群の定義
Defenition of Group

定義 1 次の 0.∼3. を満たす集合 G を，演算 $\cdot$ について**群 (group)** をなすという．

0. G は演算 $\cdot$ について閉じて (closed) いる．[*1]
1. $\forall a, b, c \in G$ について
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$
が成り立つ．これを**結合法則 (associativity)** という．
2. $\forall a \in G$ について
$$a \cdot e = e \cdot a = a$$
となる元 $e \in G$ が存在する．e を G の**単位元 (identity element)** という．[*2]
3. $\forall a \in G$ について
$$a \cdot b = b \cdot a = e$$
となる $b \in G$ が存在する．b を a の**逆元 (inverse element)** といい，a^{-1} で表す．

例 1 $\mathbb{N}$ は乗法 $\cdot$ について群をなさない．逆元が必ずしも存在しない．[*3]

例 2 $\mathbb{Z}$ は乗法 $\cdot$ について群ではない（$0 \in \mathbb{Z}$ の逆元が存在しない）．

例 3 正の実数全体の集合 $\mathbb{R}^+$ は乗法について群をなす．

例 4 実数全体の集合 $\mathbb{R}$ は加法について群をなす．

定義 2 群 G の演算 $\cdot$ について

4. $\forall a, b$ に対して，**交換法則 (commutativity)**
$$a \cdot b = b \cdot a$$
が成り立つならば，G を**可換群 (commutative group)** または**アーベル群 (abelian group**[*4]**)** という．

例 5 $G = \{1, -1\}$ は乗法について群である．

例 6 $G = \{1, -1, i, -i\}$ $\left(i = \sqrt{-1}\right)$ は乗法について群である．

以下，演算子を省略する．

定理 1 群 G において次のことが成り立つ．

[*1] 演算の結果が集合 G から出ないという意味で**閉じた**という．閉じた二項演算を**内部二項演算**ということもある．
[*2] e はドイツ語の Einheit(英語の unit) に由来する記号である．
[*3] このように自然数の集合などを $\mathbb{N}$ と板書体で表す流儀と，太字体 $\boldsymbol{N}$ で表す流儀と両方ある．本シリーズでは混用している．
[*4] 人名に由来する名称であるが，遍在するためしばしば小文字で始める．

1. 単位元 e は唯一 (unique) である．
2. $\forall a \in G$ について逆元 a^{-1} は唯一である．

1. ［証明］群 G において異なる二つの単位元が存在すると仮定する．その二つを e, e' とすると，

$$ee' = e$$

また

$$ee' = e'$$

でもある．つまり $e = e'$ となり，異なるという仮定と矛盾する．よって単位元は唯一である．

［証明おわり］

2. ［証明］a の逆元が異なる二つの元 b, c で表されるとすると，

$$ab = e$$

両辺の左から c をかけて

$$cab = ce$$

$$eb = ce$$

$$b = c$$

となり，異なるという仮定と矛盾する．よって a の逆元は唯一である．［証明おわり］

定理 2 群 G において次のことが成り立つ．

1. $e^{-1} = e$
2. $(ab)^{-1} = b^{-1}a^{-1}$
3. $(a^{-1})^{-1} = a$

1. ［証明］

$$ee = e$$

より e は e の逆元である．［証明おわり］

2. ［証明］

$$\begin{aligned}
(ab)(ab)^{-1} &= e \\
a\{b(ab)^{-1}\} &= e \\
a^{-1}a\{b(ab)^{-1}\} &= a^{-1}e \\
e\{b(ab)^{-1}\} &= a^{-1}e \\
b(ab)^{-1} &= a^{-1} \\
b^{-1}b(ab)^{-1} &= b^{-1}a^{-1} \\
\therefore (ab)^{-1} &= b^{-1}a^{-1}
\end{aligned}$$

［証明おわり］

3. $aa^{-1} = e$ であることは a^{-1} の逆元は a であることを表している．

$$\therefore (a^{-1})^{-1} = a$$

［証明おわり］

定理 3 群 G において次のことが成り立つ．

1. $ax = ay \Longrightarrow x = y$（**消去律**）
2. $\forall a, b \in G$ について $ax = b$ となる $x \in G$ が存在する．（**方程式の解の存在**）

1. ［証明］$ax = ay$ の両辺に左から a^{-1} をかけて

$$\begin{aligned} a^{-1}ax &= a^{-1}ay \\ ex &= ey \\ \therefore x &= y \end{aligned}$$

［証明おわり］

2. $aa^{-1}b = b \Longleftrightarrow a(a^{-1}b) = b$ つまり $ax = b$ となる x は必ず存在し，$x = a^{-1}b$ である． ［証明おわり］

群は集合と演算をセットにして考えるので，単に G と書く代わりに，$(G, \circ)$ のように演算記号を添えて表すこともある．

定義 3 群の要素（元）の個数を**位数 (order)** と呼ぶ．位数が有限である群を**有限群**と呼ぶ

参考文献

[1] 「ウィキペディア」<http://ja.wikipedia.org/wiki/>

[2] 石村園子『すぐわかる代数』（東京図書，2003 年）

[3] 長岡亮介『線形代数学』（放送大学教育振興会，2004 年）w￥＾