第4章　一般の群

この章では群の一般概念を紹介する. この特別な場合として変換群がある. この一般的な設定で群の基本的な性質を議論し, 算術へ群を適用する.

4.1　群の一般概念

変換群の研究において, **運動**を扱うか, もっと一般に**変換**を扱うかは, あまり重要ではなかった. 重要なのは, 群 G の 4 つの**性質**である. これは, G の任意の元の組に対して定義される**合成**に課せられた必要条件である：

1. G に属する 2 つの運動の合成は, G に属する；
2. 運動の合成は結合法則をみたす；
3. G には恒等変換が含まれる. 恒等変換は, 任意の運動 f との合成が f に等しいという性質で特徴づけられる；
4. G の任意の運動に対して, その逆の運動は, G の元である.

集合 G の任意の 2 つの元に, G のある 1 つの元が対応するような演算が与えられていて, 先の 4 つの性質が成り立つとき, G は群となる. たとえば, 足し算を演算とする実数の集合 $(\mathbb{R}, +)$ はこの 4 つの性質をもつから, 群である. 1 章 (Problems 1, 7 など) で, いろいろな性質の元 (数, 点, ベクトル) や異なる演算 (和, 積) に関して, これらの性質が使われていたことに注意しよう. 問題 32 と 練習 67 が類似していることも注目すべきである. これらのことは, 群の概念が一般的な設定で述べられることを示している. それでは, 群の定義を一般的な設定で述べよう.

定義 13 集合 G は次の条件をみたすとき**群**とよばれる：

I. G の任意の元の順序づけられた組 (a, b) に対して, G の元 $a * b$ が決められている (この法則を**二項演算**あるいは単に**演算**という)；

II. 演算 $*$ は結合法則をみたす. すなわち, G の任意の 3 つの元 a, b, c に対して, 次の等式が成り立つ： $(a * b) * c = a * (b * c)$ ；

III. G に**単位元**が存在する. 単位元とは G の任意の元 a に対して, $a * e = e * a = a$ となる元 e である；

IV. G の任意の元 a に対して, $a * a' = a' * a = e$ となる**逆元** $a' \in G$ が存在する.

性質 I 〜 IV を**群の公理**という. 次のことに注意しよう：変換群の定義 (p. 57) は, 群の公理のうちの 2 つ (I と IV) だけで構成されているが, 任意の変換群はこの一般的な意味で群になる. 実際, 公理 II は, 変換の合成 (p. 51) に関してつねに成立する. また, 公理 III は, 公理 I, IV から導かれる. なぜならば, 変換の合成に関する単位元は, 恒等変換であるが, IV の e (恒等変換) は I より与えられた集合 G に属するからである.

練習 70. 変換の有限集合 G に対して, 公理 IV は公理 I–III から導かれることを証明せよ.

記号 $*$(アスタリスク), $'$(プライム) や言葉「単位元」,「逆元」の代わりに, いろいろな状況に合わせて他の記号や言葉が用いられる：

1. 変換群において, 群の演算 (合成) は小さいまる ($\circ$) で表され, 単位元は id (恒等変換) で表される. また, 逆元 f' の役割は, 逆変換 f^{-1} によって果たされる.

2. 足し算を演算とする数の群 (整数, 有理数, 実数, 複素数) において, 単位元は 0 (zero), 数 a の逆元は, 逆符合の数 $-a$ である (平面上の点を複素数と考えると, 単位元は**極**とよばれ, P と表される).

3. 積を演算とする数の群 (たとえば, 正の数全体の集合など) において, 演算の印は通常省略される. すなわち, $a * b$ の代わりに ab と書く. 単位元は 1, また, a の逆元は a^{-1} である.

数やベクトルなどのような足し算を演算とする群を**加群**という. 積を演算とする群を**積の群**という.

数の積に対してとり入れられた記号は大変便利なので, どのような群に対してもよく使われる. ここでも, その記号を用いることにする. 気をつけなければならないことは, 数の積とは違って, 群の積は一般に可換ではないことである. すなわち, ab と ba は, その群の等しい元とは限らない.

問題 33 次の集合は群をなすか.

1) 足し算を演算とする偶数全体；

2) 足し算を演算とする奇数全体；

3) 引き算を演算とする実数全体；

4) 足し算を演算とする自然数全体；

5) 足し算を演算とする負でない整数全体；

6) $x * y = x + y - 1$ を演算とする実数全体.

解答. 1) 明らかに群の公理をみたす. 2) 公理 I をみたさない. つまり, 2つの奇数の和は奇数ではない. 3) 公理 I は成立するが, 公理 II は成立しない. なぜならば, 引き算は結合法則をみたさないからである. たとえば, $(6-5)-3 \neq 6-(5-3)$. 4) 公理 I, II はみたされているが, この演算に関する単位元は存在しない. つまり, 足し算に関して, 単位元の役割を果たす元は 0 だけであるが 0 は与えられた集合に含まれない. 5) 4) と比べると, 数 0 が集合の元であるという点で異なる. そこで, 単位元は存在する. しかし, 公理 IV はみたされない. なぜならば, 正の整数に対する逆元が存在しないからである. 6) この例は, もっと注意が必要である. 群の公理すべてを1つ1つチェックしよう. 任意の実数の組 (x, y) に対して, $x+y-1$ はまた実数であるから, 公理 I は成立する. 結合法則が成立するか確かめるためには, $*$ の定義を用いて2つの表示 $(x*y)*z$ と $x*(y*z)$ を計算しなければならない. 次のようになる：

$$\begin{aligned}(x*y)*z &= (x+y-1)*z = x+y-1+z-1 = x+y+z-2,\\ x*(y*z) &= x*(y+z-1) = x+y+z-1-1 = x+y+z-2.\end{aligned}$$

したがって, 公理 II はみたされる. 単位元 e は, 恒等式 $x+e-1=e$ (x は任意の元) をみたさなければならない. ゆえに, $e=1$. よって公理 III がみたされる. 最後に, 公理 IV を考える. 演算 $*$ は可換であるから, 1つの等式 $x*x'=1$ だけを考えればよい. したがって, $x+x'-1=1$ より, $x'=2-x$ である. よって, 公理 IV をみたす. このように, 公理 $I \sim IV$ が成立するから, 集合 $(\mathbb{R}, *)$ は群をなす.

練習 71. 次の集合が群をなすかどうかを調べよ. 群をなさない場合は, 公理 I ～ IV のうちのどの公理が成立しないかを示せ：

(1) 足し算を演算とする無理数全体の集合；

(2) $x*y=xy-x-y+2$ を演算とする $x>2$ なる実数全体の集合；

(3) 足し算を演算とする 2 進数の有理数 (分母が 2 の累乗である分数) の集合；

(4) 積を演算とする 0 でない 2 進数の有理数全体；

(5) 演算 $x*y=(x+y)/(1-xy)$ に関して, 群をなす実数の集合をつくることはできるか.

群の公理から簡単に導かれる性質で重要なものを述べておく.

