：

定理 4.5.1 A の素元 p_i $(i = 1, 2, \cdots, r)$ と q_j $(j = 1, 2, \cdots, s)$ に対して

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

ならば，

1) $r = s$,

2) 番号を付け直せば

$$(p_1) = (q_1),\ (p_2) = (q_2),\ \cdots,\ (p_r) = (q_r)$$

とできる．

[証明] 単項イデアル整域 A の素元 p_1 が積 $q_1q_2\cdots q_s$ を割り切るから，定理 4.4.3 の 1) により，p_a は $q_1, q_2, \cdots, q_s$ の何れかを割り切る．番号を付け直せば p_1 は q_1 を割り切るとしてよい．即ち $q_1 = p_1 \cdot a_1$ なる $a_1 \in A$ が存在する．q_1 は A の素元だから $p_1 \in A^\times$ または $a_1 \in A^\times$ である．p_1 は A の素元だから $p_1 \notin A^\times$ である．よって $a_1 \in A^\times$ となるから

$$(p_1) = (q_1), \qquad p_2 \cdots p_r = a_1 q_2 \cdots q_s$$

である．A の素元 p_2 が積 $a_1q_2\cdots q_s$ を割り切るから，定理 4.4.3 の 1) より，p_2 は $a_1, q_2, \cdots, q_s$ の何れかを割り切る．$a_1 \in A^\times$ で p_2 は A の素元だから，p_2 が a_1 を割り切ることはない．よって番号を付け直して p_2 は q_2 を割り切るとしてよい．即ち $q_2 = p_2a_2$ なる $a_2 \in A$ が存在する．q_2 は A の素元だから，$p_2 \in A^\times$ または $a_2 \in A^\times$ である．p_2 は A の素元だから $p_2 \notin A^\times$ である．よって $a_2 \in A^\times$ となって

$$(p_2) = (q_2), p_3 \cdots p_r = a_1 a_2 q_3 \cdots q_s$$

となる．以下同様に続けることができる．ここで $r < s$ とすると

$$1 = a_1 \cdots a_r q_{r+1} \cdots q_s$$

となるが，これは $q_j \in A^\times$ $(r < j \leq s)$ を意味するから，q_j が A の素元であることに反する．よって $r \geq s$ である．一方 $r > s$ とすると

$$p_{s+1} \cdots p_r = a_1 a_2 \cdots a_s \in A^\times$$

となるが，これは $p_i \in A^\times$ $(s < i \leq r)$ を意味するから，p_i が A の素元であることに反する．よって $r = s$ となり，$q_1, q_2, \cdots, q_r$ の番号を付け直せば

$$(p_1) = (q_1),\ (p_2) = (q_2),\ \cdots,\ (p_r) = (q_r)$$

となる．■

定理 4.4.3 の 2) から次の定理が得られる：

定理 4.5.2 $a \in A$ が $a \neq 0$ かつ $a \notin A^\times$ ならば，a は環 A の素元の積として書くことができる．

[証明] a が A の素元の積として書けないと仮定する．a は A の素元ではないから，定理 4.4.3 の 2) より，a を割り切る A の素元 p_1 が存在する．$a = p_1a_1$ $(a_1 \in A)$ とおくと，$0 \neq a_1 \in A$ である． $a_1 \in A^\times$ ならば $(a) = (p_1)$ となり，(a) は A の極大イデアル，即ち a は A の素元となり仮定に反するから，$a_1 \notin A^\times$ である．更に a_1 は A の素元ではない．以下同様に続けると

$$a = p_1a_1, \quad a_1 = p_2a_2, \quad \cdots a_n = p_na_n \cdots$$

なる A の素元 p_i $(i = 1, 2, \cdots)$ と $a_i \in A$ $(i = 1, 2, \cdots)$ が取れる．ここで $p_i \notin A^\times$ だから，A の単項イデアルの増加列

$$(a) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq \cdots \subsetneqq (a_n) \quad (n = 1, 2, 3, \cdots)$$

が出来るが，これは定理 4.3.5 に反する．■

定理 4.5.2 と定理 4.5.1 を合わせると，単項イデアル整域 A について次の主張が成り立つことになる：

> $a \in A$ が $a \neq 0$ かつ $a \notin A^\times$ ならば
>
> $$a = p_1 p_2 \cdots p_r, \qquad p_i \ (i = 1, 2, \cdots, r) \text{ は } A \text{ の素元}$$
>
> と書ける．このとき単項イデアル $(p_1), (p_2), \cdots (p_r)$ は順序を除くと a に対して一意的に定まる．

これを単項イデアル整域における**素元分解の一意性**と呼ぶ．

例 4.5.3 例 4.4.4 を考慮すると

> 0 でない整数 $a \in \mathbb{Z}$ に対して
>
> $$a = \pm p_1 p_2 \cdots p_r, \qquad p_i \ (i = 1, 2, \cdots, r) \text{ は正の素数}$$
>
> と書ける．このとき $p_1, p_2, \cdots, p_r$ は順序を除いて一意的である

という，お馴染みの整数の素因数分解の一意性がいえる．

例 4.5.4 体 K 上の一変数多項式環 $K[X]$ について，例 4.4.5 を考慮すると

> 0 でない多項式 $f(X) \in K[X]$ に対して
>
> $$f(X) = c \cdot p_1(X) p_2(X) \cdots p_r(X),$$
>
> と書ける．ここで $0 \neq c \in K$ であり，$p_i(X)$ $(i = 1, 2, \cdots, r)$ は最高時の係数が 1 の K 上の既約多項式である．このとき，$p_1(X), p_2(X), \cdots, p_r(X)$ は順序を除いて一意的である．

これを**多項式の既約分解の一意性**と呼ぶ．

4.6 多項式の最大公約数

体 K 上の一変数多項式環 $K[X]$ が P.I.D. であることから，多項式の少し詳しい性質を調べてみよう．

多項式 $f_1(X), f_2(X), \cdots, f_r(X) \in K[X]$ が与えられたとする．これらが生成する $K[X]$ のイデアルは $K[X]$ の単項イデアルとなるから

$$(f_1(X), f_2(X), \cdots, f_r) = (d(X))$$

なる $d(X) \in K[X]$ が存在する．$i = 1, 2, \cdots, r$ に対して

$$f_i(X) \in (f_1(X), f_2(X), \cdots, f_r) = (d(X))$$

だから $d(X)|f_i(X)$ である．そこで $D(X) \in K[X]$ を

$$D(X)|f_i(X) \qquad (i = 1, 2, \cdots, r)$$

なる次数最大のものとすると $\deg d(X) \leq \deg D(X)$ である．一方

$$f_1(X)g_1(X) + f_2(X)g_2(X) + \cdots + f_r(X)g_r(X) = d(X)$$

なる $g_i(X) \in K[X]$ $(i = 1, 2, \cdots, r)$ が存在するから

$$D(X)|d(X) \qquad \therefore \quad \deg D(X) \leq \deg d(X)$$

である．よって $\deg D(X) = \deg d(X)$ となり，$d(X) = c \cdot D(X)$ なる $0 \neq c \in K$ がとれる．$K[X]$ の単数群は

$$K[X]^\times = \{0 \neq c \in K\}$$

だから，

$$(f_1(X), f_2(X), \cdots, f_r) = (D(X))$$

となる．よって次の定理が示された：

定理 4.6.1 多項式 $f_1(X), f_2(X), \cdots, f_r(X) \in K[X]$ に対して

1) $\{f_1(X), f_2(X), \cdots, f_r(X)\}$ を全て割り切る $K[X]$ の多項式で次数最大のものは，定数倍を除いて唯一存在する．その中で最高次の係数が 1 のものを $\{f_1(X), f_2(X), \cdots, f_r(X)\}$ の最大公約数と呼び

$$\mathrm{GCD}\{f_1(X), f_2(X), \cdots, f_r(X)\}$$

と表す.

2) $D(X) = \mathrm{GCD}\{f_1(X), f_2(X), \cdots, f_r(X)\}$ とおくと

$$(f_1(X), f_2(X), \cdots, f_r(X)) = (D(X))$$

である.

