大学数学への接続シリーズ 3

# 素因数分解とイデアル

松田 修　著

2023 年 9 月 20 日

## はじめに

60 を正の整数で素因数分解すると，一意的に

$$60 = 2^2 \times 3 \times 5$$

となる．

ガウス整数は $a, b$ を整数としたときの $a + bi$ のことである．そして，ガウス整数にもガウス素数があり，ガウス整数はガウス素数で一意的に素因数分解される．

例えば，$1 + 2i$ と $1 - 2i$ はガウス素数であり，5 は一意的に

$$5 = (1 + 2i)(1 - 2i)$$

と素因数分解される．

整数やガウス整数とは異なる整数の集合は，他にもたくさんある．しかし，そのような集合の中には，素因数分解の一意性が成り立たないものがある．

イデアルは理想数というものを目指して到達した数の集合の概念である．

本書では，イデアルによる因数分解の考え方を説明する．

最後に，読者である小原 瑞季さん（東京大学 学生）から，いくつかの誤植と適切なご意見を頂き反映させました．ここに心より感謝いたします．

# 目次

**第 1 章　ガウス整数の素因数分解** 5
1.1　$\mathbb{Z}[i]$ と $\mathbb{Z}$ の共通点 . . . . . 6
1.2　$\mathbb{Z}[i]$ での割り算と余り . . . . . 7
1.3　$\mathbb{Z}[i]$ の素数と素因数分解 . . . . . 9

**第 2 章　一意的に素因数分解ができる環** 11
2.1　環の定義 . . . . . 11
2.2　真の約数と素数 . . . . . 12
2.3　一意分解整域と素因数分解 . . . . . 14

**第 3 章　素イデアル分解** 19
3.1　2 次整数環 $\mathbb{Z}^*[\sqrt{-5}]$ の不思議な素因数分解 . . . . . 19
3.2　イデアル . . . . . 20
3.3　具体的な素イデアル分解の計算 . . . . . 23

# 第 1 章

# ガウス整数の素因数分解

数学では，整数全体（整数の集合）を表す記号として，$\mathbb{Z}$（Zahlen，ドイツ語）が，よく使われる．$\mathbb{Z}$ の特徴的な性質は，「$\mathbb{Z}$ の中のどんな数もいくつかの素数を用いて素因数分解ができる」というものである．例えば，整数 60 は 3 つの素数 $2, 3, 5$ を用いて，$60 = 2^2 \cdot 3 \cdot 5$ と素因数分解できる．

さて，$i = \sqrt{-1}$ となる $i$ を考える．このとき $i^2 = -1$ となる．$i$ を**虚数単位**という．そして，$a$ と $b$ を整数として作られた新たな数 $a + bi$ を，**ガウス整数**といい，ガウス整数の集合を $\mathbb{Z}[i]$ で表す．すなわち，

$$\mathbb{Z}[i] = \{\ a + bi \mid a, b \in \mathbb{Z}\ \}$$

である．高校 2 年生で，**複素数**という数の集合 $\mathbb{C}$ を学習するが，それは，$a, b$ が実数の集合 $\mathbb{R}$ の元である数 $a + bi$ の集合のことである．したがって，ガウス整数の集合 $\mathbb{Z}[i]$ は複素数の集合の部分集合である．

$\mathbb{Z}[i]$ には素数があるだろうのか？　$\mathbb{Z}[i]$ でも素因数分解ができるのだろうか？

これが本書のモチベーションである．

## 1.1　$\mathbb{Z}[i]$ と $\mathbb{Z}$ の共通点

$\mathbb{Z}[i]$ には素数があるだろうのか？という問題を考える前に，$\mathbb{Z}[i]$ と $\mathbb{Z}$ の共通点を説明する．

実は，$\mathbb{Z}$ は**整数環**，$\mathbb{Z}[i]$ は**ガウス整数環**と呼ばれる．

ここで，**環**のことを簡単にいえば，足し算と引き算，そして掛け算という演算が定義された集合のことである．そして，これが $\mathbb{Z}$ と $\mathbb{Z}[i]$ の共通点である．

$\mathbb{Z}[i]$ の演算の定義を確認しよう．$a+bi, c+di \in \mathbb{Z}[i]$ に対して，

$$(a+bi) \pm (c+di) = (a \pm c) + (b \pm d)i \in \mathbb{Z}[i]$$

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i \in \mathbb{Z}[i]$$

である．

さらに，一般に，$a \in \mathbb{Z}$ の逆数は $\mathbb{Z}$ の中に存在しないし，$a+bi \in \mathbb{Z}[i]$ の逆数も $\mathbb{Z}[i]$ の中に存在しない．つまり，$\mathbb{Z}$ の一般的な整数 $a$ に対して逆数は

$$\frac{1}{a} \notin \mathbb{Z}$$

であり，$\mathbb{Z}[i]$ での一般的なガウス整数 $a+bi$ に対して逆数も

$$\frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \notin \mathbb{Z}[i]$$

である．

$\mathbb{Z}$ と $\mathbb{Z}[i]$ の共通点として，それぞれ掛け算が定義されていることから，$\mathbb{Z}$ と $\mathbb{Z}[i]$ の中に約数や倍数という概念が存在してくる．

