現代数学への流れ　第5回

群

定義1

G：集合

G上の演算

$$\psi : G \times G \to G$$
$$(g_1, g_2) \mapsto g_1 \cdot g_2$$

について $(G, \cdot)$ が群であるとは，以下の3つの条件をみたすことをいう．

(i)（結合法則）任意の $g_1, g_2, g_3 \in G$ に対して

$$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$$

が成り立つ．

(ii) (単位元の存在)

ある元 $e \in G$ が存在して 任意の $g \in G$ に対して

$$g \cdot e = e \cdot g = g$$

が成り立つ。 e を単位元という。

(iii) 任意の $g \in G$ に対して $g^{-1} \in G$ が存在して

$$g \cdot g^{-1} = g^{-1} \cdot g = e$$

がいえる。 g^{-1} で g の逆元という。

さらに 以下が成り立つとき。 G はアーベル群であるという。

(iv) 任意の $g_1, g_2 \in G$ に対して

$$g_1 \cdot g_2 = g_2 \cdot g_1$$

補足2 (a) (ii) の e の性質をみたす元は一意に存在する.

(∵) e' を単位元とすると.

$$e' = e \cdot e' = e$$

が言える. //

(b) g^{-1} も $g \in G$ に対して一意に決まる.

(∵) 別に $g^{-1\prime}$ が存在すれば.

$$g^{-1\prime} = g^{-1\prime} \cdot e = g^{-1\prime} \cdot (g \cdot g^{-1})$$

$$= (g^{-1\prime} \cdot g) \cdot g^{-1} = e \cdot g^{-1} = g^{-1} \quad //$$

(c) 結合法則より, 積の順序は問題にならない.

$$(xy)(zw) = ((xy)z) \cdot w = (x \cdot (yz)) \cdot w$$

など. ∴ ( ) を外して

$(xy)(zw) =$ $xyzw$ と書いて良い.

$(G, \cdot)$: 群

$h \in \mathbb{Z}$ について　$g \in G$

$h > 0$ ならば　$g^h = \underbrace{g \cdots \cdot g}_{h\text{個}}$

$h = 0$ ならば　$g^0 = e$

$h < 0$ ならば　$g^h = \underbrace{g^{-1} \cdot \cdots \cdot g^{-1}}_{|h|\text{個}}$

と定める.

Gが有限集合のとき. $|G|$ を Gの位数という.

例

$G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$,

$(G, +)$ はアーベル群

単位元は0　$h \in G$ に対して逆元は$-h$　$x \in G$　$h \in \mathbb{Z}$　$x^h = hx$ と書く.

例 $X = \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$G = X \setminus \{0\}$

$(G, \cdot)$ は アーベル群

$z \neq 0$ は 群となる.

(∵) $z \neq 0$ に対して, $z^{-1} = \frac{1}{z}$ もて. //

例 $G = S_n$: n次置換全体の集合

$(S_n, \circ)$ は 群になる.

単位元は 恒等写像 逆元は 逆写像

例 $GL_n(\mathbb{R}) = \{ A \in M_{n,n}(\mathbb{R}) \mid \det(A) \neq 0 \}$

$\mathbb{R}$ 上の $n \times n$ 行列の空間

$\therefore$ $(GL_n(\mathbb{R}), \times)$ は 群になる.

☺ 行列の積算は 結合法則をみたす.

単位行列 $E_n \in GL_n(\mathbb{R})$ は単位元.

$A \in GL_n(\mathbb{R})$ について $\det(A) \neq 0$ より

逆行列 A^{-1} が存在して $\det(A^{-1}) = \det(A)^{-1} \neq 0$

$\therefore$ $A^{-1} \in GL_n(\mathbb{R})$ //

例 $G = \{a, b\}$

$\times$	a	b
a	a	b
b	b	a

すると、$(G, *)$ は群

(二) (i) a は単位元 . 実際、

$$a^2 = a \qquad ab = ba = b$$

(ii) $a^{-1} = a \qquad b^{-1} = b$

(iii)

(a) $(xy)z = x(yz)$

x, y, z どれが a どきは . ok .