整数の場合と同様に，多項式の剰余の定理（命題 4.1.1）から，多項式の Euclid の互除法を導くことができる．まず

命題 4.6.2 $f(X), g(X) \in K[X]$ $(g(X) \neq 0)$ に対して，$f(X)$ を $g(X)$ で割って

$$f(X) = q(X) \cdot g(X) + r(X), \qquad r(X) = 0 \text{ 又は } \deg r(X) < \deg g(X)$$

なる $q(X), r(X) \in K[X]$ をとる（多項式の剰余の定理）．このとき

$$\mathrm{GCD}\{f(X), g(X)\} = \mathrm{GCD}\{g(X), r(X)\}$$

である．

[**証明**] 多項式 $0 \neq d(X) \in K[X]$ に対して，$d(X)$ が $f(X), g(X)$ を共に割り切ることと，$d(X)$ が $g(X), r(X)$ を共に割り切ることは同値だから，その中で次数最高のものは一致する，よって $\mathrm{GCD}\{f(X), g(X)\} = \mathrm{GCD}\{g(X), r(X)\}$ となる．■

このことから，整数の場合と同様に，多項式の Euclid 互除法を考えることができる．

$f(X), g(X) \in K[X]$ $(g(X) \neq 0)$ とする．整数の場合と同様に，次々と割り算を繰り返して

$$\begin{aligned}
f(X) &= q_1(X) \cdot g(X) + r_1(X), \quad \deg r_1(X) < \deg g(X) \\
g(X) &= q_2(X) \cdot r_1(X) + r_2(X), \quad \deg r_2(X) < \deg r_1(X) \\
r_1(X) &= q_3(X) \cdot r_2(X) + r_3(X), \quad \deg r_3(X) < \deg r_2(X) \\
r_2(X) &= q_4(X) \cdot r_3(X) + r_4(X), \quad \deg r_4(X) < \deg r_3(X) \\
&\vdots \\
r_{n-2}(X) &= q_n(X) \cdot r_{n-1}(X) + r_n(X), \quad \deg r_n(X) < \deg r_{n-1}(X) \\
r_{n-1}(X) &= q_{n+1}(X) \cdot r_n(X)
\end{aligned}$$

とする．余りの多項式の次数は

$$\deg g(X) > \deg r_1(X) > \deg r_2(X) > \deg r_3(X) > \cdots \geq 0$$

という具合に，次々と小さくなるから，最悪の場合でも次数が 0，即ち 0 でない定数多項式となって，どこかで割り切れる．

ここで命題 4.6.2 を繰り返し用いれば

$$\begin{aligned}
\mathrm{GCD}\{f(X), g(X)\} &= \mathrm{GCD}\{g(X), r_1(X)\} \\
&= \mathrm{GCD}\{r_1(X), r_2(X)\} \\
&= \mathrm{GCD}\{r_2(X), r_3(X)\} \\
&= \cdots \\
&= \mathrm{GCD}\{r_{n-1}(X), r_n(X)\}
\end{aligned}$$

となる．ここで $r_n(X)$ は $r_{n-1}(X)$ を割り切るから，$\mathrm{GCD}\{r_{n-1}(X), r_n(X)\}$ は $r_n(X)$ をその最高時の係数で割ったものに等しい．即ち

$$\mathrm{GCD}\{f(X), g(X)\} = c^{-1} r_n(X) \quad (c = r_n(X) \text{ の最高時の係数})$$

となる．これが多項式の Euclid の互除法である．

5 環の準同型定理

5.1 環の準同型写像

定義 5.1.1 環 A から環 B への写像 $f : A \to B$ に対して

1) 任意の $x, y \in A$ に対して

$$f(x+y) = f(x) + f(y), \qquad f(xy) = f(x)f(y)$$

2) $f(1_A) = 1_B$

が成り立つとき，写像 f を**環の準同型写像**と呼ぶ．

定義 5.1.2 環 A から環 B への環準同型写像 $f : A \to B$ が全単射であるとき，f を環 A から環 B への**環の同型写像**と呼ぶ．

注意 5.1.3 環 A から環 B への環の準同型写像 $f : A \to B$ に対して，

1) $f(0_A) = 0_B$ である：実際，

$$f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$$

だから，両辺に $-f(0_A)$ を加えれば

$$f(0_A) = f(0_A) - f(0_A) = 0_B$$

となる．

2) 任意の $x \in A$ に対して $f(-x) = -f(x)$ である：実際，

$$f(x) + f(-x) = f(x + (-x)) = f(x - x) = f(0_A) = 0_B$$

だから $f(-x) = -f(x)$ である．

例 5.1.4 整数係数の一変数多項式環 $\mathbb{Z}[X]$ から $\mathbb{Z}[i]$ $(i^2 = -1)$ への写像

$$f : \mathbb{Z}[X] \to \mathbb{Z}[i] \qquad (\varphi(X) \mapsto \varphi(i))$$

は環の準同型写像である．

課題 5.1 例 1.1.8 の 1) で定義した環 $A = \mathbb{Z} \times \mathbb{Z}$ から整数環 $\mathbb{Z}$ への写像

$$f : A \to \mathbb{Z} \qquad ((x, y) \mapsto y)$$

は環の準同型写像であることを示せ.

課題 5.2 例 1.1.8 の 2) で定義した環 $A = \mathbb{Z} \times \mathbb{Z}$ から $\mathbb{Z}[i]$ $(i^2 = -1)$ への写像

$$f : A \to \mathbb{Z}[i] \qquad ((x, y) \mapsto x + iy)$$

は環の同型写像であることを示せ.

5.2 環の準同型定理

環 A から環 B への環の準同型写像

$$f : A \to B$$

に関して，次の定理を**環の準同型定理**と呼ぶ：

定理 5.2.1 1) $\mathrm{Im}(f) = \{f(x) \mid x \in A\}$ は B の部分環である．これを f **の像 (Image)** と呼ぶ.

2) $\mathrm{Ker}(f) = \{x \in A \mid f(x) = 0_B\}$ は A のイデアルである．これを f **の核 (Kernel)** と呼ぶ.

3) 次の環の同型が成り立つ：

$$\overline{f} : A/\mathrm{Ker}(f) \tilde{\to} \mathrm{Im}(f) \qquad (\overline{x} \mapsto f(x)).$$

[**証明**] 1) $f(1_A) = 1_B, f(0_A) = 0_B$ だから $1_B, 0_B \in \mathrm{Im}(f)$ である．任意の $z, w \in \mathrm{Im}(f)$ に対して，$z = f(x), w = f(y)$ $(x, y \in A)$ とできるから

$$z + w = f(x) + f(y) = f(x + y) \in \mathrm{Im}(f), \quad zw = f(x)f(y) = f(xy) \in \mathrm{Im}(f)$$

である．また注意 5.1.3 の 2) から

$$-z = -f(x) = f(-x) \in \mathrm{Im}(f)$$

である.

2) 注意 5.1.3 より $f(0_A) = 0_B$ だから $0_A | in \mathrm{Ker}(f)$ となり，特に $\mathrm{Ker}(f) \subset A$ は空集合ではない．また $x, y \in \mathrm{Ker}(f)$ とすると，$f(x) = f(y) = 0_B$ だから

$$f(x + y) = f(x) + f(y) = 0_B + 0_B = 0_B \quad \therefore \ x + y \in \mathrm{Ker}(f)$$

となる．更に任意の $a \in A$ に対して

$$f(ax) = f(a)f(x) = f(a) \cdot 0_B = 0_B \quad \therefore \ ax \in \mathrm{Ker}(f)$$

となる．

3) まず $x, y \in A$ が剰余類環 $A/\mathrm{Ker}(f)$ で同じ剰余類を与えるとする．即ち $x \equiv y (\mathrm{mod}\ \mathrm{Ker}(f))$，つまり $x - y = z \in \mathrm{Ker}(f)$ であると仮定する．このとき $x = y + z$ だから

$$f(x) = f(y + z) = f(y) + f(z) = f(y) + 0_B = f(y)$$

となる．よって写像

$$\overline{f} : A/\mathrm{Ker}(f) \to B \qquad (\overline{x} \mapsto f(x))$$

は well-defined である．ここで $\overline{x}, \overline{y} \in A/\mathrm{Ker}(f)$ に対して

$$\overline{f}(\overline{x} + \overline{y}) = \overline{f}(\overline{x + y}) = f(x + y) = f(x) + f(y) = \overline{f}(\overline{x}) + \overline{f}(\overline{y}),$$

$$\overline{f}(\overline{x} \cdot \overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x}) \cdot \overline{f}(\overline{y})$$

である．更に

$$\overline{f}(\overline{1}_A) = f(1_A) = 1_B$$

となるから，$\overline{f}$ は環の準同型写像である．

$\overline{f}$ が全射であることは $\mathrm{Im}(f)$ の定義から明らかである．

剰余類 $\overline{x}, \overline{y} \in A/\mathrm{Ker}(f)$ に対して

$$\begin{aligned} \overline{f}(\overline{x}) = \overline{f}(\overline{y}) &\Rightarrow f(x) = f(y) \\ &\Rightarrow f(x - y) = f(x) - f(y) = 0_B \\ &\Rightarrow x - y \in \mathrm{Ker}(f) \Rightarrow A/\mathrm{Ker}(f) \text{ で } \overline{x} = \overline{y} \end{aligned}$$