**定義（約数と倍数）**　0 でない $a, b \in \mathbb{Z}$ について $a = bc$ となる $c \in \mathbb{Z}$ が存在するとき，$b$ は $a$ の**約数**（または**因数**），$a$ は $b$ の**倍数**であるという．

同様に，0 でない $a+bi, c+di \in \mathbb{Z}[i]$ について $a+bi = (c+di)(f+gi)$ となる $f+gi \in \mathbb{Z}[i]$ が存在するとき，$c+di$ は $a+bi$ の**約数**（または**因数**），$a+bi$ は $c+di$ の**倍数**であるという．

**例 1.1.** $1+i \in \mathbb{Z}[i]$ は $2 \in \mathbb{Z}[i]$ の約数であることを示せ．

解答．$(1+i)(1-i) = 2$ より $1+i$ は 2 の約数である．（解答終）

**問題 1.1.** $1+2i \in \mathbb{Z}[i]$ は $5 \in \mathbb{Z}[i]$ の約数であることを示せ．

## 1.2　$\mathbb{Z}[i]$ での割り算と余り

0 でない $a, b \in \mathbb{Z}$ について $a$ が $b$ の倍数になっていない場合がある．その場合は，筆算などを行うことで，$a = bc + r,\ |r| < |b|$ となる $c, r \in \mathbb{Z}$ を求めることができる．ここで，$|r|$ は $r$ の**絶対値**，すなわち，$|r|$ は数直線上における 0 と $r$ との距離である．このとき $c$ は $a$ を $b$ で割ったときの**商**，$r$ は $a$ を $b$ で割ったときの**余り**，と呼ばれる．例えば，$30 = 7 \cdot 4 + 2$ なので，30 を 7 で割ったときの商は 4 で，余りは 2 である．

以下に，ガウス整数 $\mathbb{Z}[i]$ での割り算と余りについて説明するが，その前に，まず，複素数 $a+bi$ の絶対値 $|a+bi|$ の定義の確認する．

複素数 $a+bi$ に対して，$xy$ 平面上の点 $(a, b)$ を対応させるとき，この平面を**ガウス平面**という．そして，ガウス平面における原点から $(a, b)$ までの距離を $a+bi$ の**絶**

**対値**と定める．このことから，

$$|a+bi| = \sqrt{a^2+b^2}$$

となる．そして絶対値は，以下の性質をもつ．

$$|(a+bi)(c+di)| = |a+bi||c+di|, \quad \left|\frac{a+bi}{c+di}\right| = \frac{|a+bi|}{|c+di|}$$

それでは，ガウス整数 $\mathbb{Z}[i]$ での割り算と余りについて説明する．

$a+bi, c+di \in \mathbb{Z}[i]$（ただし $c+di \neq 0$）について

$$a+bi = (c+di)(f+gi) + (r+si), \quad |r+si| < |c+di| \tag{1.1}$$

となるとき，$f+gi$ は $a+bi$ を $c+di$ で割ったときの**商**，$r+si$ は $a+bi$ を $c+di$ で割ったときの**余り**，と呼ばれる．

実は，以下の定理が証明されている．

**定理 1.1.**　$a+bi$ を $c+di$ で割ったとき，等式 (1.1) を満たす商 $f+gi$ と，余り $r+si$ が存在する．

**注意**　定理 1.1 において，商と余りが一意的に定まるわけではない．

**例 1.2.** $7+5i \in \mathbb{Z}[i]$ を $2+i \in \mathbb{Z}[i]$ で割った商と余りを 2 組求めよ．

解答．$7+5i = (3+i)(2+i)+2$，$|2| < |1+2i| = \sqrt{5}$ より，商 $3+i$，余り 2 が存在する．また，$7+5i = 4(2+i)+(-1+i)$，$\sqrt{2} = |-1+i| < |1+2i| = \sqrt{5}$ より，商 4，余り $-1+i$ が存在する．（解答終）

**問題 1.2.** $10+5i \in \mathbb{Z}[i]$ を $2+3i \in \mathbb{Z}[i]$ で割った商と余りを 2 組求めよ．

## 1.3　$\mathbb{Z}[i]$ の素数と素因数分解

$\mathbb{Z}[i]$ の一般的な数 $a+bi$ は逆数を持たないが，逆数をもつ数もいくつかある．逆数をもつ数を**単数**という．$\mathbb{Z}[i]$ の単数は，$\pm 1$, $\pm i$ である．

**定義（$\mathbb{Z}[i]$ の素数）**　0 でもない単数でもない $p+qi \in \mathbb{Z}[i]$ を

$$p+qi=(a+bi)(c+di)$$

と表すとき，$a+bi$ または $c+di$ が必ず単数となるとき，$p+qi$ を**素数**という．

では，$\mathbb{Z}[i]$ の素数をどのようにして見つけていけばよいか．エラトステネスのふるいと同じ方法がある．つまり，$|a+bi|$ が小さい順にその数が素数かどうか判定していけばよい．具体的に，$p>0, q>0$ である $|p+qi|^2 \leq 53$ までの素数 $p+qi$ を列挙しよう．

| $\lvert p+qi\rvert^2$ | 素数 |
|---|---|
| 2 | $1+i$ |
| 5 | $2+i$, $1+2i$ |
| 9 | 3 |
| 13 | $3+2i$, $2+3i$ |
| 17 | $1+4i$, $4+i$ |
| 29 | $2+5i$, $5+2i$ |
| 37 | $1+i$, $6+i$ |
| 41 | $4+5i$, $5+4i$ |
| 49 | 7 |
| 53 | $2+7i$, $7+2i$ |