(b) $(bb)b = b(bb)$ も ok . //

補題) G : 群 $\quad x, y, z \in G$ について

(i) $xy = xz \Rightarrow y = z$

(ii) $xy = z \Rightarrow y = x^{-1}z \qquad x = zy^{-1}$

(ii) $y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz)$

$= (x^{-1}x)z = e\cdot z = z$

(ii)

$y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}z$

$x = x(yy^{-1}) = (xy)y^{-1} = zy^{-1}$ //

例 G: 群 $x, y, z \in G$

$xy^{-1}zxyx = e$

$\Rightarrow y^{-1}zxy = x^{-1}x^{-1} \Rightarrow zx = yx^{-1}x^{-1}y^{-1}$

$\Rightarrow z = yx^{-2}y^{-1}x^{-1}$

命題4　　G: 群

(i) $x, y \in G$ に対し $(xy)^{-1} = y^{-1}x^{-1}$

(ii) $x \in G$ に対し $(x^{-1})^{-1} = x$

(i) $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = e$

$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}y = e$

(ii) $(x^{-1})\cdot x = e = x\cdot x^{-1}$ より $x = (x^{-1})^{-1}$ が従う.

例　$S_3 = \{id, (12), (13), (23), (123), (132)\}$

$\sigma\tau$ の表

$\sigma \backslash \tau$	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(132)	(123)	(23)	(13)
(13)	(13)	(123)	id	(132)	(12)	(23)
(123)	(123)	(13)	(23)	(12)	(132)	id
(132)	(132)	(23)	(12)	(13)	id	(123)

例 $c > 0$: 実数

$G = (-c, c)$

ψ

$x, y \qquad x +_c y = \dfrac{x+y}{1+\frac{xy}{c^2}} \qquad \in (-c, c)$

$x, y \in (-c, c)$ を示す

$(c-x)(c-y) > 0$

$c^2 - (x+y)c + xy > 0$

$$\Rightarrow \quad 1+\frac{xy}{c^2} > \frac{1}{c}(x+y) \quad \Rightarrow \quad c > \frac{x+y}{1+\frac{xy}{c^2}}$$

よって $(c+x)(c+y) > 0 \quad \Rightarrow \quad -c < \dfrac{x+y}{1+\frac{xy}{c^2}}$ //

これより、 $(\mathbb{R}, \tau_c)$ は可換群.

(i) $x, y, z \in \mathbb{R}$

$$(x \overset{+}{c} y) \overset{+}{c} z = \left(\frac{x+y}{1+\frac{xy}{c^2}}\right) \overset{+}{c} z = \frac{\frac{x+y}{1+\frac{xy}{c^2}} + z}{1+\frac{1}{c^2}\left(\frac{x+y}{1+\frac{xy}{c^2}}\right)\cdot z}$$

$$= \frac{\left(x+y+z+\frac{xyz}{c^2}\right)}{1+\frac{xy}{c^2}+\frac{yz}{c^2}+\frac{zx}{c^2}} \quad \cdots (*)$$

$$x \oplus (y \oplus z) = x \oplus_c \left(\frac{y+z}{1+\frac{yz}{c^2}} \right) = \frac{x + \frac{y+z}{1+\frac{yz}{c^2}}}{1 + \frac{1}{c^2} x \cdot \left(\frac{y+z}{1+\frac{yz}{c^2}} \right)}$$

$$= \frac{\left(x + y + z + \frac{xyz}{c^2} \right)}{1 + \frac{xy}{c^2} + \frac{yz}{c^2} + \frac{zx}{c^2}} = (*)$$

(ii) $0 \oplus_c x = \frac{0+x}{1} = x$

$x \oplus_c 0 = \frac{x+0}{1} = x$

(iii) $x \oplus_c (-x) = 0 = (-x) \oplus_c x$

(iv) $x \oplus_c y = y \oplus_c x$ is ok. //

可換環と体

定義 R：集合　$+, \cdot$: R 上の二つの演算

以下が成り立つとき、$(R, +, \cdot)$ を可換環であるという。

(i) $(R, +)$ はアーベル群

(ii) 任意の $r_1, r_2, r_3 \in R$ に対して　$(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$