だから $\overline{f}$ は単射である．■

環の準同型写像の核の意味を理解するのに，次の命題が判りやすい：

命題 5.2.2 環 A から環 B への環の準同型写像 $f : A \to B$ の関して

$$f \text{ は単射} \ \Leftrightarrow \ \mathrm{Ker}(f) = \{0_A\}$$

である．よってこのとき f は環の準同型写像

$$f : A \xrightarrow{\sim} \mathrm{Im}(f)$$

を与える．

[証明] $\Rightarrow$) $x \in \mathrm{Ker}(f)$ とすると，$f(x) = 0_B = f(0_A)$ である．f は単射だから $x = 0_A$ となる．よって $\mathrm{Ker}(f) = \{0\}$ となる．

$\Leftarrow$) $x, y \in A$ に対して $f(x) = f(y)$ とする．

$$f(x-y) = f(x) - f(y) = 0_B, \qquad \therefore \ x - y \in \mathrm{Ker}(f)$$

となる．$\mathrm{Ker}(f) = \{0_A\}$ だから $x - y = 0_A$，即ち $x = y$ となる．よって f は単射である．■

課題 5.3 例 1.1.8 の 1) で定義した環 $A = \mathbb{Z} \times \mathbb{Z}$ から整数環 $\mathbb{Z}$ への準同型写像

$$f : A \to \mathbb{Z} \qquad ((x, y) \mapsto y)$$

(課題 5.1 参照) について次の問いに答えよ：

1) $\mathrm{Im}(f)$ を求めよ．

2) $\mathrm{Ker}(f)$ を求めよ．

3) 環の準同型定理を用いて

$$\mathfrak{a} = \{(x, 0) \in A \mid x \in \mathbb{Z}\}$$

は A の素イデアルであるが極大イデアルではないことを示せ．

課題 5.4 整数環 $\mathbb{Z}$ を係数とする変数 X の多項式環 $\mathbb{Z}[X]$ から複素数体 $\mathbb{C}$ への写像

$$f : \mathbb{Z}[X] \to \mathbb{C} \qquad \big(\varphi(X) \mapsto \varphi(i)\big)$$

(i は虚数単位) に関して，次の問いに答えよ：

1) f は環の準同型写像であることを示せ．

2) $\mathrm{Im}(f)$ を決定せよ．

3) $\mathrm{Ker}(f)$ を決定せよ．

4) 環の準同型定理を用いて $\mathbb{Z}[X]$ は単項イデアル整域ではないことを示せ．

5.3 中国剰余定理

正の整数 $0 < a \in \mathbb{Z}$ は互いに素な正の整数 $a_1, a_2, \cdots, a_r$ の積であるとする：

$$a = a_1 a_2 \cdots a_r, \qquad \mathrm{GCD}\{a_i, a_j\} = 1 \quad (i \neq j).$$

このとき次の定理が成り立つ．この定理を「中国剰余定理」(Chinese Remainder Theorem) と呼ぶ：

定理 5.3.1 環の同型

$$\mathbb{Z}/(a) \tilde{\to} \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \cdots \times \mathbb{Z}/(a_r)$$

$$(x \pmod a \mapsto (x \pmod{a_1}, x \pmod{a_2}, \cdots, x \pmod{a_r})))$$

が成り立つ．

[証明] 環の準同型写像

$$f : \mathbb{Z} \to \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \cdots \times \mathbb{Z}/(a_r) \tag{5.1}$$

$$(x \mapsto (x \pmod{a_1}, x \pmod{a_2}, \cdots, x \pmod{a_r})))$$

を考える．環の準同型定理を用いるために，まず $\mathrm{Ker}(f)$ を決定する．$x \in \mathbb{Z}$ に対して，$\mathrm{GCD}\{a_i, a_j\} = 1$ $(i \neq j)$ に注意すると

$$\begin{aligned} x \in \mathrm{Ker}(f) &\Leftrightarrow x \equiv 0 \pmod{a_1} \quad (i = 1, 2, \cdots, r) \\ &\Leftrightarrow x \in (a_i) \quad (i = 1, 2, \cdots, r) \\ &\Leftrightarrow a_i | x \quad (i = 1, 2, \cdots, r) \\ &\Leftrightarrow a | x \quad \therefore x \in (a) \end{aligned}$$

だから $\mathrm{Ker}(f) = (a)$ である．よって環の準同型定理により，環の同型写像

$$\overline{f} : \mathbb{Z}/(a) \tilde{\to} \mathrm{Im}(f)$$

$$(x \pmod a \mapsto (x \pmod{a_1}, x \pmod{a_2}, \cdots, x \pmod{a_r})))$$

が成り立つ．ここで有限集合の元の個数を数えると

$$\sharp(\mathrm{Im}(f)) = \sharp(\mathbb{Z}/(a)) = a,$$

$$\begin{aligned} \sharp(\mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \cdots \times \mathbb{Z}/(a_r)) =& \sharp(\mathbb{Z}/(a_1)) \cdot \sharp(\mathbb{Z}/(a_2)) \cdots \sharp(\mathbb{Z}/(a_r)) \\ =& a_1 \cdot a_2 \cdots a_r = a \end{aligned}$$

となる．よって

$$\mathrm{Im}(f) = \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \cdots \times \mathbb{Z}/(a_r)$$

となる．■

中国剰余定理（定理 5.3.1）の証明をみると，環の準同型写像 (5.1) は全射である．言い換えれば，任意の $s_i \in \mathbb{Z}$ $(i = 1, 2, \cdots, r)$ に対して

$$x \equiv s_1 \pmod{a_1}, \quad x \equiv s_2 \pmod{a_2}, \quad \cdots \quad x \equiv s_r \pmod{a_r}$$

なる $x \in \mathbb{Z}$ が存在する．このような $x \in \mathbb{Z}$ は具体的に次のようにして求めることが出来る：

$j = 1, 2, \cdots, r$ に対して，$\{a_1, a_2, \cdots, a_r\}$ から a_j 以外全体の積を b_j とすると，$\mathrm{GCD}\{a_k, a_l\} = 1$ $(k \neq l)$ であることから

$$\mathrm{GCD}\{b_1, b_2, \cdots, b_r\} = 1$$

となる．よって

$$b_1 B_1 + b_2 B_2 + \cdots + b_r B_r = 1$$

となるような $B_j \in \mathbb{Z}$ $(j = 1, 2, \cdots, r)$ を求めることが出来る．ここで

$$x = b_1 B_1 s_1 + b_2 B_2 s_2 + \cdots + b_r B_r s_r \in \mathbb{Z}$$

とおくと．ここで $i = 1, 2, \cdots, r$ に対して，$j \neq i$ ならば $b_j \equiv 0 \pmod{a_i}$ だから

$$\begin{aligned} x \equiv b_i B_i s_i \pmod{a_i} &= \left(1 - \sum_{j \neq i} b_j B_j\right) s_i \\ &\equiv s_i \pmod{a_i} \end{aligned}$$

となる．

課題 5.5 中国剰余定理の説明にある方法に従って，5 で割ると 1 余り，7 で割ると 2 余り，11 で割ると 3 余る正の整数を一つ求めよ．

5.4 代数的数の最小多項式

体 K の部分体 F を考える．$\alpha \in K$ をとる．

定義 5.4.1 1) $\varphi(\alpha) = 0$ となる $0 \neq \varphi(X) \in F[X]$ が存在するとき，α は F 上**代数的**であるという．

2) $\varphi(\alpha) = 0$ となる $\varphi(X) \in F[X]$ が $\varphi(X) = 0$ に限るとき，α は F 上**超越的**であるという．

例 5.4.2 1) $\sqrt{2} \in \mathbb{R}$ は $\mathbb{Q}$ 上代数的である．実際，$\varphi(X) = X^2 - 2 \in \mathbb{Q}[X]$ に対して $\varphi(\sqrt{2}) = 0$ となる．

2) 円周率 π や自然対数の底 e は $\mathbb{Q}$ 上超越的であることが証明されている．

$\alpha \in K$ に対して，F 上の一変数多項式環 $F[X]$ から体 K への環の準同型写像

$$f : F[X] \to K \qquad \big(\varphi(X) \mapsto \varphi(\alpha)\big)$$

ができる．このとき

$$\begin{aligned}\mathrm{Im}(f) &= \{\varphi(\alpha) \mid \varphi(X) \in F[X]\} \\ &= \left\{ \sum_{i=0}^{n} a_i \alpha^i \;\middle|\; a_i \in F, n = 0, 1, 2, \cdots \right\} = F[\alpha] \\ \mathrm{Ker}(f) &= \{\varphi(X) \in F[X] \mid \varphi(\alpha) = 0\}\end{aligned}$$