次の定理が証明されている．

**定理 1.2.**　$\mathbb{Z}[i]$ の任意の数は単数倍を無視すると一意的に素因数分解される．

次の定理も有用である．

**定理 1.3.**　$\mathbb{Z}$ の素数 $p > 2$ が $p \equiv 3 \mod 4$ ならば，$p$ は $\mathbb{Z}[i]$ でも素数である．

**例 1.3.** $5 \in \mathbb{Z}[i]$ は素数でないことを示し，さらに $35 \in \mathbb{Z}[i]$ を素因数分解せよ．

解答．$5 = (2+i)(2-i) = (1+2i)(1-2i)$ より 5 は素数でない．

注意点は，$-i(1+2i) = 2-i$ であり，$2-i$ は $1+2i$ の単数倍になっていることである．同様に，$i(1-2i) = 2+i$ から，$2+i$ は $1-2i$ の単数倍になっている．

また 7 は素数である．したがって，35 の素因数分解は，単数倍を無視すると $35 = 5 \cdot 7 = 7(2+i)(2-i)$ となる．（解答終）

**問題 1.3.** $2 \in \mathbb{Z}[i]$ は素数でないことを示し，さらに $6 \in \mathbb{Z}[i]$ を素因数分解せよ．

# 第 2 章

# 一意的に素因数分解ができる環

## 2.1　環の定義

**環**（Ring）とは，和と差と積が定義された集合のことである．そして，$\mathbb{Z}$ と $\mathbb{Z}[i]$ は環であった．

環の正確な定義を述べよう．

**定義（環）**集合 $R$ には 2 つの内部演算 $+$（加法）と $\cdot$（乗法）が定義されていて，$R$ の任意の元 $a, b, c$ に対して，以下の全ての性質が成り立つとき，$R$ を**環**と呼ぶ．

(1) $a + b = b + a$

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

(3) $a + 0 = 0 + a$ となる 0 という元（**零元**）が存在する．

(4) $a + a' = 0$ となる $a'$ という元（$a$ の**反対元**）が存在する．

(5) $a \cdot (b + c) = ab + bc$，$(a + b) \cdot c = ac + bc$

環 $R$ が，乗法において $ab = ba$ を満たすとき，$R$ は**可換環**と呼ばれる．また，環 $R$ が，$a \cdot 1 = 1 \cdot a$ となる 1 という元（**単位元**）が存在するとき，$R$ は**単位的環**と呼ばれる．単位的環 $R$ の元 $u$ が $u \cdot u' = 1$ となる $u' \in R$ を持つとき，$u$ を**単数**という．

さて，$R$ を単位的可換環とする．$a \in R$ に対して $ab = ba = 0$ となる 0 でない $b \in R$ が存在するとき，$a$ を**零因子**という．そして，0 以外に零因子を持たない単位的可換環を**整域**という．そして $\mathbb{Z}$ も $\mathbb{Z}[i]$ もどちらも整域である．

**問題 2.1.** $\mathbb{Z}[\sqrt{2}] = \{\ a + b\sqrt{2} \mid a, b \in \mathbb{Z}\ \}$ は整域であることを証明せよ．

## 2.2　真の約数と素数

整数環 $\mathbb{Z}$ やガウス整数環 $\mathbb{Z}[i]$ における約数や倍数の概念は，単位的可換環 $R$ において一般的に定義される．

**定義（単位的可換での約数と倍数）**　$R$ を単位的可換環とする．

0 でない $a, b \in R$ について $a = bc$ となる $c \in R$ が存在するとき，$b$ は $a$ の**約数**（または**因数**），$a$ は $b$ の**倍数**であるという．

$p, q \in R$ が，$p = uq$ で $u$ が単数となるとき，$p$ と $q$ は**同伴**であるという．

**定義（真の約数）** $R$ を単位的可換環，$b \in R$ を 0 でない $a \in R$ の約数とする．

(1) $b$ が単数，または $b$ は $a$ と同伴であるとき，$b$ を $a$ の**自明な約数**という．

(2) $b$ が $a$ の自明な約数でないとき，$b$ を $a$ の**真の約数**という．

単位的可換環 $R$ における素数（素数）の定義は以下である．

**定義（単位的可換での素数）** $R$ を単位的可換環とする．

$p \in R$ が，0 でも単数でもなく，さらに真の約数を持たないならば，$p$ は $R$ の**素数**と呼ばれる．

**例 2.1.** $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ において，以下を証明せよ．

(1) $1 + \sqrt{2}$ は単数である．

(2) $N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$ と定義すると，

$$N((a + b\sqrt{2})(c + d\sqrt{2})) = N(a + b\sqrt{2})N(c + d\sqrt{2})$$

が成り立つ．

(3) $1 + 2\sqrt{2}$ は素数である．

解答．(1) $(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$ より $1 + \sqrt{2}$ は単数である．