(iii) 任意の $r_1, r_2 \in R$ に対して。　$r_1 \cdot r_2 = r_2 \cdot r_1$

(iv) ~~あ~~ ある元 $1_R \in R$ が存在して 任意の $r \in R$ に対して　$1_R \cdot r = r$ が成える。

(v) 任意の $r_1, r_2, r_3 \in R$ に対して。　$r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$

さらに $(K, +, \cdot)$ が体であるとは 以下の二つが成り立つことをいう。

(vi) $0_R \neq 1_R$

(vii) 任意の $r \in R \setminus \{0\}$ に対して ある $r^{-1} \in R$ が存在して $r \cdot r^{-1} = 1_R$ がいえる.

補足 (a) 1_R は一意に決まる.

(:) 別に $1_R'$ が存在したとすると.

$$1_R' = 1_R' \cdot 1_R = 1_R$$

がいえる. //

(b) R が体のとき, 任意の $r \in R \setminus \{0\}$ に対して r^{-1} は一意に決まる.

(:) 別に $r^{-1}{}'$ が存在したとすると.

$$r^{-1}{}' = r^{-1}{}' \cdot 1_R = r^{-1}{}' \cdot (r \cdot r^{-1}) = (r^{-1}{}' \cdot r) \cdot r^{-1}$$

$$= 1_R \cdot r^{-1} = r^{-1}$$

//

(c) 任意の $r \in R$ に対して $0 \cdot r = 0$ が成り立つ.

$(0+0) \cdot r = 0 \cdot r + 0 \cdot r$

$\| \quad \Rightarrow \quad 0 = 0 \cdot r$

$0 \cdot r$

//

(d) 任意の $r \in R$ に対して $(-1) \cdot r = -r$ が成り立つ.

$r + (-1) \cdot r = 1 \cdot r + (-1) \cdot r$

$= (1 + (-1)) \cdot r = 0 \cdot r = 0$

より $(-1) \cdot r = -r$.

//

(e) $0_R = 1_R$ ならば $R = \{0\}$ が成り立つ.

$r \in R$ について

$r = r \cdot 1_R = r \cdot 0_R = 0$

//

例一　$R=(\mathbb{Z},+,\cdot)$ 可換環．体でない

$R=(\mathbb{Q},+,\cdot)$ 体

$R=(\mathbb{R},+,\cdot)$ 体

$R=(\mathbb{C},+,\cdot)$ 体

例一　$n\in\mathbb{N}$ を一つ固定する．

$\mathbb{Z}$ 上の同値関係 $\equiv_n$ を

$x\equiv_n y \iff n\mid x-y$

で定義する．$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv_n$ と定める．

x の同値類を $\overline{x}$ と記す.

このとき. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ がいえる.

$\mathbb{Z}/n\mathbb{Z}$ 上の演算 $+$, $\cdot$ を以下で定義する.

$$\overline{x} + \overline{y} = \overline{x+y}$$

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

このとき. $+$, $\cdot$ は well-defined !!

(:) $x_1 \equiv x_2$ $y_1 \equiv y_2$ より.

$\therefore$ $x_1 = x_2 + nk$ $y_1 = y_2 + nl$ とできる.

このとき. $x_1 + y_1 = x_2 + nk + y_2 + nl = x_2 + y_2 + n(k+l)$

より. $x_1 + y_1 \equiv x_2 + y_2$ がいえる.

$$x_1 - y_1 = (x_2 + nk)(y_2 + nl)$$

$$= x_2 y_2 + n(x_2 l + k y_2 + nkl)$$

即, $x_1 y_1 \equiv x_2 y_2$ が成る. //

$(\mathbb{Z}/n\mathbb{Z}, \overline{+}, \overline{\cdot})$ は可換環になる.

☺ 略. $+$, $\cdot$ が可換環の性質を満たすことが成る. //

例 $\mathbb{Z}/24\mathbb{Z}$

$\overline{16} + \overline{10} = \overline{26} = \overline{2}$ $\qquad -\overline{10} = \overline{14}$

$\overline{6} \cdot \overline{7} = \overline{35} = \overline{11}$