である．ここで

I) $\mathrm{Ker}(f) = \{0\}$ のとき（即ち α が F 上超越的であるとき）．命題 5.2.2 より，環の同型

$$f : F[X] \xrightarrow{\sim} F[\alpha]$$

が成り立つ．即ち $F[\alpha]$ は多項式環 $F[X]$ と同型だから，体ではない．

II) $\mathrm{Ker}(f) \supsetneqq \{0\}$ のとき（即ち α が F 上代数的であるとき）．定理 4.1.2 より，$\mathrm{Ker}(f)$ の元で次数最小のものを $p(X)$ とすると

$$\mathrm{Ker}(f) = (p(X)) = \{p(X) \cdot \psi(X) \mid \psi(X) \in F[X]\}$$

である．即ち $\varphi(X) \in F[X]$ に対して

$$\varphi(\alpha) = 0 \;\Leftrightarrow\; p(X) | \varphi(X)$$

である．環の準同型定理 5.2.1 から，環の同型写像

$$\overline{f} : F[X]/(p(X)) \xrightarrow{\sim} F[\alpha] \qquad \left(\overline{\varphi(X)} \mapsto \varphi(\alpha)\right)$$

が得られる．ここで $F[\alpha]$ は体 K の部分環だから整域である．よって $F[X]/(p(X))$ は整域となる．即ち $p(X)$ は F 上の既約多項式となる．更に定理 4.4.2 より $F[X]/(p(X))$ は体となるから，それと同型な $F[\alpha]$ も体となる．

$p(X)$ をその最高時の係数で割れば，$p(X)$ の最高時の係数は 1 であると仮定してよい．このとき $p(X)$ を α の F **上の最小多項式**と呼ぶ．

課題 5.6 1 の 3 乗根 $\omega = \dfrac{-1+\sqrt{3}i}{2}$ の $\mathbb{Q}$ 上の最小多項式を求めよ．

6　有理数体上の一変数多項式環

この節では有理数体 $\mathbb{Q}$ 上の一変数多項式環 $\mathbb{Q}[X]$ を詳しく調べることにする．例 4.5.4 にあるように，$\mathbb{Q}[X]$ では多項式の既約分解の一意性が成り立っているから，既約多項式がどのようなものであるかが判れば，多項式全体について理解が進むことになる．とは言え，既約多項式を具体的に把握することは意外に難しいくて，幾つかの準備が必要である．

6.1 原始的多項式

定義 6.1.1 整数係数多項式

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \qquad (a_i \in \mathbb{Z}, n \geq 1)$$

に対して

$$\mathrm{GCD}\,\{a_0, a_1, \cdots, a_{n-1}, a_n\} = 1$$

のとき，$f(X)$ を**原始的多項式**と呼ぶ.

次の定理は **Gauss の補題**と呼ばれている：

定理 6.1.2 $f(X), g(X) \in \mathbb{Z}[X]$ が共に原始的多項式ならば $f(X)g(X)$ も原始的多項式である.

[**証明**] まず

$$\begin{aligned} f(X) &= a_0X^m + a_1X^{m-1} + \cdots + a_{m-1}X + a_m, \\ g(X) &= b_0X^n + b_1X^{n-1} + \cdots + b_{n-1}X + b_n \end{aligned}$$

とおくと

$$\mathrm{GCD}\{a_0, a_1, \cdots, a_m\} = 1, \quad \mathrm{GCD}\{b_0, b_1, \cdots, b_n\} = 1$$

である．任意の正の素数 p をとる.

$$k = \mathrm{Min}\{i \mid p \not| a_i\}, \qquad l = \mathrm{Min}\{j \mid p \not| b_j\}$$

とおくと，$p|a_i$ $(0 \leq i < k)$, $p|b_j$ $(0 \leq j < l)$ である．$f(X)g(X)$ の X^{k+l} の係数は

$$\begin{aligned} &a_kb_l + a_{k+1}b_{l-1} + \cdots \\ &\quad + a_{k-1}b_{l+1} + \cdots \end{aligned}$$

となるが，$a_{k+1}b_{l-1} + \cdots$, $a_{k-1}b_{l+1} + \cdots$ は共に p で割り切れ，a_kb_l は p で割り切れない．よって $f(X)g(X)$ の X^{k+l} の係数は p で割り切れない．よって $f(X)g(X)$ の全ての係数の最大公約数は 1 となり，$f(X)g(X)$ は原始的多項式となる．■

命題 6.1.3 原始的多項式 $f(X), g(X) \in \mathbb{Z}[X]$ と正の $a, b \in \mathbb{Q}$ に対して

$$a \cdot f(X) = b \cdot g(X) \;\Rightarrow\; \begin{cases} a = b, \\ f(X) = g(X) \end{cases}$$

である.

[証明] $\dfrac{a}{b} \in \mathbb{Q}^\times$ を既約分数で

$$\frac{a}{b} = \frac{p}{q}, \quad p, q \in \mathbb{Z}, \quad \mathrm{GCD}\{p, q\} = 1$$

とおくと $p \cdot f(X) = q \cdot g(X)$ である．$\deg f(X) = \deg g(X) = n$ で

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n,$$
$$g(X) = b_0 X^n + b_1 X\ n - 1 + \cdots + b_{n-1} X + b_n$$

とおくと，$p \cdot a_i = q \cdot b_i\ (i = 0, 1, 2, \cdots, n)$ である．ここで $\mathrm{GCD}\{p, q\} = 1$ だから $p | b_i, q | a_i\ (i = 0, 1, 2, \cdots, n)$ となるが，

$$\mathrm{GCD}\{a_0, a_1, \cdots, a_n\} = \mathrm{GCD}\{b_0, b_1, \cdots, b_n\} = 1$$

だから $p = q = 1$ である．よって $a = b$ となり $f(X) = g(X)$ となる．■

有理数係数多項式 $f(X) \in \mathbb{Q}[X]$ に対して，$f(X)$ の係数の分母を通分して分子の最大公約数をくくりだせば，正の $c(f) \in \mathbb{Q}$ と原始的多項式 $f_0(X) \in \mathbb{Z}[X]$ があって

$$f(X) = c(f) \cdot f_0(X)$$

と書けることがわかる．命題 6.1.3 より，このような正の $c(f) \in \mathbb{Q}$ と原始的多項式 $f_0(X) \in \mathbb{Z}[X]$ は $f(X) \in \mathbb{Q}[X]$ に対して一意的に定まる．$c(f)$ を $f(X)$ の**内容 (content)** と呼び，$f_0(X)$ を $f(X)$ の**原始的部分**と呼ぶ．

定理 6.1.4 $f(X), g(X) \in \mathbb{Q}[X]$ に対して

$$c(f \cdot g) = c(f) \cdot c(g)$$

である．従って積 $f(X) \cdot g(X) \in \mathbb{Z}[X]$ の原始的部分は $f_0(X) \cdot g_0(X)$ である．

[証明] $f(X) = c(f) \cdot f_0(X), g(X) = c(g) \cdot g_0(X)$ として，$f_0(X), g_0(X) \in \mathbb{Z}[X]$ は原始的多項式である．Gauss の補題 (定理 6.1.2) より $f_0(X) g_0(X) \in \mathbb{Z}[X]$ は原始的多項式で

$$f(X) g(X) = c(f) c(g) \cdot f_0(X) g_0(X)$$

だから，命題 6.1.3 より $c(f \cdot g) = c(f) \cdot c(g)$ となる．■

課題 6.1 整数係数多項式

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \in \mathbb{Z}[X] \quad (a_0 \neq 0)$$

に対して

$$c(f) = \mathrm{GCD}\{a_0, a_1, \cdots, a_{n-1}, a_n\}$$

であることを示せ．

課題 6.2 整数係数多項式 $f(X), g(X) \in \mathbb{Z}[X]$ に対して，次は同値であることを示せ：

1) 積 $f(X) \cdot g(X)$ は原始的多項式である．

2) $f(X), g(X)$ は共に原始的多項式である．

6.2 整数係数の既約多項式

例 4.4.5 にある既約多項式の特徴づけを参考にして，整数環 $\mathbb{Z}$ 上の既約多項式を次のように定義する：

定義 6.2.1 整数係数多項式 $p(X) \in \mathbb{Z}[X]$ で

1) $\deg p(X) \geq 1$, かつ

2) $p(X) = f(X)g(X)$ $(f(X), g(X) \in \mathbb{Z}[X])$ ならば $\deg f(X) = 0$ または $\det g(X) = 0$