(2)

$$\begin{aligned} \text{左辺} &= N((a + b\sqrt{2})(c + d\sqrt{2})) = N(ac + 2bd + (ad + bc)\sqrt{2}) \\ &= (ac + 2bd)^2 - 2(ad + bc)^2 = a^2c^2 - 2(a^2d^2 + b^2c^2) + 4b^2d^2 \end{aligned}$$

$$\begin{aligned} \text{右辺} &= N(a+b\sqrt{2})N(c+d\sqrt{2}) = (a^2-2b^2)(c^2-2d^2) \\ &= a^2c^2 - 2(a^2d^2+b^2c^2) + 4b^2d^2 \end{aligned}$$

よって，左辺 = 右辺となる．

(3) $1+2\sqrt{2} = (a+b\sqrt{2})(c+d\sqrt{2})$ とする．$N(1+2\sqrt{2}) = (1+2\sqrt{2})(1-2\sqrt{2}) = -7$ である．よって，設問 (2) より $N(a+b\sqrt{2})N(c+d\sqrt{2}) = -7$ である．したがって，$N(a+b\sqrt{2}) = \pm 1$ とできる．これは，$a+b\sqrt{2}$ が単数であることを意味する．よって，$c+d\sqrt{2}$ は $1+2\sqrt{2}$ の自明な約数である．したがって，$1+2\sqrt{2}$ は素数である．

（解答終）

**問題 2.2.** $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$ において，以下を証明せよ．

(1) $3+2\sqrt{2}$ は単数である．

(2) $1+3\sqrt{2}$ は素数である．

## 2.3　一意分解整域と素因数分解

整域 $R$ の中に一意的に素因数分解ができるものがある．

**定義（一意分解整域）**　$R$ を整域とする．$R$ が以下の条件をみたすとき，$R$ は**一意分解整域**と呼ばれる．

条件：0 でも単数でもない $a \in R$ に対して，$a = p_1p_2\cdots p_r$ となる素数 $p_1,\cdots,p_r \in R$ が存在する．

このとき，$a = p_1p_2\cdots p_r$ を $a$ の**素因数分解**という．

上の定義で何故“一意”という言葉が使われているか．それは以下の定理があるからである．

**定理 2.1.**　$R$ を一意分解整域とする．このとき，0 でも単数でもない $a \in R$ の素因数分解は一意的である．すなわち，もし素数 $p_i, q_j \in R$ が存在して，

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

と 2 通りに素因数分解されたとしても，$r = s$ であり，さらに，積の順序を入れ替えれば，$p_i = u_i q_i$ で $u_i$ は単数となる．

整数環 $\mathbb{Z}$ とガウス整数環 $\mathbb{Z}[i]$ は一意分解整域である．より一般的な整数環でこのことを考えるために，2 次整数環 $\mathbb{Z}^*[\sqrt{D}]$ というものを，以下のように定義する．

**定義（2 次整数環）**　$D$ を平方因数をもたない整数とする．

(1) $D \equiv 2, 3 \mod 4$ のとき，

$$\mathbb{Z}^*[\sqrt{D}] = \{\ a + b\sqrt{D} \mid a, b \in \mathbb{Z}\ \}$$

(2) $D \equiv 1 \mod 4$ のとき，

$$\mathbb{Z}^*[\sqrt{D}] = \left\{\ \frac{a}{2} + \frac{b}{2}\sqrt{D} \mid a, b \in \mathbb{Z},\ \ a \equiv b \mod 2\ \right\}$$

以下のことが知られている．

**定理 2.2.**　$D < 100$ において，一意分解整域である 2 次整数環 $\mathbb{Z}^*[\sqrt{D}]$ は，以下である．

$D = -1, -2, -3, -7, -11, -19, -43, -67, -163, 2, 3, 5, 6, 7, 11, 13, 14, 17, 19,$
$21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83,$
$86, 89, 93, 94, 97.$

定理 2.2 の証明においては，ノルム $N(a+b\sqrt{D})$ が重要な役割を果たしている．

**定義（ノルム）**　$D$ を平方因数をもたない整数とし，2 次整数環 $\mathbb{Z}^*[\sqrt{D}]$ を考える．このとき，

$$N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - b^2 D$$

を $a+b\sqrt{D}$ の**ノルム**という．

簡単な計算から，以下の定理が得られる．

**定理 2.3.**

$$N((a+b\sqrt{D})(c+d\sqrt{D})) = N(a+b\sqrt{D})N(c+d\sqrt{D})$$

素数の判定には以下の定理が有用である．

**定理 2.4.**　$a+b\sqrt{D}$ は，$|N((a+b\sqrt{D})|$ が整数環 $\mathbb{Z}$ で素数ならば，2 次整数環 $\mathbb{Z}^*[\sqrt{D}]$ で素数である．

**例 2.2.** $\mathbb{Z}^*[\sqrt{3}]$ において，$-12+5\sqrt{3}$ を，素因数分解せよ．

解答．$|N(-12+5\sqrt{3})| = 69 = 3 \times 23$ である．よって，

$$-12+5\sqrt{3} = (a+b\sqrt{3})(c+d\sqrt{3}),\ |N(a+b\sqrt{3})| = 3,\ |N(c+d\sqrt{3})| = 23$$

