情報数理C

土谷 昭善 (akiyoshi@is.sci.toho-u.ac.jp)

目 次

1　整数の性質

このテキストでは，自然数は 1 以上の整数とする．また $\mathbb{N}, \mathbb{Z}, \mathbb{Z}_{\geq 0}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ をそれぞれ自然数全体，整数全体，非負整数全体，有理数全体，実数全体，複素数全体の集合とする．

1.1　整数の割り算

整数の性質を考える上で，割り算の「余り」を考えることは非常に重要である．まずは整数上の「割り算」を厳密に定義することからはじめる．ただし，ここで考えたいのは「$5 \div 2 = 2.5$」のように小数点以下まで考える割り算ではなく,「$5 \div 2 = 2$ 余り 1」のように，小学生の頃学習した「余りのある割り算」である．

定義 1.1. 整数 n を整数 $d(\neq 0)$ で**割る**とは，整数の組 (q, r) で条件

(1) $n = dq + r$,

(2) $0 \leq r < |d|$

を満たすものを見つけることである．特に，q をこの割り算の**商**，r を**余り**という．

すると，上で述べた「$5 \div 2 = 2$ 余り 1」という割り算は $n = 5, d = 2$ に対して，$(q, r) = (2, 1)$ という整数の組を見つけることを意味している．特に，$5 = 2 \times 2 + 1$ という表示がこの割り算では重要となる．またこの定義を使えば，負の整数の割り算に関しても「余り」を定義することができる．ただし,「余り」がいつでも非負になることに注意する．例えば，-7 を -3 で割ると，$-7 = (-3) \times 2 + (-1)$ という表示があるが，-1 は余りではない．$-7 = (-3) \times 3 + 2$ という表示の 2 が余りとなる．

さて，小学校の頃を思い出すと，整数の割り算では，商も余りも必ず存在し，さらにその答えが一つ（一意的）であった．この性質は割り算において非常に重要である．これを証明する．

定理 1.2 (剰余の定理)**.** 整数 n と整数 $d(\neq 0)$ に対し，整数の組 (q, r) で条件

(1) $n = dq + r$,

(2) $0 \leq r < |d|$

を満たすものが一意的に存在する．

Proof. $d \neq 0$ なので，ある整数 q で $|d|q \leq n < |d|(q+1)$ となるものが存在する．$r = n - |d|q$ とすると，$0 \leq r < |d|$ である．$d > 0$ の場合はこの (q, r) は条件 (1)，(2) を満たす．一方，$d < 0$ の場合は，q を $-q$ に取り替えることによって (q, r) が条件 (1)，(2) を満たす．よって条件 (1)，(2) を満たす整数の組 (q, r) がいつでも存在する．次に一意性を言うために，(q, r) と (q', r') がともに条件 (1)，(2) を満たす整数の組とする．このとき，$n = dq + r = dq' + r'$ なので，$d(q - q') = r' - r$ が従う．$0 \leq r < |d|$ および $0 \leq r' < |d|$ から

$$-|d| < r' - r < |d|$$

が成り立つ．特に，

$$0 \leq |r' - r| < |d|$$

である．したがって，

$$0 \leq |d| \cdot |q - q'| < |d|$$

から

$$0 \leq |q - q'| < 1$$

となるが，$q-q'$ は整数なので，$q-q'=0$，つまり $q=q'$ が得られる．上の等式に代入することで，$r'-r=0$，つまり $r=r'$ も得られ，一意性が示された． □

補足 1.3. 足し算，引き算，掛け算ができる集合を**環**という．もちろん整数の集合 $\mathbb{Z}$ は環である．環の中でも「余りを考慮した割り算」ができる環を**ユークリッド整域**という．他の例として，実数係数の（1 変数）多項式全体の集合 $\mathbb{R}[x]$ はユークリッド整域である（高校数学の多項式の割り算を思い出そう）．このユークリッド整域が後々見る整数の性質と深く関わっている．

次に整数に関する幾つかの用語を定義していく．

定義 1.4. 整数 n が整数 $d(\neq 0)$ の**倍数**である（または d は n の**約数**である）とは，ある整数 x が存在して，$n=dx$ と書けるときにいう．これは，n を d で割ったときの余りが 0 となることと同値である．このとき，d は n を**割り切る**といい，$d|n$ と書く．d が n を割り切らないときは $d \nmid n$ と書く．

例えば，$2|6$，$2 \nmid 5$，$-3|6$ である．

補足 1.5. 任意の整数 $0 \neq d \in \mathbb{Z}$ に対して，$0=0\cdot d$ であるので，d は 0 の約数である．つまり $d|0$ がいつでも成り立つ．

定義 1.6. 整数 $a_1,\dots,a_n \in \mathbb{Z}$ を考える．ただし少なくとも 1 つは 0 でないとする．

(1) 整数 d が $a_1,\dots,a_n$ の**公約数**であるとは，任意の $1\leq i\leq n$ に対して $d|a_i$ が成り立つときにいう．公約数のうち最大のものを**最大公約数** (greatest common divisor) といい，$\gcd(a_1,\dots,a_n)$ と書く．特に，$\gcd(a_1,\dots,a_n)=1$ のとき，整数 $a_1,\dots,a_n$ は**互いに素**という．

(2) 整数 ℓ が $a_1,\dots,a_n$ の**公倍数**であるとは，任意の $1\leq i\leq n$ に対して，$a_i|\ell$ が成り立つときにいう．正の公倍数のうち最小のものを**最小公倍数** (least common multiple) といい，$\mathrm{lcm}(a_1,\dots,a_n)$ と書く．

