環論 NO.10 要約

$\boxed{\text{今日のテーマ}}$ 整域における整除の問題

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. 環 R と $a, b \in R$ とにたいして、

(1) $a \in bR$ のとき、 a は b の**倍元**であるといい、$b|a$ で書き表す。b を主語として、b は a の**約元**であるともいう。
(2) ある $u \in R^\times$ があって、$a = bu$ をみたすとき、a と b とは**同伴**であるという。

命題 10.1. 整域 R の元 a, b にたいして、

(1) $(a) \subset (b) \Leftrightarrow b|a$.
(2) a と b が同伴 $\Leftrightarrow (a) = (b)$.

定義 10.3. 整域 R が与えられているとする。$d_0 \in R$ が $a, b \in R$ の**最大公約元** (gcd) であるとは

$$\forall d \in R\,(\ d|d_0 \quad \Leftrightarrow \quad (d|a \text{ かつ } d|b)\ )$$

が成り立つときに言う。

定義 10.4. 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 10.5. 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。

定義 10.6. R は可換環であるとする。R の元 x が**既約**であるとは、 x が 0 でも可逆元でもなく、なおかつ

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

をみたすときに言う。

補題 10.2. 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。

- $\mathbb{Z}[\sqrt{5}]$ では素因数分解は一意的でない。例えば

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