群（group）

集合：A

A 上の２項演算：☆：$A \times A \to A$

１．☆は結合的（associative）

$\forall a, b, c \in A, (a ☆ b) ☆ c = a ☆ (b ☆ c)$

２．単位元 $e \in A$ が存在する

３．任意の $x \in A$ に対し逆元が存在する

↓

（A, ☆）を群とよぶ

群の例　$(Z_n, +)$

$Z_n = \{0, 1, \cdots, n-1\}$

＋：n の剰余和（addition modulo *n*）

は群をなす

群:(A, ☆)において

$$\forall x,y \in A, \quad x☆y = y☆x$$

の時, ☆は可換(commutative)とよび, (A, ☆) を可換群(commutative group)またはアーベル群(abelian group)とよぶ

例　整数の集合:Z, 加算:＋

1. ＋は結合的

$$\forall a, b, c \in Z, (a + b) + c = a + (b + c)$$

2. 単位元は $0 \in Z$

3. $x \in Z$ の逆元は $-x \in Z$

　ただし 0 の逆元は 0

4. ＋は可換

$$\forall a, b \in Z, a + b = b + a$$

したがって(Z,+)は可換群

剰余和における結合律

$Z_3 = \{0, 1, 2\}$

$(a + b) + c$

$$
= \begin{cases} a+b+c & a+b+c < 3 \\ a+b+c-3 & 3 \leqq a+b+c < 6 \\ a+b+c-6 & a+b+c \geqq 6 \end{cases}
$$

$a + (b + c)$

$$
= \begin{cases} a+b+c & a+b+c < 3 \\ a+b+c-3 & 3 \leqq a+b+c < 6 \\ a+b+c-6 & a+b+c \geqq 6 \end{cases}
$$

従って＋は結合的

同型写像

群$(G,\ ☆)$, $(G',\ \triangle)$において写像 $f\colon G\to G'$が存在し,

$$\forall a, b\in G,\quad f(a☆b) = f(a)\triangle f(b)$$

ならば f を G から G’への準同型写像（homomorphism）

とよび，G と G’は準同型である（homomorphic）とよぶ

語源：homo（同じ）morph（形態）ism（作用）

とくに f が全単射であるとき f を同型写像（isomorphism），

G と G’は同型である（isomorphic）といい $G\cong G'$ と書く

語源：iso（同じ）

補足説明

・同型な群同士は記号の付け方を変えたものに過ぎない

・群は自動的に半群およびモノイドでもあるので同型の定義はそれらの代数系においても定義できる

$(A, ☆)$, $(B, △)$の単位元をそれぞれ e_A, e_B とする

$$f(e_A)△f(e_A) = f(e_A ☆ e_A) = f(e_A)$$

両辺に $f(e_A)$の逆元$(f(e_A))^{-1}$を左から作用させると

$$(f(e_A))^{-1}△(f(e_A)△f(e_A)) = (f(e_A))^{-1}△f(e_A)$$

結合律が成り立つので

$$((f(e_A))^{-1}△f(e_A))△f(e_A) = e_B$$

$$f(e_A) = e_B$$

を得る

$\forall a \in A,\ f(a^{-1})△f(a)= f(a^{-1} ☆ a)=f(e_A)= e_B$

同様に $f(a)△f(a^{-1}) = e_B$ を得る. よって$(f(a))^{-1}= f(a^{-1})$

巡回群(cyclic group)

e:単位元, α :生成元(generator), ☆:2 項演算子

$$e \ ☆ \alpha = \alpha$$

$$\alpha ☆ \alpha = \alpha^{2}$$

$$\alpha^{2} \ ☆ \alpha = \alpha^{3}$$

一般に

$$\alpha^{k} \ ☆ \ \alpha = \alpha^{k+1} \quad k=0,1,2,\cdots$$

ただし $\alpha^{0} = e$

$$C_n=\{\alpha^{0}, \ \alpha, \ \alpha^{2}, \ \cdots, \ \alpha^{n-1}\}$$

とすると(C_n , ☆) を巡回群とよぶ

$C_n=\{ \ \alpha^{0}, \ \alpha, \ \alpha^{2}, \ \cdots, \ \alpha^{n-1}\}$

の各要素 α^{k} に「☆ α 」を作用させる

$\{\alpha, \ \alpha^{2}, \ \alpha^{3}, \ \cdots, \ \alpha^{n}\}$

$=C_n$

となるはずなので

$$\alpha^{0} \ = \ \alpha^{n}$$

(C_n , ∘) は(Z_n, +)と対応する(n の剰余和)

対称群（symmetric group）

$A = \{1, 2, \cdots, n\}$上の全単射写像を n 次の置換（permutation of deree n）とよぶ

n 次の置換は写像の合成に関して群を成す

↓

n 次の対称群（symmetric group of degree n）：S_n

部分群（subgroup）

群(G,☆)に対して H⊆G，H≠ ϕを考える

（H,☆）が群となるとき，（H,☆）を(G,☆)の部分群とよぶ．
簡略化して「H は G の部分群である」という

自明な（trivial）部分群

G⊆G なので（G,☆）は(G,☆)の部分群
{e}⊆G なので（{e},☆）は(G,☆)の部分群
自明な部分群以外の部分群を真の（proper）部分群とよぶ

H が G の部分群であるための必要十分条件は

(1)　$a, b \in H \Rightarrow a☆b \in H$

(2)　$a \in H \Rightarrow a^{-1} \in H$

がともに成り立つことである
(1), (2)より $a☆a^{-1} = e \in H$
となり，e∈H が保証される