なるものを，$\mathbb{Z}$ **上の既約多項式**とよぶ．

$\mathbb{Z}$ 上の既約多項式と $\mathbb{Q}$ 上の既約多項式は次のように関係している：

定理 6.2.2 $\mathbb{Z}$ 上の既約多項式 $p(X) \in \mathbb{Z}[X]$ は $\mathbb{Q}$ 上の既約多項式である．

[**証明**] $p(X) = f(X)g(X)$ $(f(X), g(X) \in \mathbb{Q}[X])$ とする．

$$p(X) = c(p) \cdot p_0(X), \quad f(X) = c(f) \cdot f_0(X), \quad g(X) = c(g) \cdot g_0(X)$$

とおける．ここで $c(p), c(f), c(g)$ はそれぞれ $p(X), f(X), g(X)$ の内容であり，$p_0(X), f_0(X), g_0(X) \in \mathbb{Z}[X]$ は原始的多項式である．定理 6.1.4 より $c(f) \cdot c(g) = c(f \cdot g) = c(p)$ である．よって $p_0(X) = f_0(X)g_0(X)$ となり

$$p(X) = c(p)f_0(X) \cdot g_0(X)$$

となる．$c(p) \in \mathbb{Z}$ だから $c(p)f_0(X) \in \mathbb{Z}[X]$ である．$p(X)$ は $\mathbb{Z}$ 上の既約多項式だから

$$\deg c(p)f_0(X) = 0 \quad \text{または} \quad \deg g_0(X) = 0$$

となる．よって $\deg f(X) = 0$ または $\deg g(X) = 0$ となる．即ち $p(X)$ は $\mathbb{Q}$ 上の既約多項式である．■

6.3 Eisenstein の判定法

$\mathbb{Q}$ 上の既約多項式を具体的に捕まえる手段として，次の判定法は便利である：

定理 6.3.1 (Eisenstein の判定法) 整数係数多項式

$$p(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in \mathbb{Z}[X]$$

に対して，

$$p \not| a_0,\ \ p|a_i\ (i = 1, 2, \cdots, n),\ \ p^2 \not| a_n$$

なる素数 p があるならば，$p(X)$ は $\mathbb{Q}$ 上の既約多項式である．

[証明] 剰余類環 $\mathbb{F}_p = \mathbb{Z}/(p)$ は体である．そこで整数係数多項式

$$f(X) = c_0X^m + c_1X^{m-1} + \cdots + c_{m-1}X + c_m \in \mathbb{Z}[X]$$

に対して，$\mathbb{F}_p$ に係数をもつ多項式

$$\overline{f}(X) = \overline{c_0}X^m + \overline{c_1}X^{m-1} + \cdots + \overline{c_{m-1}}X + \overline{c_m} \in \mathbb{F}_p[X]$$

を考える．ここで $\overline{c_i} \in \mathbb{F}_p$ は $c_i \in \mathbb{Z}$ の剰余類である．このとき $f(X) \mapsto \overline{f}(X)$ は $\mathbb{Z}[X]$ から $\mathbb{F}_p[X]$ への環の準同型写像となる．さて問題の $p(X)$ が $\mathbb{Q}$ 上の既約多項式であることを示すには，定理 6.2.2 より，$p(X)$ が $\mathbb{Z}$ 上の既約多項式であることを示せば十分である．そこで $p(X) = f(X) \cdot g(X)$ $(f(X), g(X) \in \mathbb{Z}[X])$ かつ $\deg f(X) = l \geq 1, \deg g(X) = m \geq 1$ と仮定する．

$$f(X) = b_0X^l + b_1X^{l-1} + \cdots + b_{l-1}X + b_l,$$
$$g(X) = c_0X^m + c_1X^{m-1} + \cdots + c_{m-1}X + c_m$$

とおくと，$a_0 = b_0c_0$ だから $p \not| b_0, p \not| c_0$ である．すると $\mathbb{F}_p$ 上の多項式として $\overline{p}(X) = \overline{f}(X) \cdot \overline{g}(X)$ となる．一方，$p(X)$ の係数に関する仮定から

$$\overline{p}(X) = \overline{a_0}X^n \in \mathbb{F}_p[X]$$

となる．$X \in \mathbb{F}_p[X]$ は $\mathbb{F}_p$ 上の既約多項式だから，$\mathbb{F}_p$ 上の多項式の既約分解の一意性から

$$\overline{f}(X) = \overline{b_0}X^l, \qquad \overline{g}(X) = \overline{c_0}X^m$$

となる．よって $p|b_l, p|c_m$ となる．ところで $a_n = b_lc_m$ だから $p^2|a_n$ となり，仮定に反する．よって $\deg f(X) = 0$ または $\deg g(X) = 0$ となる．■

Eisenstein の判定法の具体的な応用例として

定理 6.3.2 素数 p に対して

$$p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$$

は $\mathbb{Q}$ 上の既約多項式である．

[証明] $(X-1)p(X) = X^p - 1$ だから

$$Xp(X+1) = (X+1)^p - 1 = \sum_{k=0}^{p} \binom{p}{k} X^k - 1 = \sum_{k=1}^{p} \binom{p}{k} X^k.$$

そこで

$$\begin{aligned} q(X) = p(X+1) &= \sum_{k=1}^{p} \binom{p}{k} X^{k-1} \\ &= a_0 X^{p-1} + a_1 X^{p-2} + \cdots + a_{p-2} X + a_{p-1} \end{aligned}$$

とおく.

$$a_0 = \binom{p}{p} = 1 \qquad \therefore \ p \not| a_0$$

である．$1 \leq k \leq p-1$ に対して，$k \not| p$ に注意すると

$$a_{p-k} = \binom{p}{k} = \frac{p!}{k!(p-k!)} = p \cdot \frac{(p-1)!}{k!(p-k)!}$$

となり $p | a_{p-k}$ である．更に

$$a_{p-1} = \binom{p}{1} = p \qquad \therefore \ p^2 \not| a_{p-1}$$

となる．よって Eisenstein の判定法により $q(X)$ は $\mathbb{Q}$ 上の既約多項式である．よって $p(X) = q(X-1)$ も $\mathbb{Q}$ 上の既約多項式である．■

課題 6.3 Eisenstein の判定法を用いて

$$f(X) = 6X^4 + 21X^3 + 49X^2 + 91X + 77$$

は $\mathbb{Q}$ 上の既約多項式であることを示せ.

課題 6.4 素数 p に対して $\omega = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p} \in \mathbb{C}$ とおく.

1) $\omega \in \mathbb{C}$ は $\mathbb{Q}$ 上代数的であることを示せ.

2) $\omega \in \mathbb{C}$ の $\mathbb{Q}$ 上の最小多項式は

$$p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$$

であることを示せ.

6.4　整数係数多項式の素因子分解

$f(X), g(X) \in \mathbb{Z}[X]$ に対して

1) $g(X) = q(X) \cdot f(X)$ なる $q(X) \in \mathbb{Q}[X]$ が存在するとき，$f(X)$ は $\mathbb{Q}[X]$ で（あるいは $\mathbb{Q}$ 上）$g(X)$ を割り切るという．

2) $g(X) = q(X) \cdot f(X)$ なる $q(X) \in \mathbb{Z}[X]$ が存在するとき，$f(X)$ は $\mathbb{Z}[X]$ で（あるいは $\mathbb{Z}$ 上）$g(X)$ を割り切るという．

命題 6.4.1 整数係数多項式 $f(X), g(X) \in \mathbb{Z}[X]$ $(f(X) \neq 0)$ に対して，次は同値である：

1) $f(X)$ は $\mathbb{Q}$ 上 $g(X)$ を割り切る．

2) $f(X)$ の原始的部分 $f_0(X)$ は $\mathbb{Z}$ 上 $g(X)$ を割り切る．

[**証明**] 1) $\Rightarrow$ 2) $g(X) = q(X) \cdot f(X)$ なる $q(X) \in \mathbb{Q}[X]$ がとれる．定理 6.1.4 より

$$c(g) = c(q) \cdot c(f), \qquad g_0(X) = q_0(X) \cdot f_0(X)$$

である．$c(g) \in \mathbb{Z}$ だから

$$g(x) = c(g)q_0(X) \cdot f_0(X), \qquad c(g)q_0(X) \in \mathbb{Z}[X]$$

となる．

2) $\Rightarrow$ 1) $g(X) = q(X) \cdot f_0(X)$ なる $q(X) \in \mathbb{Z}[X]$ がとれる．$f(X) = c(f) \cdot f_0(X)$ だから

$$g(X) = c(f)^{-1}q(X) \cdot f(X), \qquad c(f)^{-1}q(X) \in \mathbb{Q}[X]$$

となる．■

この命題から直ちに次の系を得る：

系 6.4.2 $f(X), g(X) \in \mathbb{Z}[X]$ について $f(X)$ が原始的ならば

$f(X)$ は $\mathbb{Q}$ 上 $g(X)$ を割り切る　$\Leftrightarrow$　$f(X)$ は $\mathbb{Z}$ 上 $g(X)$ を割り切る

