代数学Ｉ補充テキスト２（２００９年６月）

1　群の同型写像

G, H を群とする．写像

$$f\colon G \longrightarrow H$$

が**（群の）同型写像** (isomorphism) であるとは

1. f は１対１かつ上への写像である．
2. $f(g_1g_2) = f(g_1)f(g_2), \quad g_1, g_2 \in G$

という２条件を満たすことである．このとき必然的に

$$f(e_G) = e_H \qquad (e_G,\ e_H \text{ はそれぞれ } G,\ H \text{ の単位元 }),$$

$$f(g^{-1}) = f(g)^{-1}, \qquad g \in G$$

が成り立つ．（証明は教科書 16 ページにあるが, 自分でも試みよ．）群 G, H の間に同型写像 f があるとき, G, H は**（群として）同型** (isomorphic as groups) であるといい, 記号で

$$G \cong H$$

とかく．このとき $H \cong G$ である．（$f\colon G \longrightarrow H$ が同型写像のとき, 逆写像 $f^{-1}\colon H \longrightarrow G$ も同型写像だから．）さらに G_1, G_2, G_3 が群で $G_1 \cong G_2$, $G_2 \cong G_3$ のとき $G_1 \cong G_3$ である．（$f_1\colon G_1 \longrightarrow G_2$, $f_2\colon G_2 \longrightarrow G_3$ がともに同型写像のとき, 合成写像 $f_2 \circ f_1\colon G_1 \longrightarrow G_3$ も同型写像だから．）

注意 同型な群は, 群としてのすべての性質が同じである．このため同型な群は「実質的に同一の群」とみなされることが多い．

群の同型のことをよりよく理解するには, **群表**（group table）を考えればよい．（最近の教科書だと書いてないことが多いのは残念である．）

これは、掛け算の「九九の表」に相当する．ある１つの群を考えるということは「何か新しい掛け算を考える」ということだから, その掛け算の「九九の表」のようなものを作ってみようというのは自然な発想である．

群 G の位数が n のとき, $(n+1) \times (n+1)$ の表を用意して, $(1,1)$ のマス目（左上のマス目）

は空白のままにして, その後, 1 行目に群 G の元を横一列に記入していく. 1 列目も同様で, G の元を縦一列に記入する. 元を記入する順序はとくに決まっていないし, 縦と横で元の順序が違っていても構わない. 次に, 残りの $n \times n$ 個のマス目にも記入していく. まず, (2,2) のマス目には (2,1) に書いてある元 x と (1,2) に書いてある元 y の積 xy を記入する. 一般に (m, n) のマス目（上から m 番目, 左から n 番目のマス目, $m, n \geq 2$）には $(m, 1)$(第 1 列の上から m 番目）に書いてある元 s と $(1, n)$（第 1 行の左から n 番目）に書いてある元 t の積 st を記入する. これで群表の完成である. 群の位数（群に含まれる元の個数）が無限だと, 現実には表は作れないかもしれないが, 工夫すれば何とかなる.

例 1 $G = \{1, -1\}$ とおくと, G は普通の掛け算について群になっている. この群の群表は

	1	-1
1	1	-1
-1	-1	1

(1)

となる. あるいは, $e = 1, a = -1$ とおいて

	e	a
e	e	a
a	a	e

(2)

としてもよい. 次に, $H =$ { 偶, 奇 } という集合を考えてみよう. 偶＝偶数, 奇＝奇数 のつもりである. このとき, 通常の加法を演算とすると

$$\text{偶} + \text{偶} = \text{偶}\ ,\ \text{偶} + \text{奇} = \text{奇}\ ,\ \text{奇} + \text{偶} = \text{奇}\ ,\ \text{奇} + \text{奇} = \text{偶}$$

となり, H は加法に関して群をなすことがわかる. (単位元は 偶 である. ）この群の群表は

	偶	奇
偶	偶	奇
奇	奇	偶

(3)

となる. (1) と (2) については, 単に記号を書き換えただけだから, $1 \longrightarrow e,\ -1 \longrightarrow a$ と置き換えれば, 表 (1) が表 (2) に 移るのは当たり前だが, (2) と (3) の間でも $e \longrightarrow$ 偶, $a \longrightarrow$ 奇 と置き換えれば表（2）が表（3）に移るのが分かる. このようなとき, 2 つの群 G と H は同型であるといい, そのときの対応 $e \longrightarrow$ 偶, $a \longrightarrow$ 奇 のことを同型写像というのである. 前ページにある同型写像の定義の 1 は, 群表の「縁」の部分（第 1 行と第 1 列）の記号の書き換えを意味し, 同型写像の定義の 2 は群表の「中身」の部分が上の書き換えをすればぴっ

