現代数学の流れ　第17回

定義1　G：群　$g \in G$

$g^n = e$ となる $n \in \mathbb{N}$ が存在するとき、そのような n の最小の値を g の位数という。$g^n = e$ となる $n \in \mathbb{N}$ が存在しないとき、g の位数は ∞ とする。

ユークリッドの互除法

$a, b \in \mathbb{Z}$ について　$b \neq 0$ とき、

$$a = bq + r \quad (0 \leq r < |b|)$$

となる $q, r \in \mathbb{Z}$ が見つかる。

q を a を b で割ったときの商といい、r を余りという。

$a, b \in \mathbb{Z}$ について　$lcm(a,b)$ を a, b の最小公倍数　という。

$gcd(a,b)$ を a, b の最大公約数

定理 $a, b \in \mathbb{Z}$ $b \neq 0$ について

$$a = bq + r \quad (0 \leq r < |b|)$$

$(q, r \in \mathbb{Z})$ とおく.

$$\gcd(a, b) = \gcd(b, r)$$

が言える.

$m \mid \gcd(a, b) \Rightarrow m \mid a$ かつ $m \mid b$

$\Rightarrow m \mid bq + r$ かつ $m \mid b$

$\Rightarrow m \mid r$ かつ $m \mid b$

$\Rightarrow m \mid \gcd(b, r)$

証明. $m \mid \gcd(b, r) \Rightarrow m \mid b$ かつ $m \mid r$

$\Rightarrow m \mid b$ かつ $m \mid a - bq$

$\Rightarrow m \mid b$ かつ $m \mid a$

$\Rightarrow m \mid \gcd(a, b)$

$\therefore \gcd(a, b) = \gcd(b, r)$ //

$a, b \in \mathbb{Z}$ $(b \neq 0)$ について.

$a_0 = a \qquad b_0 = b$

$a_0 = b_0 q_0 + r_0 \quad (0 \leq r_0 < |b_0|)$

$a_1 = b_0 \qquad b_1 = r_0$

$a_1 = b_1 q_1 + r_1 \quad (0 \le r_1 < |b_1|)$

$a_2 = b_1 \qquad b_2 = r_1$

$\vdots$

$a_N = b_N q_N + r_N$

$a_{N+1} = b_N \qquad b_{N+1} = r_N$

とすると. $r_0 < |b_0| \qquad r_1 < |b_1| = r_0 \qquad r_2 < b_2 = r_1$

ポイント a と, $r_0 > r_1 > r_2 > \cdots > r_N \ge 0$

ポイント. ところで $r_N = 0$ となる. すると.

$\gcd(a,b) = \gcd(a_0, b_0) = \gcd(b_0, r_0) = \gcd(a_1, b_1) = \cdots$

$\cdots = \gcd(a_N, b_N) = \gcd(b_N, r_N) = \gcd(a_{N+1}, 0)$

$= a_{N+1}$

となり、このとき

$$\gcd(a,b) = b_N = r_{N-1} = a_{N-1} - b_{N-1} q_{N-1}$$

$$= b_{N-2} - r_{N-2} q_{N-1} = b_{N-2} - (a_{N-2} - b_{N-2} q_{N-2}) q_{N-1}$$

$$= a_{N-2} x_{N-2} + b_{N-2} y_{N-2} \quad (x_{N-2} = -q_{N-1},\ y_{N-2} = 1 + q_{N-2} q_{N-1})$$

$$= b_{N-3} x_{N-2} + (a_{N-3} - b_{N-3} q_{N-3}) y_{N-2}$$

$$= a_{N-3} x_{N-3} + b_{N-3} y_{N-3} \quad (x_{N-3} = y_{N-2},\ y_{N-3} = x_{N-2} - q_{N-3} y_{N-2})$$

$$\vdots$$

$$= a_0 x_0 + b_0 y_0$$

$$= a x_0 + b y_0$$

とでき、$\gcd(a,b) = ax + by$ をみたす $x, y \in \mathbb{Z}$ が見つかる。

これをユークリッドの互除法という。

例1 $a = 39 \quad b = 25$

$39 = 1 \cdot 25 + 14$

$25 = 1 \cdot 14 + 11$

$14 = 1 \cdot 11 + 3$

$11 = 3 \cdot 3 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$\therefore \quad 1 = 3 - 1 \cdot 2 = 3 - (11 - 3 \cdot 3) = 4 \cdot 3 - 11$

$= 4 \cdot (14 - 11) - 11 = 4 \cdot 14 - 5 \cdot 11 = 14 \cdot 4 - 5 \cdot (25 - 14)$