1. 群における単位元は一意的である. すなわち, 群の公理 III をみたす元 e は1つしかない. 実際, 群 G の2つの元 e_1, e_2 が, 任意の元 $a \in G$ に対して次をみたすとする：

$$ae_1 = e_1a = ae_2 = e_2a = a$$

この式に $a=e_1, a=e_2$ を代入すると, $e_1 = e_1e_2 = e_2$ となるからである.

2. G の任意の元 a, b に対して, 方程式 $ax = b$ は, 一意的に可解である. これは, $ax = b$ であるような G の元 x がただ 1 つ存在するということである. 実際, 群の公理 II(結合法則) と IV(逆元の存在) を用いて, 与えられた等式の両辺に左から a^{-1} をかけると, $x = a^{-1}b$ となる.

   練習 72. 方程式 $xa = b$ の解を求めよ. また, その解が一意的であることを証明せよ.

3. 練習 73 の主張は次のことを意味する：
   - 与えられた元 $a \in G$ の逆元は一意的である.
   - 群の積表における任意の横列や縦列には, その群の任意の元が必ず 1 回だけ現れる. この事実の 1 つは, 等式 $ax = b$ の一意的な可解性から, もう 1 つは等式 $xa = b$ の一意的な可解性から導かれる.

4. $a \in G$ に対して, $(a^{-1})^n = (a^n)^{-1}$ が成り立つ. このように, 変換群の場合と同様に, $a^0 = e$, $a^{-n} = (a^{-1})^n$ $(n > 0)$ とおくと, 与えられた元の 0 乗や, 負の累乗を定義することができる. したがって, 任意の整数 k, l に対して,

$$a^k a^l = a^{k+l} \tag{4.1}$$

   が成り立つ.

5. 最後の関係式は, a の整数乗すべての集合が群をなすことを意味する. このような群を**巡回群**といい, a をその巡回群の**生成元**という. a の**位数**とは, $a^n = e$ となる最小の正整数 n である ($a = e$ ならば, その位数は 1 である； 任意の $n > 0$ に対して, $a^n \neq e$ ならば, a の位数は**無限である**という). a によって生成される群の位数 (元の数) は, a の位数に等しいことに注意しよう.

6. 結合法則の公理は, 2 つの積を含む群の 3 つの元の積が, 積の計算順序に依らないことを意味する. 帰納法により, この性質は, いくつの積に対しても正しくなる. すなわち, 積 $a_1a_2 \cdots a_n$ のなかに, どのように ( ) をつけても, 同じ結果になる. たとえば, $(a_1(a_2a_3))a_4 = ((a_1a_2)a_3)a_4 = (a_1a_2)(a_3a_4) = a_1(a_2(a_3a_4)) = a_1((a_2a_3)a_4)$.

さてこれまで, 変換 (変換群), あるいは数 (数の群) のどちらかを扱ってきた. 今度は, それらとはかなり異なる性質をもつ群の例をみていこう.

問題 34 図 *4.1* のように, *3* つの入力口と *3* つの出力口がある電気回路がある. それは, 任意の入力口が, ある出力口に対応するようにワイヤーでつながれている. このような電気回路を **3-switch** とよぶことにする. *3-switch* の総数は 6 であり, すべての *3-switch* は, 図 *4.1* に示されているものとする. このとき, *3-switch* の集合を群にする自然な演算を定義せよ.

解答. スイッチの集合上の自然な演算は**縦列接続**である. **2 つのスイッチ** P, P' **を縦列接続する**とは, P' の入力口と P の出力口をそれぞれつなげることである. たとえば, スイッチ P_2 とスイッチ P_4 を縦列接続すると, P_2 の入力口の数

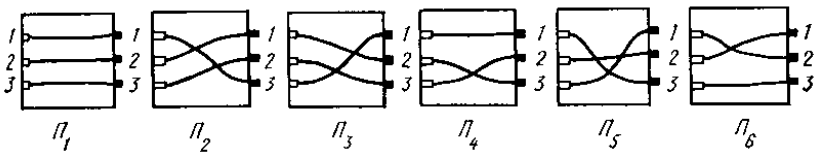


図 4.1: 3-switches

1 が P_4 の入力口の数 3 を通りぬけて, P_4 の出力口の数 2 に到達する. 結果として, 入力口の数 1 は出力口の数 2 につながることになる. 同じように, 入力口 2 は出力口 1 に, 入力口 3 は出力口 3 につながることになる. これはスイッチ P_6 と等しい. この意味で $P_2P_4 = P_6$ と書ける. この演算は可換ではない. $P_4P_2 = P_5$ であるからである.

次の表は, 3-swiches の集合における完全な積表 (厳密には, 縦列接続の表) である：

	Π_1	Π_2	Π_3	Π_4	Π_5	Π_6
Π_1	Π_1	Π_2	Π_3	Π_4	Π_5	Π_6
Π_2	Π_2	Π_3	Π_1	Π_6	Π_4	Π_5
Π_3	Π_3	Π_1	Π_2	Π_5	Π_6	Π_4
Π_4	Π_4	Π_5	Π_6	Π_1	Π_2	Π_3
Π_5	Π_5	Π_6	Π_4	Π_3	Π_1	Π_2
Π_6	Π_6	Π_4	Π_5	Π_2	Π_3	Π_1

この積表から, 3-switches の集合は群をなすことがわかる. しかし, どのようにしてこのことを証明したらよいか？ 群の公理をすべてチェックする方法では, 公理 II(結合法則) だけでも, $6^3 = 216$ 通りの等式をチェックしなければならない. しかし, 幸いにも, これらすべてをチェックしなくてもよい. スイッチの積表で, 文字 P_1, P_2, P_3, P_4, P_5, P_6 をそれぞれ, id, R, R^2, R_a, R_c, R_b で置き換えて, この表の最後の横列と最後の 2 つの縦列を交換すると, その表はまさに D_3 の積表となるからである. このことは, 3-switches の縦列接続に関する関係式と D_3 の合成に関する関係式が同じであることを意味する. したがって, 3-switches の集合における縦列接続という演算は, D_3 の変換における合成の性質をすべてもつことになる. すなわち, 3-switches の演算に関して結合法則が成り立ち, 3-switches の集合には, 単位元 (ここでは, switch P_1) が存在し, 任意の swich に対してその逆元が存在することになる. よって, 3-switches の集合は, 縦列接続という演算に関して群をなす.

上記の例の数学的内容は, 集合 $\{1, 2, 3\}$ からそれ自身 $\{1, 2, 3\}$ への 1 対 1 写像, 別の言葉で言うと, この集合の**変換**をすべて記述したことにある.

集合 $\{1, 2, \cdots, n\}$ の変換は, n 個の元の**置換**または**位数 n の置換** といわれる. 1 が i_1, 2 が i_2, $\cdots$, n が i_n になる置換は, $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ と表される. 一般に, 位数 n の置換は, $n!$ 個あり, 群をなす. この群を S_n と表す.

