

今日のテーマ 《素元分解環》(2)

素元の定義

$p$ : 素元<sup>def</sup>  $p \neq 0$  かつ  $(p)$  は  $R$  の素イデアル  
 $\Leftrightarrow p \neq 0$  かつ  $(\forall a \in R \forall b \in R (p|ab \implies (p|a \text{ or } p|b)))$   
 「 $ab$  が  $p$  で割れるなら  $a$  と  $b$  のどちらかは  $p$  で割れる。」

参照: 整域の定義 (零因子を 0 以外にもたない)

「 $ab$  が 0 と等しいなら  $a$  と  $b$  のどちらかは 0 である。」

既約元の定義

$p$ : 既約元<sup>def</sup>  $(\forall y \in R \forall z \in R (yz = x \implies (y \in R^\times \text{ または } z \in R^\times)))$   
 「分解できない」 (分解できたとしたら片方が可逆元)

**命題 12.1.**  $R$  が素元分解環ならば、 $R \setminus \{0\}$  の各元は

$$up_1p_2 \dots p_l \quad (l \in \mathbb{N}, u \in R^\times, p_1, \dots, p_l \text{ は } R \text{ の素元})$$

と書くことができるが、この書き方は並び方と同伴を除いて一意である。すなわち、

$$up_1p_2 \dots p_l = vq_1q_2 \dots q_m$$

$$(l, m \in \mathbb{N}, u, v \in R^\times, p_1, \dots, p_l, q_1, \dots, q_m \text{ は } R \text{ の素元})$$

ならば、 $l = m$  であって、なおかつある置換  $\sigma \in \mathfrak{S}_l$  があって各  $j$  に対して  $p_j$  と  $q_{\sigma(j)}$  はそれぞれ同伴になる。

**問題 12.1.** 整域  $R$  の元  $a, b$  の最大公約元が 2 つあったとすれば、それらは互いに同伴であることを証明せよ。

- ED: Euclidean domain
- PID: principal ideal domain
- UFD: unique factorization domain 直訳は「一意分解整域」。