$= 9 \cdot 14 - 5 \cdot 25 = 9 (39 - 25) - 5 \cdot 25$

$= 9 \cdot 39 - 14 \cdot 25$

$\therefore \quad x = 9 \quad y = -14.$

例3　$a, b \in \mathbb{Z}$　（$b \neq 0$ または $a \neq 0$）

$g < d$　$(a, b) = d$　とおく。

ここで、　$\{ax + by \mid x, y \in \mathbb{Z}\} = d\mathbb{Z} = \{dx \mid x \in \mathbb{Z}\}$

$a = dk$　$b = dl$　とでき

$\therefore$　$ax + by = d(kx + ly) \in d\mathbb{Z}$

$\therefore$　$\{ax + by \mid x, y \in \mathbb{Z}\} \subset d\mathbb{Z}$

次に逆を示す。

まず　$\{ax + by \mid x, y \in \mathbb{Z}\}$ は $\mathbb{Z}$ の 部分群 になっていることに注意つつ、

$\therefore$　$d \in \{ax + by \mid x, y \in \mathbb{Z}\}$ を示せば 良いが。

これは　ユークリッドの 互除法 より　従う。

11

R: 可換環

$$R^\times = \{ r \in R \mid r \cdot r' = 1 \text{ となる } r' \in R \text{ が存在する} \}$$

とおけば $(R^\times, \cdot)$ は 可換 アーベル群になる.

(:) 結合法則, 可換性 および 単位元 は ok.

積で閉じていることは.

$r_1, r_2 \in R^\times$ に対して $r_1^{-1}, r_2^{-1} \in R$ があること.

$$(r_1 r_2)\ r_2^{-1} \cdot r_1^{-1} = 1$$

より $r_1 r_2 \in R^\times$

逆元は $r \cdot r^{-1} = 1$ より. $r^{-1} \in R^\times$

//

証明

$n \in \mathbb{N}$

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} = \left\{ \overline{m} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(n, m) = 1 \right\}$$

m, n が互いに素なので.

$$mx + ny = 1$$

となる $x, y \in \mathbb{Z}$ が 見つかる.

$$\therefore \quad \overline{m} \cdot \overline{x} + \overline{n} \cdot \overline{y} = \overline{1}$$

$$\| \\ \overline{m} \cdot \overline{x}$$

より. $\overline{m} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$

逆に $\overline{m} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$ なので. $\overline{m} \cdot \overline{x} = 1$ となる $x \in \mathbb{Z}$ が 存在する.

$\therefore \quad mx - 1 = ny$ とでき. $\therefore \quad 1 = mx + n \cdot (-y)$ となる.

$\therefore \quad \gcd(h, n) = 1$ が言える. //

系1 p: 素数 のとき.

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{p-1}\}$ は体になる.

例1 $\left(\mathbb{Z}/10\mathbb{Z}\right)^{\times} = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$

命題6 $M \subset \mathbb{Z}$: 部分群

$\Rightarrow$ ある $d \in \mathbb{Z}$ が存在して $M = d\mathbb{Z}$ が言える.

(:) $M = \{0\}$ なら $d = 0$ で ok.

そこで $M \neq \{0\}$ とする. $h \in M \Rightarrow -h \in M$ より

$\{h \in M \mid h > 0\}$

は空でない.

そこで $d = \min\{ h \in M \mid h > 0 \}$ とおく.

$M = d\mathbb{Z}$

が言える.

$d\mathbb{Z} \subset M$ は ok.

$h \in M$ について

$h = dq + r \quad (0 \leq r < d)$

と書く. $r = h - dq \in M$ が言える.

d の最小性より, $r = 0$ が言える.

$\therefore \quad h \in d\mathbb{Z}$ // //

系1　G：群　$g \in G$

g a 位数が $d > 0$ （有限）

ここで、

$$g^n = e \quad \Leftrightarrow \quad n \text{ は } d \text{ の倍数}$$

が言える。

$(\Leftarrow)$ は明らか。

$(\Rightarrow)$　$M = \{ n \in \mathbb{Z} \mid g^n = e \}$ とおく。

M は $\mathbb{Z}$ の部分群

$$d = \min \{ n \in M \mid n > 0 \} = g \text{ の位数}$$

で　$M = d\mathbb{Z}$ が言える。

$\therefore$　$n \in M$ は d の倍数

//

命題8

G: 群　$g \in G$　　$\mathrm{ord}(g) = g$の位数 $= d < +\infty$

のとき、$H = \langle g \rangle = \{ g^n \in G \mid n \in \mathbb{Z} \}$ は有限群で

$|H| = d$ である。

(∵)

$n = qd + r$　$(0 \leq r < d)$ とおくと、

$$g^n = g^{qd+r} = (g^d)^q \cdot g^r = g^r$$

$\therefore H = \{ g^0, \cdots, g^{d-1} \}$ となる

$0 \leq i < j < d$ について

$$g^i = g^j \Rightarrow g^{j-i} = e$$

$0 \leq j-i < d$ より、$j = i$　$\therefore g^i = g^j$　より　$|H| = d$.