さて, 与えられた位数の置換すべての集合に, 2 つの異なる群構造の導入方法がある. 1 つの方法は, ちょうど変換と同じように置換を扱う方法で, 置換 s_1 と s_2 の積 $s_1 s_2$ を写像の合成 $s_1 \circ s_2$ として定義する方法である. 合成 $s_1 \circ s_2$ は, 最初に変換 s_2 を施し, 次に変換 s_1 を施すものである. この定義より, 次を得る：

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

もう 1 つの定義の仕方は, s_1 を施してから, s_2 を施すものである. この具体例は, さきほどみた問題 34 における swich の縦列接続である.

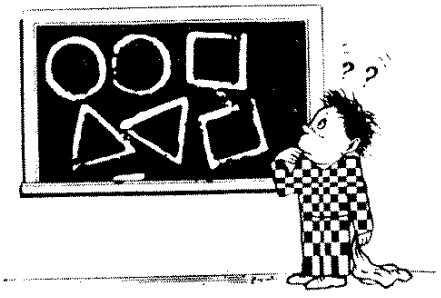
数学者には 2 つの流派があって, 置換の積を $s_1 \circ s_2$ と定義する流派と, $s_2 \circ s_1$ と定義するべきだとする流派とに分かれる. S_n の積表は, その積の定義の仕方により異なるが, 主対角線に関する対称変換によってうつり合うから, あまり見た目に違いはない. のちに, この 2 つの定義からそれぞれ導かれる置換群は, 実は**同型である**ことを説明する.

ここで, いくつかの問題をあげる. それらは異なる群ができる例である.

練習 73. 黒板にいくつかの円, 四角形, 三角形が描かれている. 次のルールで, そのなかの 2 つの図を消して, 1 つの図で置き換えることにする：

- 2 つの円 $\longrightarrow$1 つの三角形；
- 2 つの四角形 $\longrightarrow$ 2 つの三角形；
- 2 つの三角形 $\longrightarrow$ 1 つの四角形；
- 1 つの円と 1 つの四角形 $\longrightarrow$ 1 つの四角形；
- 1 つの円と 1 つの三角形 $\longrightarrow$ 1 つの三角形；
- 1 つの四角形と 1 つの三角形 $\longrightarrow$ 1 つの円.

このとき, 最後に残る絵は, 置き換えの順序によらず 1 つに決まることを証明せよ.



練習 74. A, B を, 1 変数の有理式, すなわち, 実数係数の x 変数多項式どうしの割算とする. このとき, **重ね合わせ** $A * B$ をつくることができる. $A_1 = 1 - x$, $A_2 = 1/x$ からつくられる重ね合わせの集合全体 Φ は, 群をなすことを証明せよ. また, その位数とすべての元を求め, 積表を作れ.

練習 75. 定数でない有理式 B で, $B * A_1 = B * A_2 = B$ をみたすものを求めよ. ただし, $A_1 = 1 - x, A_2 = 1/x$ とする.

4.2 同型

問題 34 を解くとき, 2 つの演算 (縦列接続と変換の合成) が同じ内部構造であることから, 縦列接続の性質を変換の合成の性質から推測した. このような状態を特徴づけるのにちょうど良い概念が, 同型である.

定義 14 群 G と群 H の元どうしの間に, $g_1 \leftrightarrow h_1, g_2 \leftrightarrow h_2$ ならば, $g_1 g_2 \leftrightarrow h_1 h_2$ となるような *1* 対 *1* 対応 ($\leftrightarrow$ と表す) が存在するとき, G と H は**同型である**という. また, この対応は, *2* つの群の演算に**一致している**という.

同型の定義をもっと正確に述べると, 次のようになる：G の任意の元 g_1, g_2 に対して, 次のような 1 対 1 対応 $\varphi : G \to H$ が存在するとき, G と H は**同型である**という. すなわち, 次の式が成り立つ：

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)(for\ \forall g_1, g_2 \in G). \tag{4.2}$$

写像 φ を G から H への 1 対 1 上への**同型写像**という.

一見, 後者の定義は, 前者の定義と異なっているようにみえる. なぜならば, その 2 つの群は対称的に配置されていないからである. しかし, 実は, 2 つの群は平等な権利をもつ. なぜなら, φ が G から H への上への同型写像であるとすると, φ^{-1} は, H から G への上への同型写像になるからである. 実際, $h_1 = \varphi(g_1), h_2 = \varphi(g_2)$ とすると, (4.2) 式の両辺に φ^{-1} をかけることによって, $\varphi^{-1}(h_1)\varphi^{-1}(h_2) = \varphi^{-1}(h_1 h_2)$ となる.

とくに, 有限群において, 同型写像を作る一番直接的な方法は, 対応する元の組をすべてはっきりと示すことである. そして, 元を対応する元で置き換えてできた表が, もう一方の群の積表になっているかどうかを確認する. もちろん, 与えられた表と, 二番目の群の積表とを厳密に一致させるためには, 横列と縦列を交換する必要があるかもしれない. 問題 34 では, この手続きをとった.

練習 76. 3-swiches の群と正三角形の対称群 D_3 の元どうしの間の次の対応は, 同型であるかを確かめよ: $id \leftrightarrow P_1$, $R_2 \leftrightarrow P_2$, $R \leftrightarrow P_3$, $S_b \leftrightarrow P_4$, $S_c \leftrightarrow P_5$, $S_a \leftrightarrow P_6$.

練習 77 は次の重要な結果を導く：

『群 G と群 H が同型であるとき, 同型写像 $\phi : G \to H$ は一般に一意的ではない. とくに, 群からそれ自身への, 恒等写像以外の同型写像が存在する.』

練習 77.　D_3 から D_3 への同型写像をすべて求めよ.

熱心な読者は, いままでにでてきた群どうしに類似した性質があることに気づいただろう. この類似性を明確な問題として述べてみよう.

練習 78.　固定された極上 (p. 9 参照) の足し算を演算とする平面上の点全体の集合は, 平面ベクトルの加群に同型な群を形成することを証明せよ. また, 点 (またはベクトル) にある座標系の座標点を対応させると, 次に定義された演算をもつ実数の組に同型であることを証明せよ：

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

練習 79.　問題 7 (p. 20) で述べられた積に関して正六角形の頂点の集合は, C_6 に同型な巡回群をなすことを証明せよ. ただし, C_6 は, 1 点を中心とする $60°n$ の回転の群である.

練習 80.　練習 74 で定義された演算に関して, 集合 { 円, 三角形, 四角形 } は巡回群 C_3 と同型であることを証明せよ. この 2 つの群の間に, 異なる同型写像はいくつあるか.

練習 81.　練習 74 で定義された有理式の群は, 二面体群 D_3 と同型であることを証明せよ.

練習 80, 81 の結果は, 次のように一般化される：

『同じ位数の巡回群は同型である.』

事実, G と H を同じ位数の巡回群とし, g, h をそれぞれ G, H の生成元とすると, 写像 $\varphi : G \to H$ を $\varphi(g^k) = h^k$ と定義することによって, 指数積の法則 (4.1) がどちらの群においても成立するから, 次のように φ は同型写像であることがわかる：

$$\varphi(g^k g^l) = \varphi(g^{k+l}) = h^{k+l} = h^k h^l = \varphi(g^k)\varphi(g^l).$$

さらに, 巡回群と同型な群は巡回群である. なぜならば, 同型写像によって生成元をうつすと, また生成元になるからである.

