代数学 IB NO.10 要約

今日のテーマ《素元分解環》
「素因数分解の一意性」が成り立つような環を素元分解環と呼ぶ。
ただし、

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

のような無用の分解を避けるために、± 1 に類するもの (可逆元) を特別扱いすることにする。

定義 10.1. 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 (可逆元) 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 10.1. $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, $\mathbb{C}[X]^\times = \mathbb{C}^\times$.

環論においては、元 x の性質を調べる代わりに、x の生成するイデアル (x) を調べるとうまくいくことがある。以下の議論でも頻繁に使われるので注意しておくとよい。歴史的には、一般の環では元だけの扱いに限界があって、イデアルを導入するとうまくいくということに Dedekind が気付き、そこで展開されたイデアル論に古典的な幾つかの議論が吸収されたのだ。

補題 10.1. 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 10.2. 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 10.3. 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 10.1. 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 (今週と来週) 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 10.1. 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 10.2. 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 10.4. 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 10.3. 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 が単項イデアル環で、なおかつ整域ならば、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。次の補題がその問題に答える:

補題 10.4. 単項イデアル環 R のイデアルの増大列

$$I_1 \subset I_2 \subset I_3 \subset I_4 \subset \dots$$

は必ずどこかで止まる。すなわちある N があって、

$$I_N = I_{N+1} = I_{N+2} = \dots$$

がなりたつ。

(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。

問題 10.1. 素元分解環 R の元 a, b, m について、

$$\gcd(a, b) = \gcd(a, b + ma)$$

が成り立つことを示しなさい。

ヒント: gcd の定義

$$d | \gcd(a, b) \quad \Leftrightarrow \quad (d|a \text{ かつ } d|b)$$

を有効に使うこと。

問題 10.2. $m, n \in \mathbb{Z}$ が $\mathbb{Z}$ において互いに素 (すなわち、m, n の最大公約数が 1) ならば、$\mathbb{Z}[\sqrt{-1}]$ の元としても互いに素であることを証明せよ。

問題 10.3. $\mathbb{Z}[\sqrt{-1}]$ が素元分解環であることをもちいて、互いに素な $m, n \in \mathbb{Z}$ に対して $\mathbb{Z}[\sqrt{-1}]$ の元として

$$\gcd(m + n\sqrt{-1}, m - n\sqrt{-1}) = 1$$

が成り立つことを示しなさい。