と置くことができる．よって

$$ac + 3bd = -12, \quad ad + bc = 5, \quad |a^2 - 3b^2| = 3, \quad |c^2 - 3d^2| = 23$$

を得る．これより，解の 1 つとして $a = 3, b = -2, c = 2, d = 3$ を得る．$\mathbb{Z}[\sqrt{3}]$ は一意分解整域であるので, $-12+5\sqrt{3}$ の素因数分解は, $-12+5\sqrt{3} = (3-2\sqrt{3})(2+3\sqrt{3})$ としてよい．（解答終）

**問題 2.3.** $\mathbb{Z}^*[\sqrt{3}]$ において，$-9 + 4\sqrt{3}$ を，素因数分解せよ．

# 第 3 章

# 素イデアル分解

## 3.1　2 次整数環 $\mathbb{Z}^*[\sqrt{-5}]$ の不思議な素因数分解

まず，$D = -5 \equiv 3 \mod .4$ なので，$\mathbb{Z}^*[\sqrt{-5}] = \mathbb{Z}[\sqrt{-5}]$ であることを注意する．その上で，$6 \in \mathbb{Z}^*[\sqrt{-5}]$ を因数分解してみると，

$$6 = 2 \cdot 3 \quad \text{または，} \quad 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

とできる．

2 と 3 は素数なのか？

まず，$N(2) = 4$ であるため，$2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ で $N(a + b\sqrt{-5}) = 2$, $N(c + d\sqrt{-5}) = 2$ と置ける．よって

$$ac - 5bd = 2, \quad ad + bc = 0, \quad |a^2 + 5b^2| = 2, \quad |c^2 + 5d^2| = 2$$

を得るが，これを満たす整数 $a, b, c, d$ は存在しない．したがって，2 は素数である．同様に $N(3) = 9$ であるため，$3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ で $N(a + b\sqrt{-5}) = 3$, $N(c + d\sqrt{-5}) = 3$ と置ける．よって

$$ac - 5bd = 3, \quad ad + bc = 0, \quad |a^2 + 5b^2| = 3, \quad |c^2 + 5d^2| = 3$$

を得るが，やはりこれを満たす整数 $a, b, c, d$ は存在しない．したがって，3 は素数である．

$1+\sqrt{-5}$ と $1-\sqrt{-5}$ は素数なのか？

まず，$N(1+\sqrt{-5}) = 6$ であるため，$1+\sqrt{-5} = (a+b\sqrt{-5})(c+d\sqrt{-5})$ で $N(a+b\sqrt{-5}) = 2$，$N(c+d\sqrt{-5}) = 3$ と置ける．よって

$$ac-5bd=1,\quad ad+bc=1,\quad |a^2+5b^2|=2,\quad |c^2+5d^2|=3$$

を得るが，これを満たす整数 $a,b,c,d$ は存在しない．したがって，$1+\sqrt{-5}$ は素数である．同様にして，$N(1-\sqrt{-5})$ も素数であることがわかる．

つまり，$\mathbb{Z}^*[\sqrt{-5}]$ において，6 は，$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ というように 2 通りに素因数分解されてしまうのである．

**問題 3.1.** $\mathbb{Z}^*[\sqrt{-5}]$ において，21 は 2 通りに素因数分解されることを示せ．

## 3.2　イデアル

2 次整数環 $\mathbb{Z}^*[\sqrt{-5}]$ においては，たとえば 6 や 21 などのように，素因数分解が 2 通りに表されてしまった．

$\mathbb{Z}^*[\sqrt{-5}]$ の数を 1 通りに分解できる方法はないのだろうか．

１９世紀のドイツの数学者エルンスト・クンマー (Ernst Eduard Kummer) は，この問題に対し，**理想数**というアイデアから研究を行った．そして，１９世紀のドイツの数学者リヒャエル・デーデキント (Julius Wilhelm Richard Dedekind) は，クンマーの理想数を発展させ，**イデアル**と**素イデアル**いうアイデアを提示した．

デーデキントが証明した定理を，本書の内容の範囲で述べると以下のようになる．

**定理 3.1.**　$D$ を平方数でない正の整数とし，2 次整数環 $\mathbb{Z}^*[\sqrt{D}]$ を考える．このとき，$\mathbb{Z}^*[\sqrt{D}]$ の（$\mathbb{Z}^*[\sqrt{D}]$ 自身を除いた）任意のイデアルは，有限個の素イデアルの積で一意的に分解される．

それでは，以下にイデアルと素イデアルの定義を述べる．

**定義（イデアル）** 可換環 $R$ の空でない部分集合 $I$ が，以下の 2 つの条件をみたすとき，$I$ を $R$ の**イデアル**という．

(1) 任意の $a, b \in I$ に対し，$a + b \in I$, $-a \in I$

(2) 任意の $x \in R$, $a \in I$ に対し，$xa \in I$

例えば，2 次整数環 $\mathbb{Z}^*[\sqrt{-5}]$ において，

$$(2) = \{\ 2(a + b\sqrt{-5}) \mid a, b \in \mathbb{Z}\ \}$$

と置くと，(2) は $\mathbb{Z}^*[\sqrt{-5}]$ のイデアルである．また，

$$(1 + \sqrt{-5}) = \{\ (1 + \sqrt{-5})(a + b\sqrt{-5}) \mid a, b \in \mathbb{Z}\ \}$$

