**今日のテーマ**《単項イデアル整域は素元分解環である》
今回は、単項イデアル整域 (単項イデアル環で、整域にもなっているもの、略して PID) は、「素因数分解」が出来ることをしめす。

まず、

$$12 = (-3) \times (-4) = (-1) \times 3 \times (-4) = \dots$$

のような無用の分解を避けるために、$\pm 1$ に類するものを特別扱いすることにする。

**定義 11.1.** $R$ は環であるとする。$R$ の元のうち、積に関して可逆なものの全体を $R^\times$ であらわす。

$$R^\times = \{x \in R; \exists y \in R \text{ に対して } xy = yx = 1 \text{ が成り立つ } \}$$

**例 11.1.** $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, $\mathbb{C}[X]^\times = \mathbb{C}^\times$.

**補題 11.1.** 可換環 $R$ の元 $x$ について、次は同値である。

(1) $x \in R^\times$
(2) $(x) = R$

**定義 11.2.** 可換環 $R$ の元 $x$ が素元であるとは、$(x)$ が $R$ の素イデアルであるときにいう。

**定義 11.3.** 整域 $R$ が素元分解環であるとは、$R$ の任意の元 $x$ について、次のいずれかが成り立つときに言う。

(1) $x$=0
(2) $x \in R^\times$
(3) $x$ は $R$ の素元の積に分解される。

例えば、 $\mathbb{Z}$ ,$\mathbb{C}[X]$ は素元分解環である。もっと一般に、次のことが成り立つ。

**定理 11.1.** $R$ が単項イデアル整域ならば、$R$ は素元分解環である。

この定理の証明はいくつかの段階にわかれる。
まず、次の事実の拡張からはじめよう。

**事実 11.1.** 整数 $x, y, z$ があって、 $yz$ は $x$ で割り切れ、かつ $x, y$ が互いに素であるとする。このとき、$z$ は $x$ で割り切れる。

整数 $x, y$ が互いに素なら、$(x, y) = \mathbb{Z}$ であったことを思い起こすと、次の補題は上の事実の拡張であることが分かるだろう。

**補題 11.2.** 可換環 $R$ の元 $x, y, z$ があって、 $yz$ は $x$ で割り切れ、かつ $(x, y) = R$ であるとする。このとき、$z$ は $x$ で割り切れる。

**定義 11.4.** $R$ は可換環であるとする。$R$ の元 $x$ が既約であるとは、

$$\forall y \forall z (y, z \in R, yz = x \implies (y \in R^\times \text{ または } z \in R^\times))$$

のときに言う。

**補題 11.3.** $R$ は整域であるとする。このとき、

(1) $R$ の素元は、必ず既約である。
(2) $R$ の既約元は、必ずしも素元とは限らない。
(3) $R$ が $PID$ ならば、$R$ の既約元は必ず素元である。

上の補題により、単項イデアル整域 $R$ の元 $x$ を素因数分解する手順は次のようになる。

(1) $x = 0$ または $x \in R^\times$ ならば、おしまい。
(2) $x$ が素元ならば、やはりおしまい。
(3) それ以外なら、$x = yz$ $(y, z \in R \setminus R^\times, y, z \neq 0)$ と分解できる。
(4) $y, z$ について同様のことをする。(例えば $y, z$ が 素元でなければ、 $y = y_1 y_2$ となる。)
(5) 繰り返す。

あとの問題は、一つの元が無限に分解されていかないか、ということである。これを解決するのには、前回の補題を用いればよい。

(参考) $\mathbb{C}[X]$ の部分環 $R = \mathbb{C}[X^2, X^3]$ を考えると、

$$R = \{f \in \mathbb{C}[X];\ f \text{ の } X \text{ に関する一次の項の係数は } 0\}$$

であることが分かる。ここで、$a = X^2, b = X^4, c = X^3$ とおくと、$ab = c^2$ であるが、

(1) $a$ は $R$ のなかで既約である
(2) $a$ は $R$ のなかで $c$ の約数ではない。

ということが分かる。このように、単に「環」といってもこのような「特異な」環も含まれるので、その元の取り扱いには通常の整数を取り扱う以上の注意が必要である。

$\mathbb{Z}[\sqrt{5}]$ のなかの

$$(\sqrt{5} - 1)(\sqrt{5} + 1) = 2 \cdot 2$$

なども、素因数分解の非一意性の例である。

※レポート問題

つぎのうち一問を選択して解きなさい。(期限:次の講義の終了時まで。)

(I) 整域 $R$ に対して、次のことを示しなさい。
  (a) $R^\times$ は乗法に関して群をなす。
  (b) $R$ に次のような同値関係をいれることが出来る。

  $$x \sim y \Leftrightarrow (\exists u \in R^\times \text{ に対して } x = uy \text{ が成り立つ})$$

  (この同値関係で同値な二つの元を、<u>同伴な</u> 二つの元と呼ぶ。)
  (c) $x$ が $y$ の倍元で、$y$ が $x$ の倍元でもあるなら、$x$ と $y$ とは同伴である。

(II) 整域 $R$ が与えられているとし、$p, p_1, p_2, p_3 \ldots p_k$ は全て $R$ の素元であるとする。このとき、もし $x = p_1 p_2 \ldots p_k$ が $p$ の倍元であれば、$p_1, p_2, \ldots, p_k$ のうちどれか一つは必ず $p$ と同伴であることを示しなさい。(同伴の定義は前問参照。但し、前問に答えることは要求しない。(前問の結果は仮定してよい。))

(III) $\mathbb{Z}[\sqrt{-1}]$ はユークリッド環、したがって素元分解環である。(証明不要) そこで、$z = 16 + 63i$ を $\mathbb{Z}[\sqrt{-1}]$ において素元分解せよ。(ヒント: まず $z\bar{z}$ の素因数分解を試みよ。素因数分解の一意性を信じれば、いろんな数の共通因数が求めたくなる筈である。そういうときはユークリッドの互除法を用いよ。最後に、数が本当に素元であるかどうか知りたいときには、

$$\begin{aligned} x = yz &\implies x\bar{x} = y\bar{y}z\bar{z} \\ &\implies |x|^2 \text{ は } |y|^2 \text{ と } |z|^2 \text{ の積に分解される} \end{aligned}$$

ということをうまく用いよ。)