中国剰余定理 (chinese remainder theorem)

目次

定義 1 : イデアル (ideal) R を可換環とする。以下を見たす R の部分集合 I を R 上のイデアルという。

(I1) $\forall x, y \in I, x + y \in I$

(I2) $\forall x \in I, a \in R, ax \in I$

系 1 : 単項イデアル (principal ideal) 可換環 R のある元 $m \in R$ によって書かれる集合 I

$$I = \{am \mid a \in R\}$$

はイデアルとなる。この I を m を生成元とする単項イデアルという。また、m を生成元とする単項イデアルを mR と書くこともある。

定義 2 : 剰余類 (residue class) 可換環 R 上のイデアル I と任意の $x \in R$ に対して

$$x + I = \{x + a \mid a \in I\}$$

を x を代表元とする剰余類という。また x を代表元とする剰余類を $\overline{x}$ とも書く。

定理 1 : ある $x, y \in R$ が $x - y \in I$ であるとき、$x + I = y + I$ である。

Proof. I の生成元が m であるとする。まず定義より $x + I$ の任意の元 a はある $q \in R$ によって

$$a = x + mq$$

と書くことができる。ここで仮定より、ある p によって $x - y = mp \Leftrightarrow x = y + mp$ となる。この x を代入すると

$$\begin{aligned} a &= y + mp + mq \\ &= y + m(p + q) \end{aligned}$$

となり、$a \in y+I$ が得られた。ここで a は任意の $x+I$ の元であるため $a \in x+I \Rightarrow a \in y+I$ が示された。同様にして $a \in y+I \Rightarrow a \in x+I$ が示される。以上より示された。 □

定義 3 : 剰余環 (quotient ring) 可換環 R 上のイデアル I に対して

$$R/I = \{x + I \mid x \in R\}$$

として書かれる集合 R/I を R 上の剰余環という。

定理 2 : 可換環 R 上の剰余環 R/I は可換環となる。

Proof. □

定理 3 : hoge

定理 4 : ある剰余環 R/mR と R/nR の元からなる組の集合

$$\{(a + mR, b + nR) \mid a, b \in R\}$$

は以下に定める加法と乗法に対して環となる。

加法 任意の $a, b, a', b' \in R$ に対して $(a+mR, b+nR)+(a'+mR, b'+nR) = ((a+a')+mR, (b+b')+nR)$

乗法 任意の $a, b, a', b' \in R$ に対して $(a+mR, b+nR)\times(a'+mR, b'+nR) = ((a\times a')+mR, (b\times b')+nR)$

Proof. □

定理 5 : 中国剰余定理 (Chinese Remainder Theorem) ある整数 m, n に対して最小公倍数と最大公約数をそれぞれ

$$l = \mathrm{lcm}(m, n), \quad g = \gcd(m, n)$$

とする。このとき剰余環 $\mathbb{Z}/l\mathbb{Z}$ と $\{((ga + r) + m\mathbb{Z}, (gb + r) + n\mathbb{Z}) \mid a, b, c \in \mathbb{Z}, 0 \le r < g\}$ は環同型となる。

Proof. $(gx + r) + l\mathbb{Z} \in \mathbb{Z}/l\mathbb{Z}$ に対してある $\phi((gx + r) + l\mathbb{Z})$ を

$$\phi((gx + r) + l\mathbb{Z}) = ((gx + r) + m\mathbb{Z}, (gx + r) + n\mathbb{Z})$$

とすると ϕ は $\mathbb{Z}/l\mathbb{Z}$ を始域、$\{((ga + r) + m\mathbb{Z}, (gb + r) + n\mathbb{Z}) \mid a, b, c \in \mathbb{Z}, 0 \le r < g\}$ を終域とする同型写像となることを示す。

まず、ϕ が写像となることを示す。任意の $x \in \mathbb{Z}, 0 \leq r < \mathbb{Z}, y \in (gx+r)+l\mathbb{Z}$ に対して、ある $a \in \mathbb{Z}$ が存在し

$$y = gx + r + la$$

が成立する。前提より、$l = \frac{mn}{g}, g|m, g|n$ であるため

$$y = gx + r + \frac{mn}{g}a = gx + r + m\left(\frac{n}{g}a\right) = gx + r + n\left(\frac{m}{g}a\right)$$

となる。したがって、任意の x, r に対して

$$(gx+r)+l\mathbb{Z} \subset (gx+r)+m\mathbb{Z}, \quad (gx+r)+l\mathbb{Z} \subset (gx+r)+n\mathbb{Z}$$

となる。よって ϕ は

$$y = gx + r + \frac{mn}{g}a = gx + r + m\left(\frac{n}{g}a\right) = gx + r + n\left(\frac{m}{g}a\right)$$

したがって □