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

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。とくに整除の問題はイデアルの包含関係に翻訳される。

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を R の**可逆元**と言い、その全体を $R^\times$ 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 10.2. $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, $\mathbb{C}[X]^\times = \mathbb{C}^\times$.

補題 10.3. 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 10.4. 環 R と $a, b \in R$ とにたいして、

(1) $a \in bR$ のとき、 a は b の (R における) **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 (R における) **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 (R において) **同伴**であるという。

命題 10.5. 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 10.6. 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。

a, b の最大公約元がもし存在すれば、それを $\gcd(a, b)$ と書く。
定義を追っかけていくと、すぐに次のことがわかる。

命題 10.7. 整域 R が与えられているとする。$a, b \in R$ に対して、

$d_0 = \gcd(a, b) \Leftrightarrow (d_0)$ は (a, b) を含む単項イデアルの中で最小。

とくに、a, b の最大公約数は同伴を除いて一意的である。

定義 10.8. 可換環 R の元 x が**素元**であるとは、$x \neq 0$ で、かつ (x) が R の素イデアルであるときにいう。

- $R = \mathbb{Z}[\sqrt{-5}]$ では

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3.$$

が成り立つ。このことから、$2, 3$ は ($1 + \sqrt{-5}, 1 - \sqrt{-5}$ も) それぞれ R の素元ではないことがわかる。ところが、これらの数は R ではこれ以上分解できない (次回。) R では「素因数分解の一意性」が成り立たないのである。