である．

定理 6.4.3 $p(X) \in \mathbb{Z}[X]$ $(\deg p(X) > 0)$ に対して，次は同値である：

1) $\mathbb{Z}[X]/(p(X))$ は整域である．

2) $p(X) \in \mathbb{Z}[X]$ は原始的かつ $\mathbb{Z}$ 上で既約である．

[証明] 1) $\Rightarrow$ 2) $p(X) = f(X)g(X)$ $(f(X), g(X) \in \mathbb{Z}[X])$ とする．$\mathbb{Z}[X]/(p(X))$ は整域だから，$\mathbb{Z}[X]$ で $p(X)|f(X)$ または $p(X)|g(X)$ である．$p(X)|g(X)$ として $g(X) = p(X)h(X)$ $(h(X) \in \mathbb{Z}[X])$ とすると

$$p(X) = f(X)g(X) = f(X)h(X)p(X) \qquad \therefore \quad f(X)h(X) = 1$$

となり，$f(X) = \pm 1$ となる．特に $\deg f(X) = 0$ となるから，$p(X)$ は $\mathbb{Z}$ 上の既約多項式である．$p(X) = c(p) \cdot p_0(X)$ だから，$f(X) = c(p), g(X) = p_0(X)$ とおけば，$c(p) = 1$ となるから $p(X)$ は原始的である．

2) $\Rightarrow$ 1) $p(X) \in \mathbb{Q}[X]$ で生成された $\mathbb{Q}[X]$ の単項イデアルを $\mathfrak{p} = (p(X))$ とおく．定理 6.2.2 より $p(X)$ は $\mathbb{Q}[X]$ の既約多項式（即ち素元）だから，定理 4.4.2 より $\mathbb{Q}[X]/\mathfrak{p}$ は整域である．ここで環の準同型写像

$$f : \mathbb{Z}[X] \to \mathbb{Q}[X]/\mathfrak{p} \qquad (\varphi(X) \mapsto \varphi(X) \pmod{\mathfrak{p}})$$

を考える．$\varphi(X) \in \mathbb{Z}[X]$ に対して，$p(X) \in \mathbb{Z}[X]$ が原始的多項式であることに注意すると，命題 6.4.1 より

$$\begin{aligned} \varphi(X) \in \mathrm{Ker}(f) &\Leftrightarrow \varphi(X) \in \mathfrak{p} \\ &\Leftrightarrow p(X) \text{ は } \varphi(X) \text{ を } \mathbb{Q}[X] \text{ で割り切る} \\ &\Leftrightarrow p(X) \text{ は } \varphi(X) \text{ を } \mathbb{Z}[X] \text{ で割り切る} \\ &\Leftrightarrow \varphi(X) \in (p(X)) \end{aligned}$$

となるから，$\mathrm{Ker}(f) = (p(X))$ である．よって環の準同型定理から，環の同型写像

$$\overline{f} : \mathbb{Z}[X]/(p(X)) \xrightarrow{\sim} \mathrm{Im}(\varphi) \qquad (\varphi(X) \pmod{(p(X))} \mapsto \varphi(X) \pmod{\mathfrak{p}})$$

が成り立つ．$\mathrm{Im}(f) \subset \mathbb{Q}[X]/\mathfrak{p}$ は整域の部分環だから整域である．よって $\mathbb{Z}[X]/(p(X))$ も整域となる．■

注意 6.4.4 定理 6.4.3 の 2) $\Rightarrow$ 1) の証明は，次のように展開することもできる：

[別証] $f(X), g(X) \in [X]$ に対して

$$\overline{f(X)} \cdot \overline{g(X)} = \overline{f(X) \cdot g(X)} = 0 \in \mathbb{Z}[X]/(p(X))$$

とする．これは $f(X) \cdot g(X) \in (p(X))$ を意味するから，$p(X)$ は $\mathbb{Z}$ 上で積 $f(X) \cdot g(X)$ を割り切る．従って $p(X)$ は $\mathbb{Q}$ 上で $f(X) \cdot g(X)$ を割り切る．ここで $p(X)$ は $\mathbb{Z}$ 上の既約多項式だから，定理 6.2.2 より $\mathbb{Q}$ 上の既約多項式，即ち $\mathbb{Q}[X]$ の素元となる（例 4.4.5 参照）．よって定理 4.4.3 の 1) より，$p(X)$ は $\mathbb{Q}$ 上で $f(X)$ または $g(X)$ を割り切る．ここで $p(X)$ は原始的多項

式だから，系 6.4.2 より，$p(X)$ は $\mathbb{Z}$ 上で $f(X)$ または $g(X)$ を割り切る．即ち $f(X) \in (p(X))$ または $g(X) \in (p(X))$ となるから

$$\overline{f(X)} = 0 \in \mathbb{Z}[X]/(p(X)) \quad \text{または} \quad \overline{g(X)} = 0 \in \mathbb{Z}[X]/(p(X))$$

となる．■

定理 6.4.3 と定理 4.4.2 を見比べると，$\mathbb{Z}$ 上既約かつ原始的な $p(X) \in \mathbb{Z}[X]$ が単項イデアル整域における素元の働きをしていることが判るだろう．定理 4.4.3 の 1) の証明と同様にして，次の命題が成り立つことが判る：

命題 6.4.5 $p(X) \in \mathbb{Z}[X]$ は $\mathbb{Z}$ 上既約かつ原始的であるとする．整数係数多項式 $f_i(X) \in \mathbb{Z}[X]$ $(i = 1, 2, \cdots, r)$ に対して，$p(X)$ が $\mathbb{Z}$ 上で積 $f_1(X) \cdot f_2(X) \cdots f_r(X)$ を割り切るならば，$p(X)$ は $\mathbb{Z}$ 上で $f_1(X), f_2(X), \cdots, f_r(X)$ の何れかを割り切る．

次の命題は，素数もまた $\mathbb{Z}[X]$ に於いて，単項イデアル整域の素元の働きをしていることを示している：

命題 6.4.6 正の整数 $p \in \mathbb{Z}$ に対して，次は同値である：

1) $\mathbb{Z}[X]/(p)$ は整域である．

2) p は素数である．

[**証明**] $p \in \mathbb{Z}$ が生成する $\mathbb{Z}$ の単項イデアルを $\mathfrak{p}$ と書くことにする．整数係数多項式

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \in \mathbb{Z}[X]$$

の各係数 a_i を $\mathfrak{p}$ を法として $\overline{a}_i = a_i \,(\mathrm{mod}\ \mathfrak{p}) \in \mathbb{Z}/\mathfrak{p}$ とおくと，$\mathbb{Z}/\mathfrak{p}$-係数の多項式

$$\overline{f}(X) = \overline{a}_0 X^n + \overline{a}_1 X^{n-1} + \cdots + \overline{a}_{n-1} X + \overline{a}_n \in \mathbb{Z}/\mathfrak{p}[X]$$

ができる．更に環の同型

$$\mathbb{Z}[X]/(p) \xrightarrow{\sim} \mathbb{Z}/\mathfrak{p}[X] \qquad \big(f(X) \pmod{(p)} \mapsto \overline{f}(X)\big)$$

が成り立つ．このとき

$$\mathbb{Z}[X]/(p) : \text{整域} \ \Leftrightarrow\ \mathbb{Z}/\mathfrak{p}[X] : \text{整域} \ \Leftrightarrow\ \mathbb{Z}/\mathfrak{p} : \text{整域} \ \Leftrightarrow\ p \text{ は素数}$$

