

今日のテーマ 逆元といえば、ハイ互除法。

ユークリッド環(余りを許したわり算のできる環)  $R$  においては、与えられた  $a, b \in R$  にたいし、 $a, b$  の最大公約数  $d$  が存在し、互除法により、 $al + bm = d$  を満たす  $l, m$  を具体的に求めることができるのでした。(No.8 参照。)

命題 13.1. 環  $R$  と、 $a, b, d \in R$  に対して、次の二条件は同値である。

- (1)  $R$  のイデアルの等式  $(a, b) = (d)$  が成り立つ。
- (2)  $al + bm = d$  ( $\exists l, m \in R$ ) かつ  $d|a$  かつ  $d|b$  が成り立つ。

単項イデアル整域(PID)  $R$  においては、与えられた  $a, b \in R$  について、命題 13.1 の二番目の条件を満たす  $(d)$  が存在することに注意。

定理 13.2. PID  $R$  の元  $a, b$  が互いに素であるとき、 $R/(a)$  において、 $b$  の同値類  $[b]_{(a)}$  は逆元をもつ。

実際、 $al + bm = 1$  を満たす  $l, m \in R$  が存在する。 $[l]_{(a)}$  がその逆元である。

定義 13.1.  $R_1, R_2$  は環であるとする。このとき、 $R_1, R_2$  の環としての直積とは、デカルト積集合  $R_1 \times R_2$  の上に、次のような演算を定義したものである。

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b) \times (c, d) = (ac, bd)$$

$R_1$  と  $R_2$  の環としての直積を、普通  $R_1 \times R_2$  と書く。

補題 13.1.  $R_1, R_2$  は環であるとする。このとき、

- (1)  $R_1 \times R_2$  は環になる。
- (2)  $R_1, R_2$  の単位元がそれぞれ  $1_{R_1}, 1_{R_2}$  とすると、 $R_1 \times R_2$  の単位元は  $(1_{R_1}, 1_{R_2})$  である。
- (3)  $R_1, R_2$  がともに可換ならば、 $R_1 \times R_2$  も可換である。

ベクトル空間で基本ベクトルが重要な役割を果たしたように、環の直積においても、 $e_1 = (1_{R_1}, 0_{R_2})$  と  $e_2 = (0_{R_1}, 1_{R_2})$  が重要な役割を果たす。関係式

$$e_1 + e_2 = 1, \quad e_1 e_2 = 0, \quad e_1^2 = e_1, \quad e_2^2 = e_2$$

が成り立つことに注意せよ。 $e_1, e_2$  は直積の「射影」(もしくは射影元)と呼ばれる。

命題 13.3. 環  $R$  の元  $a, b$  が  $(a, b) = (1)$  を満たすとき、

$$R/(ab) \ni [x]_{ab} \mapsto ([x]_a, [y]_b) \in R/(a) \times R/(b)$$

なる写像は環の同型を与える。

例 13.1 (環の直積分解の具体例).

- (1)  $\mathbb{Z}/12\mathbb{Z}$  は  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$  と同型である。
- (2)  $\mathbb{C}[X]/(X^2 - X)$  は  $\mathbb{C}[X]/(X) \times \mathbb{C}[X]/(X - 1)$  と同型である。

※三つの環  $R_1, R_2, R_3$  の直積も二つの場合と同様に定義される。環  $(R_1 \times R_2) \times R_3$  は  $R_1 \times R_2 \times R_3$  と同型である。4つ以上でも同様。

古典的な 105 減算は、同型  $\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$  をもとにしている。

問題

- (I)  $L = 2012113$  とおく。このとき、5桁以上の正の整数  $N (< L)$  を自分できめて、その  $N$  にたいして、 $\mathbb{Z}/L\mathbb{Z}$  において、 $N$  の逆元をもとめよ。
- (II) 1000 で割ると 17 余り、1003 で割ると 34 余るような整数  $n$  の例を一つ求めよ(途中の計算はある程度省略してよい。ただし求めた方法は書いておくこと。)