もし, ある群の内部構造に興味があるなら, その群の元の性質は忘れて, その演算の性質だけに注意すればよい.

定義 15　抽象群とは, 同型な群全体の集合族である.

たとえば, 回転群 C_n あるいは 1 の複素 n 乗根のような, 位数 n の巡回群はすべて, 位数 n の同じ 1 つの抽象群の代表元, あるいは仏教の言葉で**化身**である. 同じように, 二面体群 D_3, 置換群 S_3, スイッチの群 (問題 34), 有理式の群 (練習 74) はすべて同じ 1 つの抽象群の代表元である. のちに, 与えられた構造 (生成元の関係式の集合) から抽象群をどのように定義すればよいかを説明する (p.101)

今度は, 次のような一般的な問題を考えよう：「2 つの群が同型かどうか決定せよ.」 ふつう, 2 つの群が同型であることを証明するほうが, 同型ではないことを証明するより骨

が折れる. なぜなら, 前者の場合, 通常, 同型写像を構成しなければならないが, 後者の場合は, 同型写像によって保存されなければならない性質の中で, この 2 つの群で異なるものをみつければ十分だからである. ここで, 2 つの群が同型であるための必要条件をいくつか述べよう：

1. **群の位数** 位数が異なる群は同型ではない.

   練習 82. 足し算を演算とする整数全体の群は, 足し算を演算とする奇数全体の群に同型か.

2. **可換性** 可換群は可換でない群に同型ではない.
3. **巡回性** 巡回群は巡回でない群に同型ではない.

   練習 83. 次のリストのなかで, 同型な群はどれとどれか：C_1, D_1, C_2, D_2, C_3, $D_3, \cdots$.

4. **元の位数** 一方の群における位数 n の元の個数は, もう一方の群における位数 n の元の個数に等しくなければならない. なぜならば, 同型写像によって対応している元の位数はそれぞれ等しいからである.

多少難かしそうな最後の「元の位数」についてのみ証明しよう.

まず注意してほしいのは, 同型写像においては, 群の単位元どうしが対応することである. 実際, e を G の単位元とし, $\varphi : G \to H$ を同型写像とすると, $ee = e$ より, $\varphi(ee) = \varphi(e)\varphi(e) = \varphi(e)$ である. ゆえに, $\varphi(e) = e'$. ここで, e' は H の単位元である. 次に, g を位数 n の G の元とする. すなわち $g^n = e$ である. よって, $\varphi(g^n) = \varphi(g)^n = e'$. つまり, $h = \varphi(g)$ の位数は n 以下である. 同じように逆関数を用いると, g の位数は h の位数以下であることがわかる. ゆえに, g と h の位数は等しい.

たとえば, C_6 と D_3 を区別するためには, 2, 3, 4 のどの基準を用いてもよい. 基準 2 については, C_6 は可換で D_3 は非可換である. 基準 3 については, C_6 は巡回群であるが, D_3 は巡回群ではない. 基準 4 については, C_6 においては, 位数 1 の元が 1 つ, 位数 2 の元が 1 つ, 位数 3 の元が 2 つ, 位数 6 の元が 2 つである. 一方, D_3 においては, 位数 1 の元が 1 つ, 位数 2 の元が 3 つ, 位数 3 の元が 2 つである.

2 つの群が同型になるための必要な性質は実質的には無数にある. なぜなら, その群の元の特別な性質以外にも, 群の演算に関して公式化される性質は無数にあるからだ. しかし, 基準 1-4 によって, 同型であるかないかの問題は, 半分以上解決できるだろう. さて, G と H を与えられた群とし, G と H を区別できる性質はみつけられないと仮定しよう. このとき, G と H は同型であると予想される. この予想を証明するのに, G と H の間の同型写像 $\varphi : G \to H$ を構成しなければならない. どのようにしてこの同型写像を構成すればよいか.

e, e' をそれぞれ G, H の単位元とすると, $\varphi(e) = e'$ であることをまず思いだしていただきたい. さらに, ある適当な元 $g \in G$, $h \in H$ に対して, $\varphi(g) = h$ となるとき, 等式 (4.2) を繰り返し適用することによって, 任意の自然数 k に対して $\varphi(g^k) = h^k$ であることが導かれる.

練習 84. 等式 $\varphi(g^k) = h^k$ $(k < 0)$ を証明せよ.

このように, 写像 φ による $g \in G$ の像が定義されているとき, φ は g によって生成される部分群全体で一意的に定義される. 同じように, **いくつかの元** $g_1, \cdots, g_n \in G$ の像がわかっていたら, $g_1, \cdots, g_n$ によって表現できる任意の元の像を一意的に決めることができる. もし, $g_1, \cdots, g_n$ が G の**生成元**であるならば, $\varphi(g_1) = h_1, \cdots, \varphi(g_n) = h_n$ は, φ を完全に決定することができる. 生成元が 2 個 (g_1 と g_2) の場合, φ は次のように決まる：

$$\varphi(g_1^{k_1} g_2^{l_1} \cdots g_1^{k_s} g_2^{l_s}) = h_1^{k_1} h_2^{l_1} \cdots h_1^{k_s} h_2^{l_s}. \tag{4.3}$$

したがって, G が g_1 と g_2 によって生成されるとき, 同型写像 $\varphi : G \to H$ を構成するには, $\varphi(g_1) = h_1$, $\varphi(g_2) = h_2$ を定義し, 関係式 4.3 を用いて φ による G のすべての元の像を定義すればよい. しかし, どのようにして h_1 と h_2 をえらべばよいか？ h_1 と h_2 は H の生成元で, それらの位数はそれぞれ g_1, g_2 の位数に等しくなければならない. また, g_1 と g_2 がみたす関係式をすべてみたさなければならない. たとえば, $g_1^2 g_2^3 = e$ であるとき, $h_1^2 h_2^3 = e'$ でなければならない. しかし, これらの主張からは, 同型写像 φ の候補者を推測できるだけである. だから, 写像 φ が作られたら, φ が本当に同型写像かどうか確かめなければならない.

問題 35 $e = \dfrac{-1}{2} + \dfrac{\sqrt{3}}{2i}$ ($e^3 = 1$ に注意), $F_1(z) = ez, F_2(z) = \bar{z}$ とする. このとき, F_1, F_2 を重ね合すことにより得られる関数すべての集合は, 二面体群 D_3 と同型な群をなすことを証明せよ.

