群論 (第1回)

1. 群の定義と例

今回は群の定義と例についてみます. まずは演算の定義を復習しておきます.

定義 1-1(演算)

集合 G に対して, $G \times G$ から G への写像

$$G \times G \longrightarrow G \ \ ((x, y) \mapsto x * y)$$

を G 上の**演算**という.

例えば, 複素数体 $\mathbb{C}$ で通常の足し算や掛け算は $\mathbb{C}$ 上の演算になります.

定義 1-2 (群)

集合 G とその演算の組 $(G, *)$ が次の (1)-(3) を満たすとき, G を**群**と言い, さらに (4) も満たすとき**アーベル群**と言う.

(1) 任意の $a, b, c \in G$ に対して, $(a * b) * c = a * (b * c)$ が成り立つ. **(結合法則)**

(2) 次を満たす $e \in G$ が存在する: $a * e = e * a = a \ \ (\forall a \in G)$. **(単位元の存在)**

(3) 任意の $x \in G$ に対して, $x * y = y * x = e$ を満たす $y \in G$ が存在する. **(逆元の存在)**

(4) 任意の $x, y \in G$ に対して, $x * y = y * x$ が成り立つ. **(可換性)**

※1 (2) の性質を満たす e を G の**単位元**と呼び, e, 1_G (演算が乗法の場合), 0_G (演算が加法の場合) などの記号で表す.

※2 (3) の性質を満たす y を x **の逆元**と呼び, x^{-1} (演算が乗法の場合), $-x$ (演算が加法の場合) などの記号で表す.

[補足]

群 G に対して単位元は唯一つである. 実際, e_1, e_2 が共に G の単位元とする. e_1 が単位元より $e_2 = e_1 * e_2$ であり, e_2 も単位元より $e_1 = e_1 * e_2$ が成り立つ. よって $e_1 = e_2$ となる.

問題 1-1 群 G と $x \in G$ を考える．このとき, x の逆元は唯一つであることを示せ．

整数全体 $\mathbb{Z}$ が足し算に関して群をなすことを確認しておきます．

例 1-1

$(\mathbb{Z}, +)$ はアーベル群である．ただし, $+$ は整数の通常の足し算とする．$\mathbb{Z}$ の単位元は 0 であり, 整数 x の逆元は $-x$ である．

[証明]

定義 1-2 の (1)-(4) を確かめる．

(1) 任意の $x, y, z \in \mathbb{Z}$ に対して $x + (y + z) = (x + y) + z$. 従って $\mathbb{Z}$ は結合法則を満たす．

(2) 任意の $x \in \mathbb{Z}$ に対して $x + 0 = 0 + x = x$. 従って 0 は $\mathbb{Z}$ の単位元である．

(3) 任意の $x \in \mathbb{Z}$ に対して $x + (-x) = (-x) + x = 0$. 従って $-x$ は x の逆元である．

(4) 任意の $x, y \in \mathbb{Z}$ に対して $x + y = y + x$. 従って $\mathbb{Z}$ は可換性を満たす．

以上から $\mathbb{Z}$ はアーベル群である．

□

問題 1-2 演算 $\cdot$ は $\mathbb{C}$ の通常の掛け算とする．また $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ と置く．

(1) $(\mathbb{C}^\times, \cdot)$ はアーベル群であることを確認せよ．

(2) $(\mathbb{C}, \cdot)$ は群でないことを示せ．

問題 1-3 $\mathbb{C}$ 上の 2 次正則行列全体

$$GL_2(\mathbb{C}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{C},\ \det A \neq 0 \right\}$$

は行列の積を演算として群になることを示せ．また, アーベル群ではないことを確認せよ．

今度は少し変わった群を考えます．平方数ではない正の整数 m に対して,

$$x^2 - my^2 = 1$$

のタイプの方程式をペル方程式と言います．ペル方程式の整数解には群構造が入ります．

例 1-2

平方数ではない正の整数 m に対して, 集合

$$G = \{(x, y) \in \mathbb{Z}^2 \mid x^2 - my^2 = 1\}$$

を考える. また G 上の演算 $*$ を次で定める.

$$(a_1, b_1) * (a_2, b_2) = (a_1 a_2 + m b_1 b_2, a_1 b_2 + b_1 a_2).$$

このとき, $(G, *)$ は群になる.