となる．■

課題 1.7 より

$$\mathbb{Z}[X]^\times = \mathbb{Z}^\times = \{\pm 1\}$$

だから，命題 2.1.7 より，0 でない整数係数多項式 $f(X), g(X) \in \mathbb{Z}[X]$ に対して

$$(f(X)) = (g(X)) \Leftrightarrow f(X) = \pm g(X)$$

である．そこで，最高次の係数が正の多項式を**正の多項式**と呼ぶことにする．

定理 6.4.7 0 でない整数係数多項式 $f(X) \in \mathbb{Z}[X]$ に対して

1) $c \in \mathbb{Z}$ と正の原始的既約多項式 $p_i(X) \in \mathbb{Z}[X]$ $(i = 1, 2, \cdots, r)$ があって

$$f(X) = c \cdot p_1(X) \cdot p_2(X) \cdots p_r(X)$$

と書ける．

2) このとき $p_1(X), p_2(X), \cdots, p_r(X)$ は積の順序を除いて一意的である．

[**証明**] 1) $\deg f(X)$ に関する数学的帰納法により示す．

i) $\deg f(X) = 0$ のとき．$f(X) = c$ は定数多項式だから，$r = 0$ とすればよい．$\deg f(X) = 1$ のとき．$f(X) = \pm(aX + b) \in \mathbb{Z}[X]$ $(a > 0)$ とする．$c = \mathrm{GCD}\{a, b\}$ として，$a = c \cdot a', b = c \cdot b'$ とおくと，$a'X + b' \in \mathbb{Z}[X]$ は正の原始的既約多項式で

$$f(X) = \pm c \cdot (a'X + b')$$

となる．

ii) $\deg f(X) < n$ のとき成り立つと仮定して，$\deg f(X) = n > 1$ のとき．$f(X)$ が $\mathbb{Z}$ 上の既約多項式ならば，$f(X)$ の係数の最大公約数をくくりだして，更に符号を調節すれば，$f(X) = c \cdot p(X)$ で $c \in \mathbb{Z}$ かつ $p(X)$ は正の原始的既約多項式とできる．$f(X)$ が $\mathbb{Z}$ 上の既約多項式でないとき．

$$f(X) = g(X) \cdot h(X), \quad g(X), h(X) \in \mathbb{Z}[X], \quad \deg g(X) > 0, \deg h(X) > 0$$

とできる．このとき $\deg g(X) < n, \deg h(X) < n$ だから，帰納法の仮定から $c, d \in \mathbb{Z}$ と正の原始的既約多項式 $p_i(X), q_j(X) \in \mathbb{Z}[X]$ $(i = 1, 2, \cdots, r, j = 1, 2 \cdots, s)$ があって

$$g(X) = cp_1(X)p_2(X) \cdots p_r(X), \quad h(X) = d1_1(X)q_2(X) \cdots q_s(X)$$

とできる．よって

$$f(X) = cd \cdot p_1(X) \cdots p_r(X)q_1(X) \cdots q_s(X)$$

となる．

2) $d \in \mathbb{Z}$ と正の原始的既約多項式 $q_j(X) \in \mathbb{Z}[X]$ $(j = 1, 2, \cdots, s)$ があって

$$f(X) = d \cdot q_1(X) \cdot q_2(X) \cdots q_s(X)$$

となるとする．

$$c \cdot p_1(X) \cdot p_2(X) \cdots p_r(X) = d \cdot q_1(X) \cdot q_2(X) \cdots q_s(X)$$

だから，$p_1(X)$ は $q_1(X)q_2(X)\cdots q_s(X)$ を $\mathbb{Z}[X]$ で割り切る．命題 6.4.5 より $p_1(X)$ は $q_1(X), q_2(X), \cdots, q_s(X)$ のどれかを $\mathbb{Z}[X]$ で割り切る．番号を付け直して $p_1(X)$ は $q_1(X)$ を $\mathbb{Z}[X]$ で割り切るとして，$q_1(X) = p_1(X)g(X)$ $(g(X) \in \mathbb{Z}[X])$ とする．$q_1(X)$ は $\mathbb{Z}$ 上の既約多項式だから $\deg g(X) = 0$，即ち $g(X) = d \in \mathbb{Z}$ は定数である．よって $q_1(X) = d \cdot p_1(X)$ となるが，$q_1(X)$ は原始的だから $d = \pm 1$ となる．更に $p_1(X), q_1(X)$ の最高時の係数は正だから $d = 1$ となり，$q_1(X) = p_1(X)$ となる．よって

$$c \cdot p_2(X) \cdot p_3(X) \cdots p_r(X) = d \cdot q_2(X) \cdot q_3(X) \cdots q_s(X)$$

以下，同様に繰り返せば，$r = s$ かつ

$$q_1(X) = p_1(X),\ q_2(X) = p_2(X), \cdots .q_r(X) = p_r(X)$$

となる．■

上の定理で，更に整数の素因数分解を考えれば

0 でない整数係数多項式 $f(X) \in \mathbb{Z}[X]$ にたいして，正の素数 $q_j \in \mathbb{Z}$ $(j = 1, 2, \cdots, s)$ と正の原始的既約多項式 $p_i(X) \in \mathbb{Z}[X]$ $(i = 1, 2, \cdots, r)$ があって，積の順序を除いて一意的に

$$f(X) = \pm q_1 q_2 \cdots q_s \cdot p_1(X)p_2(X)\cdots p_r(X)$$

と書ける

ことが判る．これを**整数係数多項式の素因子分解の一意性**と呼ぶ．

課題 6.5 $X^6 - 1 \in \mathbb{Z}[X]$ を原始的既約多項式の積として表せ．

課題 6.6 $X^6 + 1 \in \mathbb{Z}[X]$ を原始的既約多項式の積として表せ．

7 Gauss の整数環

Gauss の整数環

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \qquad \left(i^2 = -1\right)$$

は単項イデアル整域で（定理 4.2.2）

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$$

だから（定理 1.3.4），$\alpha \in \mathbb{Z}[i]$ $(\alpha \neq 0, \pm 1, \pm i)$ は

$$\alpha = \pi_1 \pi_2 \cdots \pi_r \qquad (\pi_i \text{ は } \mathbb{Z}[i] \text{ の素元})$$

と書くことができて，更に $\mathbb{Z}[i]$ の単項イデアル

$$(\pi_1),\ (\pi_2),\ \cdots,\ (\pi_r)$$

は順序を除いて一意的である（定理 4.5.2，定理 4.5.1）．そこで Gauss の整数環 $\mathbb{Z}[i]$ の素元がどのようなものかが問題となる．

複素数 $z = x + iy \in \mathbb{C}$ $(x, y \in \mathbb{R})$ の共役複素数を $\overline{z} = x - iy$ として

$$N(z) = z \cdot \overline{z} = x^2 + y^2$$

を z の**ノルム**と呼ぶ．$N(zw) = N(z) \cdot N(w)$ $(z, w \in \mathbb{C})$ である．更に $\alpha \in \mathbb{Z}[i]$ に対して $N(\alpha) \in \mathbb{Z}$ で

$$\mathbb{Z}[i]^\times = \{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = 1\} \tag{7.1}$$

である．

定理 7.0.1 $\mathbb{Z}[i]$ の素元 π に対して

1) 素数 p があって $N(\pi) = p$ または $N(\pi) = p^2$ となる．
2) $N(\pi) = p$ のとき，素数 p は $\mathbb{Z}[i]$ で $p = \pi \cdot \overline{\pi}$ と分解する．
3) $N(\pi) = p^2$ のとき，素数 p は $\mathbb{Z}[i]$ の素元で，$\mathbb{Z}[i]$ の単項イデアルとして $(\pi) = (p)$ である．

[**証明**] 1) 環の準同型写像

$$f : \mathbb{Z} \to \mathbb{Z}[i]/(\pi) \qquad (x \mapsto x \pmod{(\pi)})$$

に対して

$$N(\pi) = \pi \cdot \overline{\pi} \in \mathbb{Z} \cap (\pi) = \mathrm{Ker}(f) \quad \therefore \ \mathrm{Ker}(f) \neq \{0\}$$

だから $\mathrm{Ker}(f) = (p)$ なる正の $p \in \mathbb{Z}$ がとれる．環の準同型定理より環の同型写像

$$\overline{f} : \mathbb{Z}/(p) \xrightarrow{\sim} \mathrm{Im}(f)$$

を得る．ここで $\mathrm{Im}(f)$ は体 $\mathbb{Z}[i]/(\pi)$ の部分環だから整域である．よって $\mathbb{Z}/(p)$ も整域となり，従って p は素数である．

$$p \in \mathrm{Ker}(f) = \mathbb{Z} \cap (\pi) \subset (\pi) = \{\pi\alpha \mid \alpha \in \mathbb{Z}[i]\}$$

だから $p=\pi\alpha$ $(\alpha\in\mathbb{Z}[i])$ とおく．両辺のノルムをとると

$$p^2=N(\pi\alpha)=N(\pi)\cdot N(\alpha)$$

で $N(\pi),N(\alpha)$ は正の整数である．よって $N(\pi)=p$ または $N(\pi)=p^2$ となる．

2) $N(\pi)=\pi\cdot\overline{\pi}$ だから明らか．

3) $N(\pi)=p^2$ とすると，1) の記号で $N(\alpha)=1$ となるから $\alpha\in\mathbb{Z}[i]^\times$ となる．よって $(p)=(\pi)$ となる．■

命題 7.0.2 Gauss の整数 $\pi\in\mathbb{Z}[i]$ に対して，$N(\pi)=p$ が素数ならば π は $\mathbb{Z}[i]$ の素元である．