解答. 次のことが得られる：

$$\begin{aligned}
F_3(z) &= F_1(F_2(z)) = F_1(\bar{z}) = e\bar{z}, \\
F_4(z) &= F_2(F_2(z)) = F_2(\bar{z}) = z, \\
F_5(z) &= F_1(F_1(z)) = F_1(ez) = e^2 z, \\
F_6(z) &= F_2(F_1(z)) = F_2(ez) = e\bar{z} = e^2\bar{z}.
\end{aligned}$$

容易に確かめられるように, これらの式に, さらに, F_1, F_2 をどのように重ね合わせたとしても, これらの関係式以外はでてこない. したがって, 6 つの関数 $F_1, \cdots F_6$ の集合は, 重ね合わせのもとで閉じている. このリストの任意の関数の逆関数もまた, このリストに属する. このことは, その集合が群をなすことを示している. 単位元は恒等写像 F_4 で, 関数 F_2, F_3, F_6 の位数は 2, 関数 F_1, F_5 の位数は 3 である. $F_1(F_2(z)) = F_3(z)$, $F_2(F_1(z) = F_6(z)$ より, この群は可換ではないことがわかる. これらのことを考えると, G は D_3 に同型らしいことが推測できる.

同型写像 $\varphi : G \to D_3$ を構成するとき, G は定義より, 2 つの生成元 F_1(位数 3), F_2(位数 2) をもつことに注意しよう. D_3 においても, 位数が 3 と 2 の 2 つの生成

元をみつけられる. それは, 回転と対称変換である. たとえば, $F_1 \leftrightarrow R$, $F_2 \leftrightarrow S_a$ (p. 67の記号を用いて) とする. このとき, $F_3 \leftrightarrow S_c$, $F_4 \leftrightarrow id$, $F_5 \leftrightarrow R^2$, $F_6 \leftrightarrow S_b$ である. D_3 の積表において, その対応する G の元で D_3 のすべての元を置き換えると, 次の表を得る：

	F_4	F_1	F_5	F_2	F_6	F_3
F_4	F_4	F_1	F_5	F_2	F_6	F_3
F_1	F_1	F_5	F_4	F_6	F_3	F_2
F_5	F_5	F_4	F_1	F_3	F_2	F_6
F_2	F_2	F_3	F_6	F_4	F_5	F_1
F_6	F_6	F_2	F_3	F_1	F_4	F_5
F_3	F_3	F_6	F_2	F_5	F_1	F_4

容易に確かめられるように, この表は G に対する積表である.

同型写像はこのようにして作られる. しかし, 問題の 2 つの群の間の同型写像をみつけるもっと自然な方法がある. 実は, 平面変換の解析的な表現である複素関数を思いだすとよい. とくに, 関数 $F_1(z) = ez$ は 0 の回りの 120° 回転に対応し, 関数 $F_2(z) = \bar{z}$ は, 実数軸 (図 4.2 の軸 a) に関する対称変換に対応している.

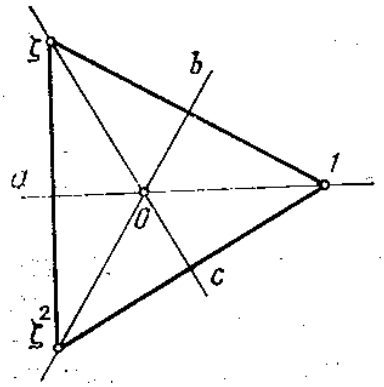


図 4.2: 複素数平面上の正三角形

よって, F_1, F_2 の重ね合わせによって得られる任意の関数に, 平面変換を対応させれば, 群の同型写像を得る.[1]

後者の方法で構成された同型写像を**自然な同型写像**という. 自然な同型写像は, 2 つの群がなぜ同型なのかを視覚的に示している.

練習 85. 次の 2 つの群の間の自然な同型写像を求めよ：

[1] 「重ね合わせ」と「合成」は実質的には同じ意味である. 「重ね合わせ」は解析における関数に対して用いられ, 「合成」は幾何における変換に対して用いられる.

(1) (問題 34)3-switches の群と D_3 ;
(2) 練習 76 における有理式の群と D_3.

いま述べている自然さとは, 決して厳密な数学的概念ではなく, むしろ, 発見を助ける性質の概念である. ある意味では, どのような同型写像も自然であるが, なぜそれが自然なのかを**理解するためには**, しばしば, 特別な数学の定理を展開しなければならない. 自然な同型写像を追求すれば, なぜ同じものが数学の異なる分野に現れてくるのかがわかるだろう. そうするは, 知識の発展を促進する強力な原動力となる.

同型の概念は, 数学のみならず, 思考するどのような分野においても重要であるからあえて「知識」という一般的な言葉を用いた. 「同型」の一般的な意味を理解するため, 次のような史上の例を考えてもらいたい.

1970 年に, モスクワにおける Gelfand の通信教育数学学校の入学試験に出題された問題のうちの 1 題は, 異なる形式で有名な雑誌社二社によって発表された. ある雑誌には, この問題は次のように記述された :

『M 市において, 3 人のギャング Archie, Boss, Wesley のうちの 1 人が, お金の入ったバッグを盗んだ. 彼らはそれぞれ 3 つの供述をした :

- Archie :
  - わたしは盗んでいない.
  - その日, わたしはその町にいなかった.
  - Wesley が盗んだにちがいない.
- Boss :
  - Wesley が盗んだのだと思う.
  - わたしが, そのバックを盗んだのなら, このように供述しない.
  - わたしはお金を沢山もっている.
- Wesle :
  - わたしは盗んでいない.
  - 上等のバックをずっと捜している.
  - Archie が, その日, この町にいなかったのは正しい.

その取り調べの間に, 3 人の供述のそれぞれのうち, 2 つは正しく, 1 つは誤りだということがわかった. では, 一体, 誰がバックを盗んだのだろうか ?』

別の雑誌では, 次のような問題を掲載した (問題のなかの名前は, ロシア民族の昔話によくでてくるものである) :

『王は, だれが冷酷な大蛇を殺したのかを知りたかった. 王は, 犯人が悪名高い 3 人 Ilya Muromets, Dobrynia Nikitich, Alyosha Popovich のうちの 1 人であることを知っていた. その 3 人は王に出頭を命ざれ, それぞれ 3 つの供述をした :

- I. M.：
  - わたしは大蛇を殺していない.
  - その日, わたしは海外に渡航中だった.
  - A. P. が殺したにちがいない.
- D. N.：
  - A. P.が殺したのだと思う.
  - わたしが殺したのなら, こんなふうに供述するはずがない.
  - 邪悪な精神がいまだに生きている.
- A. P.：
  - わたしは大蛇を殺していない.
  - すばらしい犯罪行為をしたいと思っている.
  - I. M. が, その日, 海外に行っていたのは本当である.

王は 3 人それぞれが本当のことを 2 度言い, 1 度だけうそを言っていることがわかった. それでは, 一体だれがその大蛇を殺したか？』

2 つの問題を比べてみると, あちこち異なる箇所があるが, 論理的な構造は同じであることがわかる. 次の表は, 2 つの問題における対応する名前, 物, 行為を表している：

Archie	Ilya Muromets
Boss	Dobrynia Nikitich
Wesley	Alyosha Popovich
bag	dragon
to steal	to kill
to leave the city	to go abroad

最初の問題の名前を, 上の表の右側のもので置き換えると, その問題は, 6 番目の供述以外は 2 番目の問題の文章とほぼ同じものになる. しかし, 実際には, 6 番目の供述は問題の答えに影響はないから, この意味で, この 2 つの問題は同型であるといえる.