//

準同型写像・同型

2つのベクトル空間が与えられたとき、その間の線形写像を考えた。

同様のことを群でも考えたい。

定義9 G_1, G_2 : 群

写像 $\phi: G_1 \to G_2$ が準同型であるとは

$\forall g_1, g_2 \in G_1$ に対して

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$$

が成り立つことをいう。

補足10 $\phi: G_1 \to G_2$: 群の準同型

ならば、

(1) $\phi(e_{G_1}) = e_{G_2}$

(2) $\forall g \in G_1$ $\phi(g^{-1}) = \phi(g)^{-1}$

(1) $\phi(e_{G_1}) = \phi(e_{G_1} \cdot e_{G_1}) = \phi(e_{G_1}) \cdot \phi(e_{G_1})$

$\Rightarrow \quad e_{G_2} = \phi(e_{G_1})$

(2) $\phi(g^{-1})\ \phi(g) = \phi(g^{-1}g) = \phi(e_{G_1}) = e_{G_2}$

同様に $\phi(g)\ \phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_{G_1}) = e_{G_2}$

$\therefore \quad \phi(g^{-1}) = \phi(g)^{-1}$ //

定義 群準同型 $\phi: G_1 \to G_2$ が同型であるとは、ϕ が全単射のことをいう。

命題 同型写像 $\phi: G_1 \to G_2$ の逆写像も同型。

$\phi^{-1}: G_2 \to G_1$ について

$\forall g_1, g_2 \in G_2$ について $\quad \phi^{-1}(g_1 g_2) = \phi^{-1}(g_1)\,\phi^{-1}(g_2)$

を示したい。

しかし ϕ は準同型なので

$$\phi\left(\phi^{-1}(g_1 g_2)\right) = \phi\left(\phi^{-1}(g_1)\,\phi^{-1}(g_2)\right)$$

を示せば良い.

$$\phi\left(\phi^{-1}(g_1 g_2)\right) = g_1 g_2$$

$$\phi\left(\phi^{-1}(g_1)\,\phi^{-1}(g_2)\right) = \phi\left(\phi^{-1}(g_1)\right)\phi\left(\phi^{-1}(g_2)\right) = g_1 g_2$$

∴ 題意が言える. //

定義13 $\phi: G_1 \to G_2$: 群準同型

ϕ の核 (kernel) を

$$\ker(\phi) = \{\, g \in G_1 \mid \phi(g) = e_{G_2} \,\}$$

で定める.

ϕ の像 (image) を

$$Im(\phi) = \{ \phi(g) \in G_2 \mid g \in G_1 \}$$

で定める.

命題14 (1) $Ker(\phi)$ は G_1 の部分群

(2) $Im(\phi)$ は G_2 の部分群

(証明) (1) $g_1, g_2 \in Ker(\phi)$ について

$$\phi(g_1 g_2) = \phi(g_1) \cdot \phi(g_2) = e_{G_1} \cdot e_{G_2} = e_{G_2}$$

より $g_1 g_2 \in Ker(\phi)$

$\phi(e_{G_1}) = e_{G_2}$ より, $e_{G_1} \in Ker(\phi)$

Σ 5 $\forall g \in \ker(\phi)$

$$\phi(g^{-1}) = \phi(g)^{-1} = e_{G_2}^{-1} = e_{G_2}$$

Σ 7. $g^{-1} \in \ker(\phi)$

(2) $\phi(g_1), \phi(g_2) \in \mathrm{Im}(\phi)$

$$\phi(g_1)\cdot\phi(g_2) = \phi(g_1 \cdot g_2) \in \mathrm{Im}(\phi)$$

$$e_{G_2} = \phi(e_{G_1}) \in \mathrm{Im}(\phi)$$

$\phi(g) \in \mathrm{Im}(\phi)$ について

$$\phi(g)^{-1} = \phi(g^{-1}) \in \mathrm{Im}(\phi).$$

//