も $\mathbb{Z}^*[\sqrt{-5}]$ のイデアルである．

以下の定理は，イデアルの定義から直ちに得られる．

**定理 3.2.** $R$ を単位的可換環とする．$a_1, a_2, \cdots, a_r \in R$ に対して，

$$(a_1, a_2, \cdots, a_r) = \{\ x_1a_1 + x_2a_2 + \cdots + x_ra_r \mid x_r \in R\ \}$$

と置くと，これは $R$ のイデアルとなる．

定理 3.2 で与えられたイデアル $(a_1, a_2, \cdots, a_r)$ を $a_1, a_2, \cdots, a_r \in R$ から**生成されるイデアル**という．

**定義（素イデアル）**　可換環 $R$ のイデアル $P$ が，以下の 2 つの条件をみたすとき，$P$ を $R$ の**素イデアル**という．

(1)　$P \neq R$

(2)　$a, b \in R$ について，$ab \in P$ ならば $a \in P$ または $b \in P$ である．

例えば，$\mathbb{Z}^*[\sqrt{-5}]$ において，イデアル $(2)$ とイデアル $(1+\sqrt{-5})$ はどちらも $\mathbb{Z}^*[\sqrt{-5}]$ の素イデアルではない．しかし，イデアル $(2, 1+\sqrt{-5})$ は $\mathbb{Z}^*[\sqrt{-5}]$ の素イデアルである．このことについて説明する．

$P = (2, 1+\sqrt{-5})$ と置く．このとき，$P$ の任意の元 $a$ は，ある $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ を用いて $a = 2(x_1 + x_2\sqrt{-5}) + (1+\sqrt{-5})(y_1 + y_2\sqrt{-5})$ と書けるが，これを整理すると

$$a = 2(x_1 - x_2 - 3y_2) + (1+\sqrt{-5})(2x_2 + y_1 + y_2)$$

となるので，$P = \{2x + (1+\sqrt{-5})y \mid x, y \in \mathbb{Z}\}$ であることを注意する．

そこで，$(a + b\sqrt{-5})(c + d\sqrt{-5}) \in P$ と仮定する．つまり，

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = 2x + (1+\sqrt{-5})y \tag{3.1}$$

となる $x, y \in \mathbb{Z}$ が存在していると仮定する．

式 (3.1) を変形すると，

$$(ac - 5bd) + (ad + bc)\sqrt{-5} = (2x + y) + y\sqrt{-5}$$

となり，これより

$$ac - 5bd = 2x + y, \quad ad + bc = y$$

を得る．上式の差をとると

$$(a - b)(c - d) = 6bd + 2x$$

を得る．よって，$a-b$ は偶数, または $c-d$ は偶数である．したがって，$a+b\sqrt{-5} = (a-b)+b(1+\sqrt{-5}) \in P$ または $c+d\sqrt{-5} = (c-d)+d(1+\sqrt{-5}) \in P$ である．よって，$P$ は素イデアルである．

**問題 3.2.** イデアル $(3, 1+\sqrt{-5})$ は $\mathbb{Z}^*[\sqrt{-5}]$ の素イデアルであることを示せ．

## 3.3 具体的な素イデアル分解の計算

定理 3.1 を理解するためには，イデアルの和と積の定義を理解する必要がある．

**定義（イデアルの和と積）** $I$ と $J$ を可換環 $R$ のイデアルとする．$I$ と $J$ の和と積は以下のように定義される．

和： $I+J = \{\ a+b\ \ a \in I,\ b \in J\ \}$

積： $IJ = \left\{\ \sum_{i=1}^{n} a_i b_i\ \ a_i \in I,\ b_i \in J,\ n \in \mathbb{N}\ \right\}$

以下の定理はイデアルの和と積の定義から直ちに得られる．

**定理 3.3.** $R$ を単位的可換環とし，$I = (a_1, a_2)$, $J = (b_1, b_2)$ を $R$ のイデアルとする．このとき，

$$I+J = J+I = (a_1, a_2, b_1, b_2), \quad IJ = JI = (a_1b_1, a_1b_2, a_2b_1, a_2b_2)$$

である．

以下，具体的な素イデアル分解の計算をみていこう．

**例 3.1.**　$\mathbb{Z}^*[\sqrt{-5}]$ の素イデアル $P_1 = (2, 1+\sqrt{-5})$，$P_2 = (3, 1+\sqrt{-5})$，$P_3 = (3, 1-\sqrt{-5})$ を考える．このとき，以下の素イデアル分解を示せ．

$(2) = P_1^2$，$(3) = P_2P_3$，$(1+\sqrt{-5}) = P_1P_2$，$(1-\sqrt{-5}) = P_1P_3$，$(6) = P_1^2P_2P_3$

解答．$(2) = P_1^2$ を示す．

$$P_1^2 = (2, 1+\sqrt{-5})(2, 1+\sqrt{-5}) = (4, 2+2\sqrt{-5}, -4+2\sqrt{-5}) \subset (2)$$