この同型写像は次のように利用できる. 最初の問題が解けて, 答えが 'Boss' だとわかったら, 2 番目の問題を解く必要はない. なぜならば, 上の表において, Boss に対応する名前が, 正しい答えだからである. すなわち, 答えは 'Dobrynia Nikitich' である.

同じように, 群の同型写像を次のようにも利用できる. すなわち, G と H が同型であるとき, G の演算に関して成り立つすべての主張が H の演算でも成り立つ.

群の同型写像によるもっと簡単な応用例は, 元の積の計算である. もし, ある群において, 積の計算があまり難しくなく, 手間のかからないものであるとき, その積を用いて, 別の同型な群の元の積を計算することができる. もっと正確に言うと, $\varphi : G \to H$ が, 群 $(G, *)$ と群 $(H, \circ)$ との間の同型写像であるならば, 積 $*$ は, 次の式によって計算できる：

$$g_1 * g_2 = \varphi^{-1}(\varphi(g_1) \circ \varphi(g_2)). \tag{4.4}$$

図 4.3: 同型写像

この種の古典的な計算例は, J. Napier(17 世紀初頭) によって発見された**対数** [2]による計算である. 彼は, 数の積を簡単な演算–加法–で置き換えようとした. x の十進法の対数を $\log x$ と表すと, 次の等式が成り立つ：

$$x_1 x_2 = 10^{\lg x_1 + \lg x_2}. \tag{4.5}$$

この式は, 一般的な関係式 4.4 の具体的な例である. 対数をベースに計算できる同型写像の例は $\lg : (\mathbb{R}_+, \cdot) \to (\mathbb{R}, +)$ である (積の演算における正の実数の群から加法の演算における実数全体の群への上への写像). 対数関数の 2 つの基本的性質を述べておこう：

1. 集合 R_+ 上で定義される 1 対 1 写像である.
2. 恒等式
$$\log(x_1 x_2) = \log x_1 + \log x_2.$$
が成り立つ.

したがって, 対数関数は, 群 $(R_+, \cdot)$ と群 $(R, +)$ の間の同型写像である.

練習 86.　1. 十進法の対数 $y = \log x$ を **Napier 関数** $y = A \lg x + B$ で置き換えるとき, 4.5 式に代わる式を求めよ.
2. Napier 関数が, $(\mathbb{R}_+, \cdot)$ から $(\mathbb{R}, *)$ への上への同型写像となるよ うに演算 $*$ を求めよ.

練習 86 の 2 は, いわゆる**構造の変換写像**の具体的な例である. ここで, この意味を説明しよう.

G を $\triangle$ を演算とする群とし, H を演算がないただの集合とする. 1 対 1 写像 $\varphi : H \to G$ が与えられていると仮定すると, このとき, 次の式を用いて, φ **による** G **の演算から** H **の演算を求めることができる**：

$$h_1 \bigtriangledown h_2 = \varphi^{-1}(\varphi(h_1) \triangle \varphi(h_2)).$$

実際この方法を以前に使った：

- ベクトルの加法から点の加法を導くとき (1 章)；

[2]J. Napier による対数とは, ある定数 A, B をもつ関数 $y = A \log x + B$ である. 現在の意味の対数は, Napier の弟子 G.Briggs が導入した. また, 彼は常用対数表を作った.

- 実数上に, 群の演算を $x * y = x + y - 1$ と定義したとき (問題 33). この演算は, 写像 $\varphi(x) = x - 1$ によって, $\mathbb{R}$ から $\mathbb{R}$ へうつされるふつうの加法から得られる. なぜならば, $x * y = \varphi^{-1}(\varphi(x) + \varphi(y)) = (x-1) + (y-1) + 1 = x + y - 1$ だからである.

練習 71 の演算 $x * y = \dfrac{x+y}{1-xy}$ も同様に得られる. 写像 $\varphi(x) = \tan x$ を用いて, 群構造 $(\mathbb{R}, +)$ を変えようとした. しかし, この写像は 1 対 1 対応ではない. けれども, 加群でしかも M 上の点での正接の値がすべて異なる性質をもつ任意の集合 $M \in \mathbb{R}$ に対して, これらの値の集合は, 演算 $*$ に関して群をなす.

練習 87. 次のことを証明せよ：

1. このような集合 M として, π と素な実数 α の積全体の集合をとる ことができる；
2. この性質をもつ集合 M は, 実数軸のどのような開区間も含まない.

練習 88. 1. 写像 $y = x^3$ による加法の変換によって, 結果として, 実数上のどのような 演算となるか；
2. 演算 $x * y = xy - x - y + 2$(練習 71) は, どのようにして得られたか.

構造の変換関数の言葉で, 同型写像の概念は, 次のように述べられる：写像 φ によって, 群 G からうつされる群 H の演算が G の演算と一致するとき, 写像 $\varphi : G \to H$ を, G と H の**同型写像**という.

4.3 Lagrange の定理

この節では, 群論におけるまさにその最初の定理を述べ, 証明する. この定理はフランスの有名な数学者 Lagrange によって, 18 世紀末発見された. その後, さらに群の概念は E. Galois によって 19 世紀系統的に数学に導入された.

定理 7 (Lagrange) 有限群 G の任意の部分群の位数は, G の位数の約数である.

証明 群の任意の元は, その元の位数と等しい位数の巡回部分群を生成するから, とくに, **有限群の位数は任意の元の位数でつねに割り切れる**ことがわかる.

いままでにでてきた例 (群 C_{12}, D_3 など) で, すでにこの法則に気づいた人もいるかもしれない. 一般の設定で, Lagrange の定理を証明するためには, 群の部分群による**剰余類分解**を用いなければならない.

G を位数 n の群とし, H を位数 m の G の部分群とする： $H = \{h_1, h_2, \cdots, h_m\}$. 任意の部分群には単位元が存在するから, $h_1 = e$ と仮定する.

任意の元 $g \in G - H$ に対して, 次の集合を考える：

$$gH = \{gh_1, gh_2, \cdots, gh_m\}.$$

集合 gH を H **による** G **の左剰余類**という. gH には, 次の 2 つの性質がある：

1. $|gH| = |H|$.

2. $gH \cap g = \emptyset$.

1 の証明 $gh_1, \cdots, gh_m$ がすべて異なることを示さなければならないが, 実は $gh_i = gh_k$ ならば, 両辺に左から g^{-1} をかけることによって $h_i = h_k$ となるから, これは正しい.

2 の証明 $gH \cap H \neq \emptyset$ と仮定する. $h_i \in gH \cap H$ とすると, このときある元 $h_k \in H$ が存在し $h_i = gh_k$ となる. この式の両辺に右から h_k^{-1} をかけると, $g = h_i h_k^{-1}$ となる. よって, $g \in H$ となり, これは g のとり方 (定義) に矛盾する. ゆえに, $gH \cap H = \emptyset$.

性質 2 は, 次のように一般化される：

『 $g_1H \in G/H$, $g_2 \in G - g_1H$ **ならば**, $g_1H \cap g_2H = \emptyset$.』

言い換えると, 次のようになる.