[**証明**] $\pi=\alpha\cdot\beta$ $(\alpha,\beta\in\mathbb{Z}[i])$ とおくと

$$p=N(\pi)=N(\alpha)\cdot N(\beta)$$

である．p は素数で $N(\alpha),N(\beta)$ は正の整数だから，$N(\alpha)=1$ または $N(\beta)=1$ である．よって (7.1) より，$\alpha\in\mathbb{Z}[i]^\times$ または $\beta\in\mathbb{Z}[i]^\times$ である．■

定理 7.0.3 1) $\pi=1+i$ は $\mathbb{Z}[i]$ の素元で $2=\pi\cdot\overline{\pi}$ かつ $(\pi)=(\overline{\pi})$ である．

2) 素数 p が $\mathbb{Z}[i]$ で $p=\pi\cdot\overline{\pi}$ $(\pi\in\mathbb{Z}[i])$ と分解しかつ $(\pi)=(\overline{\pi})$ ならば $p=2$ である．

[**証明**] 1) $N(\pi)=(1+i)(1-i)=2$ だから $\pi=1+i$ は $\mathbb{Z}[i]$ の素元で $2=\pi\cdot\overline{\pi}$ となる．更に

$$\overline{\pi}=1-i=(-i)\pi\quad(-i\in\mathbb{Z}[i]^\times)\qquad\therefore\ (\overline{\pi})=(\pi)$$

となる．

2) $\pi=a+bi$ $(a,b\in\mathbb{Z})$ とおく．

$$p=N(\pi)=a^2+b^2\qquad\therefore\ a\neq0,b\neq0$$

である．$(\overline{\pi})=(\pi)$ だから $\overline{\pi}=\varepsilon\cdot\pi$ $(\varepsilon=\pm1,\pm i)$ である．$\varepsilon=1$ ならば $b=0$，$\varepsilon=-1$ ならば $a=0$ となり，共に不可である．$\varepsilon=i$ ならば $a-bi=-b+ai$，よって $a=-b$ となり $p=2a^2$，従って $p=2,a=\pm1$ である．同様に $\varepsilon=-i$ ならば $p=2$ となる．■

定理 7.0.4 寄素数 p に対して，次は同値である：

1) $\mathbb{Z}[i]$ の素元 π があって $p=\pi\cdot\overline{\pi}$ と分解する．

2) $p=a^2+b^2$ なる整数 $a,b\in\mathbb{Z}$ が存在する．

3) $p \equiv 1 \pmod 4$.

[証明] 1) $\Rightarrow$ 2) $\pi = a + bi$ $(a, b \in \mathbb{Z})$ とおけば

$$p = (a + bi)(a - bi) = a^2 + b^2$$

となる．

2) $\Rightarrow$ 1) $\pi = a + bi \in \mathbb{Z}[i]$ とおけば

$$N(\pi) = (a + bi)(a - bi) = a^2 + b^2 = p$$

だから，命題 7.0.2 より π は $\mathbb{Z}[i]$ の素元で $p = \pi \cdot \overline{\pi}$ となる．

2) $\Rightarrow$ 3) p は奇数だから，a は奇数 b は偶数としてよい．$a = 2l+1, b = 2m$ とおけば

$$p = (2l + 1)^2 + (2m)^2 = 4(l^2 + l + m^2) + 1 \equiv 1 \pmod 4$$

となる．

3) $\Rightarrow$ 2) 有限体 $\mathbb{Z}/(p)$ の乗法群 $(\mathbb{Z}/(p))^\times$ の位数は $p-1$ だから，$\left|(\mathbb{Z}/(p))^\times\right|$ が 4 で割り切れる．よって 位数 4 の元 $\overline{a} \in (\mathbb{Z}/(p))^\times$ が存在する．即ち

$$a \not\equiv 1 \pmod p, \quad a^2 \not\equiv 1 \pmod p, \quad a^4 \equiv 1 \pmod p$$

なる $a \in \mathbb{Z}$ が存在する．即ち

$$p | a^4 - 1 = (a - 1)(a + 1)(a^2 + 1), \quad p \not| a - 1, \quad p \not| a + 1$$

だから，$p | a^2 + 1$ である．ここで p が $\mathbb{Z}[i]$ の素元ならば $a^2 + 1 = (a+i)(a-i)$ より $p | a - i$ または $p | a + i$ となる．よって

$$a - i = p \cdot (b + ci) \text{ または } a + i = p \cdot (b + ci) \qquad (c, d \in \mathbb{Z})$$

となる．虚部を比べれば $pc = \pm 1$ となるが，p は素数で $c \in \mathbb{Z}$ だから，これは不可能である．よって p は $\mathbb{Z}[i]$ の素元ではない．よって

$$p = \alpha \cdot \beta \qquad (\alpha, \beta \in \mathbb{Z}[i],\ N(\alpha) \neq 1, N(\beta) \neq 1)$$

と書ける．両辺のノルムをとれば $p^2 = N(\alpha) \cdot N(\beta)$ となるから，$N(\alpha) \neq 1, N(\beta) \neq 1$ に注意して

$$N(\alpha) = N(\beta) = p$$

となる．$\alpha = a + bi$ $(a, b \in \mathbb{Z})$ とおくと

$$p = N(\alpha) = a^2 + b^2$$

となる．■

定理 7.0.5 寄素数 p に対して，次は同値である：

1) p は $\mathbb{Z}[i]$ の素元である．

2) $p = a^2 + b^2$ なる整数 $a, b \in \mathbb{Z}$ は存在しない．

3) $p \equiv 3 \pmod 4$.

[**証明**] p は奇数だから $p \equiv 1, 3 \pmod 4$ である．よって定理 7.0.4 より

$$1) \quad \Rightarrow \quad 2) \quad \Leftrightarrow \quad 3)$$

だから，2) $\to$ 1) を示せばよい．背理法を用いて p は $\mathbb{Z}[i]$ の素元ではないと仮定する．すると

$$p = \alpha \cdot \beta, \qquad \alpha \notin \mathbb{Z}[i]^\times, \quad \beta \notin \mathbb{Z}[i]^\times$$

なる $\alpha, \beta \in \mathbb{Z}[i]$ がとれる．両辺のノルムをとると

$$p^2 = N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) \qquad (N(\alpha), N(\beta) \in \mathbb{Z})$$

となるから，$N(\alpha) = 1, p, p^2$ である．$\alpha \notin \mathbb{Z}[i]^\times$ だから $N(\alpha) \neq 1$ である．$N(\alpha) = p^2$ とすると $N(\beta) = 1$ となり，これは $\beta \notin \mathbb{Z}[i]^\times$ に反する．よって $N(\alpha) = p$ である．$\alpha = a + bi$ $(a, b \in \mathbb{Z})$ とおくと

$$p = N(\alpha) = a^2 + b^2$$

となり，2) に反する．よって p は $\mathbb{Z}[i]$ の素元である．■

定理 7.0.3，定理 7.0.4，定理 7.0.5 をまとめると

1) $\pi = 1 + i$ は $\mathbb{Z}[i]$ の素元，

2) $p \equiv 3 \pmod 4$ なる素数 p は $\mathbb{Z}[i]$ の素元，

3) $p \equiv 1 \pmod 4$ なる素数 p に対して，$p = a^2 + b^2$ なる整数 a, b を $a > b > 0$ ととって，$\pi = a + bi, \pi' = a - bi$ は $\mathbb{Z}[i]$ の素元

となり，$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ 倍を除いて，$\mathbb{Z}[i]$ の素元は以上で尽くされる．

例 7.0.6 $\alpha = 3 + 5i \in \mathbb{Z}[i]$ の素因子分解を求めてみよう．

$$N(\alpha) = 3^2 + 5^2 = 34 = 2 \cdot 17$$

で，$2 = (1 + i)(1 - i) = i(1 - i)^2$ である．$17 \equiv 1 \pmod 4$ だから，素数 17 は $\mathbb{Z}[i]$ では二つの素元の積に分解する．

$$17 = 4^2 + 1^2 = (4 + i)(4 - i)$$

である．よって α の素因子の候補は $1-i, 4+i, 4-i$ である．

$$\frac{\alpha}{1-i} = \frac{(3+5i)(1+i)}{2} = -1+4i = i(4+i)$$

だから

$$\alpha = i(1-i)(4+i) = (1+i)(4+i)$$

が求める素因子分解である．

課題 7.1 例 7.0.6 を参考にして，$\alpha = 3+7i \in \mathbb{Z}[i]$ の素因子分解を求めよ．

課題 7.2 $\alpha = 4+7i \in \mathbb{Z}[i]$ の素因子分解を求めよ．