であり，$2 = \{2+2\sqrt{-5}\} - \{4-4+2\sqrt{-5}\}$ より $(2) \subset P_1^2$ であることから，$P_1^2 = (2)$ が得られる．

$(3) = P_2P_3$ を示す．

$$P_1P_2 = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (9, 3+3\sqrt{-5}), 3-3\sqrt{-5}, 6) \subset (3)$$

であり，$3 = 9-6$ より $(3) \subset P_1P_2$ であることから，$P_1P_2 = (3)$ が得られる．

$(1+\sqrt{-5}) = P_1P_2$ を示す．

$$P_1P_2 = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}), -4+2\sqrt{-5}) \subset (1+\sqrt{-5})$$

であり，$1+\sqrt{-5} = \{3+3\sqrt{-5}\} - \{2+2\sqrt{-5}\}$ より $(1+\sqrt{-5}) \subset P_1P_2$ であることから，$P_1P_2 = (1+\sqrt{-5})$ が得られる．

$(1-\sqrt{-5}) = P_1P_3$ を示す．

$$P_1P_3 = (2, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (6, 2-2\sqrt{-5}, 3+3\sqrt{-5})) \subset (1-\sqrt{-5})$$

であり，$1-\sqrt{-5} = 6 - [\{2-2\sqrt{-5}\} + \{3+3\sqrt{-5}\}]$ より $(1-\sqrt{-5}) \subset P_1P_3$ であることから，$P_1P_3 = (1-\sqrt{-5})$ が得られる．

最後に，$(6) = P_1^2P_2P_3$ であることは，$P_1^2P_2P_3 = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5}) = (6)$ よりいえる．

（解答終）

**問題 3.3.** $\mathbb{Z}^*[\sqrt{-5}]$ の素イデアル $P_1 = (3, 1+2\sqrt{-5})$, $P_2 = (3, 1-2\sqrt{-5})$, $P_3 = (7, 1+2\sqrt{-5})$, $P_4 = (7, 1-2\sqrt{-5})$
を考える．このとき，以下の素イデアル分解を示せ．

$(3) = P_1P_2$, $(7) = P_3P_4$, $(1+2\sqrt{-5}) = P_1P_3$, $(1-2\sqrt{-5}) = P_2P_4$,
$(21) = P_1P_2P_3P_4$

**問題の解答**

**問題 1.1**　$(1+2i)(1-2i)=5$ より $1+2i$ は 5 の約数である．

**問題 1.2**　$10+5i=5(2+3i)-10i,\ \ |-10i|<|2+3i|=\sqrt{13}$ より，商 5，余り $-10i$ が存在する．また，$10+5i=(3-2i)(2+3i)-2,\ \ |-2|<|2+3i|=\sqrt{13}$ より，商 $3-2i$，余り $-2$ が存在する．

**問題 1.3**　$2=(1+i)(1-i)$ より 2 は素数でない．また 3 は素数である．したがって，6 の素因数分解は，単数倍を無視すると $6=2\cdot 3=3(1+i)(1-i)$ となる．

**問題 2.1**　$a+b\sqrt{2},c+d\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ に対し，$(a+b\sqrt{2})(c+d\sqrt{2})=(c+d\sqrt{2})(a+b\sqrt{2})$ が成り立ち．$1\in\mathbb{Z}[\sqrt{2}]$ であることから，$\mathbb{Z}[\sqrt{2}]$ は単位的可換環である．さらに，0 以外に零因子がないことは明らかなので，$\mathbb{Z}[\sqrt{2}]$ は整域である．

**問題 2.2**　(1) $(3+2\sqrt{2})(3-2\sqrt{2})=1$ より $3+2\sqrt{2}$ は単数である．

(2) $1+3\sqrt{2}=(a+b\sqrt{2})(c+d\sqrt{2})$ とする．

$N(1+3\sqrt{2})=(1+3\sqrt{2})(1-3\sqrt{2})=-17$ である．よって，$N(a+b\sqrt{2})N(c+d\sqrt{2})=-17$ である．したがって，$N(a+b\sqrt{2})=\pm 1$ とできる．これは，$a+b\sqrt{2}$ が単数であることを意味する．よって，$c+d\sqrt{2}$ は $1+3\sqrt{2}$ の自明な約数である．したがって，$1+3\sqrt{2}$ は素数である．

**問題 2.3**　$|N(-9+4\sqrt{3})|=33=3\times 11$ である．よって，

$$-9+4\sqrt{3}=(a+b\sqrt{3})(c+d\sqrt{3}),\ |N(a+b\sqrt{3})|=3,\ |N(c+d\sqrt{3})|=11$$

と置くことができる．よって

$$ac+3bd=-9,\ \ ad+bc=4,\ \ |a^2-3b^2|=3,\ \ |c^2-3d^2|=11$$

を得る．これより，解の 1 つとして $a=1,b=2,c=3,d=-2$ を得る．$\mathbb{Z}[\sqrt{3}]$ は一意分解整域であるので，$-9+4\sqrt{3}$ の素因数分解は，$-9+4\sqrt{3}=(1+2\sqrt{3})(3-2\sqrt{3})$ としてよい．