『 **任意の** g_1H, $g_2H \in G/H$ **に対して**, $g_1H = g_2H$ **または** $g_1H \cap g_2H = \emptyset$ **のどちらかが成り立つ**.』

事実, $g_1H \cap g_2H \neq \emptyset$ とすると, ある元 h_i, $h_k \in H$ が存在し, $g_1h_i = g_2h_k$ となる. ゆえに, $g_2 = g_1h_ih_k^{-1}$. $h_ih_k^{-1} \in H$ より, これは $g_2 \in g_1H$ を意味する. よって, $g_2H \subset g_1H$ である. 同様のことが, g_1 に対しても成り立つから, $g_2H = g_1H$ であることがわかる.

さて, G を H による左剰余類に分解するプロセスを述べよう. $H = G$ ならば, その剰余類分解は, 1 つの集合 H だけからなる. そうでなければ, 元 $g_1 \notin G - H$ をえらび, 剰余類 g_1H を考える. $H \cup g_1H = G$ ならば, そのプロセスは終わりである. $H \cup g_1H \neq G$ ならば, $g_2 \in G - (H \cup g_1H)$ をえらぶ. このように, 3 つの対ごとに素な剰余類 H, g_1H, g_2H が得られる. G が有限群ならば, このプロセスは早かれ遅かれ終わり, 次のような分解を得る：

$$G = H \cup g_1H \cup g_2H \cdots g_kH.$$

ただし, $|H| = |g_iH| = m$, $g_iH \cap H = g_iH \cap g_jH = \emptyset$ $(i \neq j)$ である.

したがって, G の元の個数 n は, g_iH の元の個数 m で割り切れる. よって, 定理は証明された.　□

式 $G = H \cup g_1H \cup g_2H \cdots g_kH$ を G **の** H **による左剰余類分解**という.

右剰余類分解もまた, 左剰余類分解と同じように考えることができる. 一般に, これらの 2 つの分解は一致しない. このことについては, 次の章で述べよう.

図 4.4, 4.5 はそれぞれ, 位数 3 と 2 の部分群による D_3 の左剰余類分解を示している.

練習 89.　D_3 のすべての部分群を求めよ.

Lagrange の定理は, 次の重要な事柄を導く.

問題 36 素数位数の有限群は巡回群であることを証明せよ.

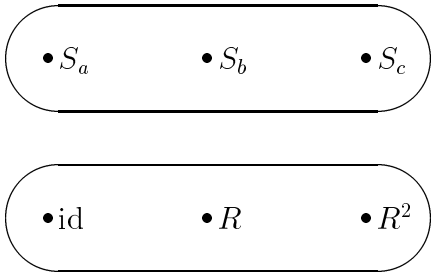


図 4.4: D_3 の剰余類分解その 1

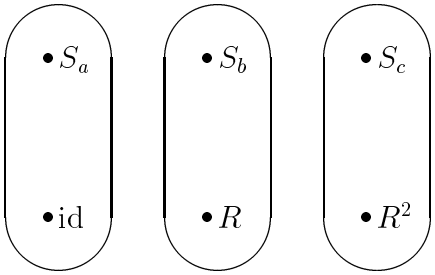


図 4.5: D_3 の剰余類分解その 2

解答. G を素数位数 p の群とし, g を単位元でない G の任意の元とする. g によって生成される G の部分群を H とすると, H の位数は, 少なくとも 2 である. なぜならば, H は, 単位元 e と g を含むからである. 素数 p の 1 より大きい約数は, p だけである. よって, H の位数は p で, $H = G$ である. このように, G は, 1 つの元 g で生成される.

問題 36 より, **素数位数の群は可換である**ことがわかる.

群の定理の応用をいくつか述べよう (とくに, Lagrange の定理を計算に用いる).

整数論でででてくる一番簡単な群は, 加法演算におけるすべての整数の集合 $\mathbb{Z}$ である. その群の演算は加法だから, ある元の累乗 (すなわち, 与えられた元をそれ自身にひき続き足して得られる元) の代わりに, その積を用いることにする. 任意の整数は, 1 との積 ($n = n \cdot 1$) で表されるから, $\mathbb{Z}$ は生成元が 1 の巡回群でもある.

練習 90. 群 $\mathbb{Z}$ に 1 以外の生成元は存在するか.

任意の群においてと同様に, $\mathbb{Z}$ においても, その任意の元 n は部分群を生成する. その部分群は n の倍数の集合で, $n\mathbb{Z}$ と表される.

練習 91. 群 $\mathbb{Z}$ の**任意の**部分群は, 適当な n で nZ と表されることを証明せよ.

練習の結果は, すでに数論においていろいろな場面に応用されている. 例として, 次の良く知られている事柄を証明しよう：

『a と b が, 互いに素な整数であるならば, ある整数 x と y が存在して, $ax+by=1$ となる.』

実際, H を a と b によって生成される $\mathbb{Z}$ の部分群とすると, 定義から, $H=\{ax+by|x,y\in\mathbb{Z}\}$ と書ける (演算として, 加法の代わりに可換積を用いると, H の元は a^xb^y と書ける). 練習 92 より, 自然数 n で, $H=n\mathbb{Z}$ となるものが存在する. H は, a と b を含むから, どちらも n で割り切れなければならない. しかし, a と b は, 互いに素な整数だから, 結局 $n=1$ でなければならない. よって, 数 1 は H に属し, ある適当な整数 x_1, x_2 で $ax_1+bx_2=1$ となるものが存在する.

さて, Lagrange の定理は, $\mathbb{Z}$ と $n\mathbb{Z}$ の組には適用できないことに注意しよう. なぜならば, $\mathbb{Z}$ と $n\mathbb{Z}$ は, どちらも無限群だからである. しかし, nZ による Z の剰余類分解をつくることは意味があり, 剰余類やモジュラ形式の算術という重要な概念を導く.

たとえば, $n=3$ とする. 部分群 $3\mathbb{Z}$(3 の倍数) のすべての元に 1 を足すと, この数の集まりは, 3 で割ると余りが 1 の集合になる. 同様に, 2 をそれぞれの元に加えると, 3 で割って余りが 2 の集合になる. 3 で割ると 1 と 2 以外の余りはないから, 整数全体の集合はこの 3 つの類に分類されることがわかる. これは $\mathbb{Z}$ **の** $3\mathbb{Z}$ **による剰余類分解**である. この分解を視覚的に表示したものは図 4.6 である. 集合 $3\mathbb{Z}$, $3\mathbb{Z}+1$, $3\mathbb{Z}+2$ は, 無限集合だから, その図ではいくつかの元だけが示されている.