[**証明**]

($*$ の well-defined 性)

まずは

$$(a_1, b_1), (a_2, b_2) \in G \Rightarrow (a_1, b_1) * (a_2, b_2) \in G$$

を確認しておく. $(a_1, b_1), (a_2, b_2) \in G$ とすると, $a_1^2 - mb_1^2 = a_2^2 - mb_2^2 = 1$. 従って

$$(a_1 a_2 + m b_1 b_2)^2 - m(a_1 b_2 + b_1 a_2)^2 = (a_1^2 - mb_1^2)(a_2^2 - mb_2^2) = 1.$$

よって, $(a_1, b_2) * (a_2, b_2) \in G$.

(G が群であること)

(1) $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$ に対して,

$$\begin{aligned}
& (a_1, b_1) * ((a_2, b_2) * (a_3, b_3)) \\
= \ & (a_1, b_1) * (a_2 a_3 + m b_2 b_3, a_2 b_3 + b_2 a_3) \\
= \ & (a_1 a_2 a_3 + m a_1 b_2 b_3 + m b_1 a_2 b_3 + m b_1 b_2 a_3,\ a_1 a_2 b_3 + a_1 b_2 a_3 + b_1 a_2 a_3 + m b_1 b_2 b_3),
\end{aligned}$$

$$\begin{aligned}
& ((a_1, b_1) * (a_2, b_2)) * (a_3, b_3) \\
= \ & (a_1 a_2 + m b_1 b_2, a_1 b_2 + b_1 a_2) * (a_3, b_3) \\
= \ & (a_1 a_2 a_3 + m b_1 b_2 a_3 + m a_1 b_2 b_3 + m b_1 a_2 b_3,\ a_1 a_2 b_3 + m b_1 b_2 b_3 + a_1 b_2 a_3 + b_1 a_2 a_3).
\end{aligned}$$

上の 2 式を比較すると,

$$(a_1, b_1) * ((a_2, b_2) * (a_3, b_3)) = ((a_1, b_1) * (a_2, b_2)) * (a_3, b_3).$$

従って G は結合法則を満たす.

(2) $(1, 0) \in G$ であり, さらに $(a, b) \in G$ に対して,

$$\begin{aligned}
(1, 0) * (a, b) &= (1 \cdot a + m \cdot b \cdot 0, 1 \cdot b + a \cdot 0) = (a, b), \\
(a, b) * (1, 0) &= (a \cdot 1 + m \cdot b \cdot 0, a \cdot 0 + 1 \cdot b) = (a, b).
\end{aligned}$$

よって, $(1, 0)$ は G の単位元.

(3) $(a,b)\in G$ を取る. $a^2-m(-b)^2=a^2-mb^2=1$ より $(a,-b)\in G$ であり,

$$\begin{aligned}(a,b)*(a,-b) &= (a^2-mb^2,-ab+ba)=(1,0).\\ (a,-b)*(a,-b) &= (a^2-mb^2,-ab+ba)=(1,0).\end{aligned}$$

よって, $(a,-b)$ は (a,b) の逆元である.

以上 (1)-(3) より G は群である.

□

問題 1-4　集合 $G=\{(a,b)\in\mathbb{R}^2 \mid a\neq 0\}$ に対して演算 $*$ を次で定める.

$$(a,b)*(c,d)=(ac,bc+d).$$

このとき, $(G,*)$ は群になることを示せ.

定理 1-1(指数法則)

G を群とする. $x\in G$ と整数 n に対して x^n を次で定義する.

$$x^n=\begin{cases}\underbrace{x*\cdots*x}_{n\text{ 個}} & n>0 \text{ のとき},\\ 1_G & n=0 \text{ のとき},\\ \underbrace{x^{-1}*\cdots*x^{-1}}_{|n|\text{ 個}} & n<0 \text{ のとき}.\end{cases}$$

このとき, 次が成り立つ.

(1) $x\in G$, $n,m\in\mathbb{Z}$ に対して, $x^{n+m}=x^n*x^m$.

(2) $x\in G$, $n,m\in\mathbb{Z}$ に対して, $x^{nm}=(x^n)^m$.

[証明]

文献 [1] の 2 章 定理 2-5 を参照のこと.

□

問題 1-5　問題 1-4 の群 $(G,*)$ を考える. 整数 n に対して, $(1,1)^n$ を計算せよ.

参考文献

[1] 木村哲三, 新妻弘, 「群・環・体入門」, 共立出版.