**問題 3.1**　$21=3\cdot 7=(1+2\sqrt{-5})(1-2\sqrt{-5})$ である．3 は素数であった．$N(7)=49$ なので，$7=(a+b\sqrt{-5})(c+d\sqrt{-5})$ で $N(a+b\sqrt{-5})=7$，$N(c+d\sqrt{-5})=7$

と置けるが,

$$ac - 5bd = 7, \quad ad + bc = 0, \quad |a^2 + 5b^2| = 7, \quad |c^2 + 5d^2| = 7$$

を満たす整数 $a, b, c, d$ は存在しない．したがって，7 は素数である．

次に，$N(1 + 2\sqrt{-5}) = 21$ なので，$1 + 2\sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5})$ で $N(a + b\sqrt{-5}) = 3$，$N(c + d\sqrt{-5}) = 7$ と置けるが,

$$ac - 5bd = 1, \quad ad + bc = 2, \quad |a^2 + 5b^2| = 3, \quad |c^2 + 5d^2| = 7$$

を満たす整数 $a, b, c, d$ は存在しない．したがって，$1 + 2\sqrt{-5}$ は素数である．同様にして，$1 - 2\sqrt{-5}$ も素数であることがわかる．

**問題 3.2** $P = (3, 1 + \sqrt{-5})$ と置く．このとき，$P$ の任意の元 $a$ は，ある $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ を用いて $a = 3(x_1 + x_2\sqrt{-5}) + (1 + \sqrt{-5})(y_1 + y_2\sqrt{-5})$ と書けるが，これを整理すると

$$a = 3(x_1 - x_2 - 2y_2) + (1 + \sqrt{-5})(3x_2 + y_1 + y_2)$$

となるので，$P = \{3x + (1 + \sqrt{-5})y \mid x, y \in \mathbb{Z}\}$ であることを注意する．

そこで，$(a + b\sqrt{-5})(c + d\sqrt{-5}) \in P$ と仮定する．つまり,

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = 3x + (1 + \sqrt{-5})y \tag{3.2}$$

となる $x, y \in \mathbb{Z}$ が存在していると仮定する．式 (3.2) を変形すると,

$$(ac - 5bd) + (ad + bc)\sqrt{-5} = (3x + y) + y\sqrt{-5}$$

となり，これより

$$ac - 5bd = 3x + y, \quad ad + bc = y$$

を得る．上式の差をとると

$$(a - b)(c - d) = 6bd + 3x$$

を得る．よって，$a - b$ は 3 の倍数, または $c - d$ は 3 の倍数である．したがって，$a + b\sqrt{-5} = (a - b) + b(1 + \sqrt{-5}) \in P$ または $c + d\sqrt{-5} = (c - d) + d(1 + \sqrt{-5}) \in P$ である．よって，$P$ は素イデアルである．

**問題 3.3**　$(3) = P_1P_2$ を示す.

$$P_1P_2 = (3, 1+2\sqrt{-5})(3, 1-2\sqrt{-5}) = (9, 3+6\sqrt{-5}, 3-6\sqrt{-5}, 21) \subset (3)$$

であり，$3 = 9 - [\{3+6\sqrt{-5}\} + \{3-6\sqrt{-5}\}]$ より $(3) \subset P_1P_2$ であることから，
$P_1P_2 = (3)$ が得られる.

$(7) = P_3P_4$ を示す.

$$P_3P_4 = (7, 1+2\sqrt{-5})(7, 1-2\sqrt{-5}) = (49, 7+14\sqrt{-5}), 7-14\sqrt{-5}, 21) \subset (7)$$

であり，$7 = 49 - 2 \cdot 21$ より $(7) \subset P_3P_4$ であることから，$P_3P_4 = (7)$ が得られる.

$(1+2\sqrt{-5}) = P_1P_3$ を示す.

$$P_1P_3 = (3, 1+2\sqrt{-5})(7, 1+2\sqrt{-5}) = (21, 3+6\sqrt{-5}, 7+14\sqrt{-5}), -19+4\sqrt{-5}) \subset (1+2\sqrt{-5})$$

であり，$1+2\sqrt{-5} = \{7+14\sqrt{-5}\} - 2 \cdot \{3+6\sqrt{-5}\}$ より $(1+2\sqrt{-5}) \subset P_1P_3$ で
あることから，$P_1P_3 = (1+2\sqrt{-5})$ が得られる.

$(1-2\sqrt{-5}) = P_2P_4$ を示す.

$$P_2P_4 = (3, 1-2\sqrt{-5})(7, 1-2\sqrt{-5}) = (21, 3-6\sqrt{-5}, 7-14\sqrt{-5}, -19-4\sqrt{-5}) \subset (1-2\sqrt{-5})$$

であり，$1-2\sqrt{-5} = \{7-14\sqrt{-5}\} - 2 \cdot \{3-6\sqrt{-5}\}]$ より $(1-2\sqrt{-5}) \subset P_2P_4$ で
あることから，$P_2P_4 = (1-2\sqrt{-5})$ が得られる.

最後に，$(21) = P_1P_2P_3P_4$ であることは,
$P_1P_2P_3P_4 = (3)(7) = (1+2\sqrt{-5})(1-2\sqrt{-5}) = (21)$ よりいえる.