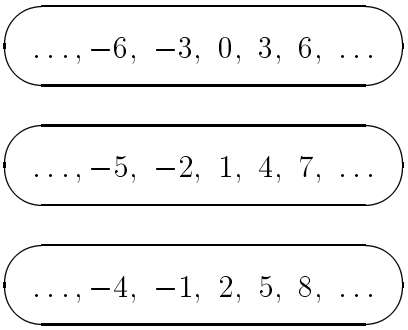


図 4.6: $3\mathbb{Z}$ による $\mathbb{Z}$ の剰余類分解

$m\mathbb{Z}$ による $\mathbb{Z}$ の剰余類を m **による剰余類**といい, $\mathbb{Z}/m\mathbb{Z}$ と表す. m で割って余りが k になる整数全体の類は, 慣例的に $\bar{k}$ と表す. 全体で, m 個の剰余類がある: $\bar{0},\bar{1},\cdots,\overline{m-1}$. たとえば, 3 を法とする剰余類は, 次の 3 つの類がある: $\bar{0},\bar{1},\bar{2}$(図 4.6).

その図をみると, 2 つの数の和は, つねに 1 つの同じ類に属し, その類は, その 2 つの数がそれぞれ属している類によってのみ決まり, 代表元のとり方に依存しないことがわかる. たとえば, 類 $\bar{1}$ から代表元 $1,-2,-7$ を, 類 $\bar{2}$ から代表元 $-4,5,8$ をとるとすると, このとき, $1+(-4)=-3,(-2)+5=3,7+8=15$ より, これらの和はすべて同じ類に属することがわかる. 一般に, 等式

$$(mx+k)+(my+l)=m(x+y)+k+l$$

は, m による剰余類の和の演算 の定義である. すなわち, $\bar{k}$ と $\bar{l}$ の和は, $\bar{k}$ の代表元と, $\bar{l}$ の代表元のとり方に依存しない. たとえば, $m=3$ ならば, 3 を法とする剰余類の

集合において, 次の和の表を得る：

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

上記の表から, 3 を法とする剰余類は, 位数 3 の巡回群であることがわかる.

練習 92. 任意の整数 m に対して, m による剰余類は, 位数 m の巡回群であることを証明せよ.

さて, 次のことを考えてみよう：

「剰余類における和の定義と同じ ようにして, 剰余類における**積**も定義することができるか？」 答えは「定義できる」である.

実際, 任意の代表元 $mk+k \in \bar{k}$, $my+l \in \bar{l}$ に対して, $(mk+k)(my+l) = m(mxy+xl+ky)+kl$ となる. この値は, m で割ると余りが kl となる整数である. また, この余りは, 代表元のとり方に依存しない. よって, この演算は剰余類の集合において, 正しく定義されている.

次の表は, 3 を法とする剰余類の集合の積表である：

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

明らかに, この積は群の公理をみたさない. なぜなら, この積表には要素がすべて 0 の縦列と横列があるが, 群の積表であれば縦列にも横列にも同じ元は 2 つ以上ない. しかし, 0 の縦列と横列をこの表から除くと次のようになり

$\times$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{1}$

この表に関しては, 群の公理がみたされる—これは位数 2 の巡回群を表している.

練習 93. 6 を法とするゼロでない剰余すべての集合は, 乗法 (かけ算) に関して群をなすか.

練習 94 より, 次のことを思いつくだろう：m **によるの剰余類から, 積を演算とする群をつくるためには, m と互いに素な剰余だけをえらべばよい**. たとえば, $m = 6$ ならば, 6 と公約数 2 をもつ元 $\bar{4}$ は, $\bar{3}$ をかけることによって $\bar{0}$ になる. しかし, $\bar{0}$ は群に属さ

ない. なぜならば, $\bar{0}$ は 0 だけを元とする列全体をつくってしまうからである. 次の重要な事実を証明しよう:

『m を法とする剰余類 $\bar{k}$ のすべての集合は, 積の演算に関して群をなす. ただし, k は m と互いに素な整数とする.』

実際, 2 つの整数が m と互いに素であるなら, それらの積もまた m と互いに素な整数となる. このことは, その演算がその与えられた集合で閉じていることを意味する. 結合法則は, 数のふつうの積の結合法則性から成り立つ. 類 $\bar{1}$ は m と互いに素で, 単位元の役割をする. 確認しなければならないただ 1 つの明らかでない性質は, その集合におけるすべての剰余類が逆元をもつことである. 言い換えれば, m と互いに素な任意の整数 a に対して, m と互いに素で $ax \equiv 1 (\mathrm{mod}\ m)$ となるような整数 x が存在することである. 最後の式は 「 ax と 1 は m を法として合同である」と読まれる. 定義より, ax は m で割ると余りが 1 の整数である. これは, 次のように言い換えられる：**$ax + my = 1$ となる整数 y が存在する**. この事実はすでに示した (練習 91 の系). x と m は互いに素であることを示さなければならないが, これは明らかである.

練習 94. 6 を法とする 2 つの剰余類の集合 $\{\overline{2}, \overline{4}\}$ は, 積に関して群をなすか.

任意の m に対して, m を法とする剰余類のうちの, m と互いに素な整数の剰余全体の積群を $\mathbb{Z}_m^*$ と表すことにする. $\mathbb{Z}_m^*$ の位数, すなわちこのような剰余の総数を m の**オイラー関数**といい, $\varphi(m)$ と表す (p. 65 参照). 次に, Lagrange の定理の算術的な応用を述べよう.

任意の群 G と G の任意の元 g に対して, 等式 $g^m = e$ が成り立つことに注意しよう. ここで, m は G の位数, e は単位元である. 実際, g の位数を k とすると, Lagrange の定理によって適当な整数 l に対して, $m = kl$ となり, $g^m = (g^k)^l = e^l = e$ が成り立つ.

$G = \mathbb{Z}_m^*$ のとき, このことは次の定理を意味する：

定理 8 *(Euler)* a が m と互いに素な整数であるとき,

$$a^{\varphi(m)} \equiv 1 \ (\mathrm{mod}\ m)$$

が成り立つ. ここで, $\varphi(m)$ は m の *Euler* 関数である. すなわち, m と互いに素な *1* から m の整数である.

$m = p$ が素数のとき, $\varphi(p) = p - 1$ であるから, Euler の定理は次の定理となる. これは **Fermat の小定理**として知られている.

定理 9 p が素数であるとき, p で割り切れない任意の整数 a に対して,

$$a^{p-1} \equiv 1 \ (\mathrm{mod}\, p) \tag{4.6}$$

が成り立つ.

歴史的備考: Fermat も Euler も彼らの定理を証明するのに, 系統的な群論による考察はしなかった. 群論は 19 世紀の初めになってやっと, E.Galois の仕事によって世に出たのであるが, Fermat も Euler も**暗黙には**群の理論, たとえば剰余類分解などを用いたにちがいない. Fermat や Euler の研究は, 群論が産まれた要因の 1 つである. 群論のいろいろな概念や定理を的確に適用することによって, 算術的な事柄はもっと明確に解明され, そして更なる一般化へと発展するだろう.

この章の最後に, 剰余や Euler の定理によって解ける数論の初等的な問題をいくつかあげておく.

練習 95. 方程式 $x^2 = 3y^2 + 8$ をみたす整数解は存在しないことを証明せよ.

練習 96. 2003^{2004} の十の位と一の位の数字を求めよ.