代数と幾何D（第3回・2007/10/10）

定義 (群，モノイド (=単位的半群)，半群)． 空でない集合 G 上に二項演算 $\circ$

$$G \times G \longrightarrow G, \quad (a,b) \longmapsto a \circ b$$

が定義され，3つの条件 (G1), (G2), (G3) を満たすとき $(G,\circ)$ を**群**, (G1), (G2) を満たすとき $(G,\circ)$ を**モノイド** (又は，**単位的半群**), (G1) のみを満たすとき $(G,\circ)$ を**半群**という．

(G1) **結合法則**　任意の $a,b,c \in G$ に対して，$(a\circ b)\circ c = a\circ(b\circ c)$ が成り立つ．
(G2) **単位元の存在**　ある $e \in G$ が存在して，任意の $a \in G$ に対して $a\circ e = e\circ a = a$ が成り立つ．
(G3) **逆元の存在**　任意の $a \in G$ に対して，ある $a' \in G$ が存在し，$a\circ a' = a'\circ a = e$ が成り立つ．

- 次の様にも表わせる：
  (G1) $\forall a,b,c \in G$ に対して，$(a\circ b)\circ c = a\circ(b\circ c)$,
  (G2) $\exists e \in G$ s.t. $a\circ e = e\circ a = a$ $(\forall a \in G)$,
  (G3) $\forall a \in G$ に対して，$\exists a' \in G$ s.t. $a\circ a' = a'\circ a = e$.
- (G2) は [$\forall a \in G$ に対して，$\exists e \in G$ s.t. $a\circ e = e\circ a = a$] とは論理的に異なる (なぜ？).

今後のルール(決まり・約束)

- 二項演算 $\circ$ が明確にされている場合には，群 $(G,\circ)$ を単に**群** G と書く．
- (定義から) 空集合は群とは言わない．
- 二項演算は通常 $a\circ b = a\cdot b = ab$ と乗法的に書く (一般には $a\circ b \neq b\circ a$).
- 群 G に対して，乗法 $(\cdot)$ による群 $(G,\cdot)$ か，加法 $(+)$ による群 $(G,+)$ かをはっきりさせたい時には，**乗法群** G，**加法群** G (又は，**加群** G) と言う (例えば，加法群 $\mathbb{Z}$ と言ったら，集合 $\mathbb{Z}$ を加法 $+$ について群 $(\mathbb{Z},+)$ とみなすいう意味).
- 加法群 $(G,+)$ に対しては，常に $a+b = b+a$ $(\forall a,b \in G)$ と約束する．
- (逆に) 可換群 $(G,\circ)$ が与えられたとき，演算 $\circ$ を $+$ と書くことにして，加法群 $(G,+)$ と呼ぶことがある (加法群 (加群) と可換群 (アーベル群) は同じ概念).
- 加法群 $(G,+)$ に対しては，単位元は 0，$a \in G$ に対する逆元は $-a$ と書く．
- 乗法群 $(G,\cdot)$ に対しては，単位元は 1（又は，1_G），$a \in G$ に対する逆元は a^{-1} と書く．
- 群 $(G,\circ)$ の集合としての位数 (元の数) を群 G の位数といい，$|G|$ 又は $\#G$ で表わす．
- 群 G に対し，$|G| < \infty$ のとき**有限群**，$|G| = \infty$ のとき**無限群**という．
- $G = \{1\}$ のとき，$(G,\cdot)$ はただ1つの元からなる群であり**自明群**と呼ぶ．
- 有限集合 $X = \{a_1,\ldots,a_n\}$ に二項演算 $\circ$ が与えられたとき，その演算結果を表にしたものを $(X,\circ)$ に対する演算表と言った（右図）．X に二項演算を1つ与える事と，演算表を1つ指定する事は同じことである．特に，G が群の時には，$(G,\circ)$ に対する演算表を**群表**という．

$\circ$	a_1	$\cdots$	a_j	$\cdots$
a_1	$a_1\circ a_1$		$\downarrow$	
$\vdots$			$\downarrow$	
a_i	$\longrightarrow$	$\longrightarrow$	$a_i\circ a_j$	
$\vdots$				

- 2つの有限群 G, G' が元の順番を適当に並べ変えた後，同じ形の群表を持つとき G と G' は同型と言い，$G \cong G'$ と書く．
- 群論では同型である群は同じものとみなす．逆に，集合として $G = G' = \{a_1,\ldots,a_n\}$ であっても，$(G,\circ)$ と $(G',\star)$ の群表が，元の順番をどう並べ替えても同じ形にならない場合 (演算の構造が異なる場合) には，群として異なるものとして区別する：$(G,\circ) \not\cong (G',\star)$.