たり一致しているということを言っているのである.
以下において, 群 G の元の個数（つまり G の位数）を $|G|$ で表すことにする.
例 2 $|G| = 1$ のとき, G は単位元のみからなる. よって, $|G| = 1$ であるよう群は すべて同型 である. 下線部のことを「同型を除いて, ただ一つ (unique up to isomorphisms)」または「同型類 (isomorphism class）はただ一つ」という. 群表が（記号の書き換えは別にすれば）ただ一種類しかないというのと同じことである.
例 3 無限巡回群は同型を除いて, ただ一つである.
（**証明**）G を無限巡回群とすると, $G = \{x^n \mid n \in \mathbb{Z}\}$ である. ただし, x の位数は ∞, つまり $x^n \neq e$ $(n = 1, 2, \ldots)$ とする. このとき $m, n \in \mathbb{Z}$ に対し $x^m x^n = x^{m+n}$ が成り立つ. また $m, n \in \mathbb{Z}$, $m \neq n$ に対し, 常に $x^m \neq x^n$ である. これを背理法で示そう. $m > n$ としてよい. (何故か？）$x^m = x^n$ と仮定する. 両辺の右から x^{-n} をかけると $x^{m-n} = e$ が得られるが, $m - n$ は 0 以上の整数であるから, これは x の位数が ∞ であることに矛盾する. よって $x^m \neq x^n$ であることが示された. よって, 無限巡回群の群表はただ一種類しかないことがわかる. つまり, 無限巡回群は同型を除いてただ一つである.
例 4 n を自然数とする. 位数 n の有限巡回群は同型を除いて, ただ一つである.
（**証明**）G を位数 n の有限巡回群とすると, $G = \{x^k \mid k = 0, 1, \ldots, n-1\}$ である. ただし, x の位数は n, つまり $x^k \neq e$ $(k = 1, 2, \ldots, n-1), x^n = e$ とする. このとき $0 \leq k, l \leq n-1$ に対し $x^k x^l = x^r$（r は $k + l$ を r で割った余り）が成り立つ. また $k \neq l$ なら $x^k \neq x^l$ である. これを背理法で示そう. $k > l$ としてよい. $x^k = x^l$ と仮定する. 両辺の右から x^{-l} をかけると $x^{k-l} = e$ が得られるが, $k - l$ は $n - 1$ 以下の自然数であるから, これは x の位数が n であることに矛盾する. よって $x^k \neq x^l$ であることが示された. 従って, 位数 n の巡回群の群表はただ一種類しかない. つまり, 位数 n の巡回群は同型を除いて, ただ一つである.
例 5 $|G| = p$ で p が素数のとき, G は（位数 p の）巡回群である.（よって, 例 3 により G は同型を除いて, ただ一つである.）
（**証明**）$x \in G$, $x \neq e$ とする. x の位数が ∞ とすると, $\{x, x^2, x^3, \ldots, x^n, \ldots\} \subset G$ となり, $\{x, x^2, x^3, \ldots, x^n, \ldots\}$ が無限集合なので $|G| = p < \infty$ に矛盾する. よって x の位数 n は自然数で $H = \{x^k \mid k = 0, 1, \ldots, n-1\}$ とおくと H は位数 n の巡回群である. H はまた G の部分群であるから, ラグランジュ (Lagrange）の定理（教科書１２ページ）より, n は $p = |G|$ の約数である. 今, p は素数と仮定しているから, $n = 1$ または $n = p$ である. また, $x \neq e$ としたことから $n \neq 1$ である. よって $n = p$, つまり $|H| = |G|$ となる. $H \subset G$ であるから $H = G$ となる. よって G は巡回群である.
例 6 $|G| = 4$ のとき, G の同型類は, ただ一つではない.
（**証明**）位数 4 の群で巡回群ではないものが存在することを示せばよい. xy 平面において a を x 軸に関する reflection（線対称移動), b を y 軸に関する reflection とし $G = \{e, a, b, ab\}$ とおくと, $a^2 = b^2 = e$, $ab = ba$ となり G は群となる. このとき G の元 a, b, ab の位数は 2 だが, 位数 4 の巡回群 $\{e, x, x^2, x^3\}$ には位数 2 の元は x^2 一つしかない. よって G は（位数は 4 だが）巡回群ではない. （[注意] G は長方形のシンメトリーの群になっている.）