例えば，$\gcd(-3,6,-9)=3, \mathrm{lcm}(-6,9)=18$ である．また $\gcd(2,4)=2$ なので，2 と 4 は互いに素ではないが，$\gcd(2,3,4)=1$ なので，2, 3, 4 は互いに素である．

1.2 イデアル

次にイデアルという概念を考える． 0 でない整数 a に対し，a の倍数全体の集合を $a\mathbb{Z} := \{ax : x\in\mathbb{Z}\}$ と書く．また 0 でない整数 a,b に対し，

$$a\mathbb{Z}+b\mathbb{Z} := \{ax+by : x,y\in\mathbb{Z}\}$$

と定義する．

定義 1.7. a,b を 0 でない整数とする．このとき，$a\mathbb{Z}$ を a で生成される**イデアル**といい，$\langle a\rangle$ と書く．また $a\mathbb{Z}+b\mathbb{Z}$ を a と b で生成される**イデアル**といい，$\langle a,b\rangle$ と書く．

例えば，$\langle 1\rangle = 1\mathbb{Z} = \{1\cdot x : x\in\mathbb{Z}\} = \mathbb{Z}$ である．同様に，$\langle -1\rangle = (-1)\mathbb{Z} = \{-1\cdot x : x\in\mathbb{Z}\} = \mathbb{Z}$ である．したがって，$\langle 1\rangle = \langle -1\rangle$ がわかる．一般に，整数 $a\in\mathbb{Z}$ に対し，$\langle a\rangle = \langle -a\rangle$ が成り立つ（証明せよ）．

さて，上の定義では 2 つの整数で生成されるイデアルを定義したが，実際にはこれは，ある 1 つの整数で生成されるイデアルと一致する．

定理 1.8. 0 でない整数 a,b に対して，$\langle a,b\rangle = \langle m\rangle$ となる正の整数 m が存在する．

Proof. $\langle a,b\rangle$ に含まれるものの中で最小の自然数を m とする．つまり，

$$m := \min\{z \in \mathbb{N} : z \in \langle a,b\rangle\}$$

である．以下，この m に対し $\langle a,b\rangle = \langle m\rangle$ を示す．

（$\subset$）$z \in \langle a,b\rangle$ とする．このとき，整数 $x,y \in \mathbb{Z}$ を用いて $z = ax + by$ と書ける．$m > 0$ なので，z は m で割ることができ，その商と余りをそれぞれ q,r とする．つまり，

$$z = mq + r,$$

ただし $0 \leq r < m$ である．$m \in \langle a,b\rangle$ より，整数 $x',y' \in \mathbb{Z}$ を用いて $m = ax' + by'$ と表せる．すると，

$$r = z - mq = (ax + by) - (ax' + by')q = a(x - x'q) + b(y - y'q)$$

である．$x - x'q, y - y'q \in \mathbb{Z}$ より，$r \in \langle a,b\rangle$ であることがわかる．すると m の最小性から $r = 0$ が従う．つまり，$z = mq$ となり $z \in \langle m\rangle$ がわかる．よって $\langle a,b\rangle \subset \langle m\rangle$ が成り立つ．

（$\supset$）$z \in \langle m\rangle$ とする．このとき，整数 k を用いて $z = mk$ と書ける．また $m \in \langle a,b\rangle$ から，整数 x,y を用いて $m = ax + by$ と書ける．すると $z = (ax + by)k = a(xk) + b(yk)$ となり，$xk, yk \in \mathbb{Z}$ から $z \in \langle a,b\rangle$ がわかる．よって $\langle a,b\rangle \supset \langle m\rangle$ が成り立つ．

以上より，$\langle a,b\rangle = \langle m\rangle$ が示された． □

定理 1.8 の m は証明から

$$m = \min\{z \in \mathbb{N} : z \in \langle a,b\rangle\}$$

であることがわかるが，この m はどう見つければいいのだろうか．実は，a,b から簡単に計算することができる．

定理 1.9. 0 でない整数 a,b に対して

$$d := \gcd(a,b) = \min\{z \in \mathbb{N} : z \in \langle a,b\rangle\}$$

である．特に，$\langle a,b\rangle = \langle d\rangle$ である．

Proof. まず $\langle a,b\rangle \subset \langle d\rangle$ を示す．$z \in \langle a,b\rangle$ とする．このとき，整数 $x,y \in \mathbb{Z}$ を用いて $z = ax + by$ と書ける．$\gcd(a,b) = d$ から整数 a',b' を使って $a = a'd, b = b'd$ と表すことができる．すると，$z = a'dx + b'dy = d(a'x + b'y)$ となり，$a'x + b'y$ は整数であるから，$z \in \langle d\rangle$ がわかる．よって $\langle a,b\rangle \subset \langle d\rangle$ である．

次に $m = \min\{z \in \mathbb{N} : z \in \langle a,b\rangle\}$ とする．定理の証明には $m = d$ を示せばよい．定理 1.8 の証明から $\langle a,b\rangle = \langle m\rangle$ となる．すると $\langle m\rangle = \langle a,b\rangle \subset \langle d\rangle$ となる．つまり $m\mathbb{Z} \subset d\mathbb{Z}$，特に $d|m$ である．よって $m,d > 0$ より $m \geq d$ が成り立つ．一方，$a,b \in \langle a,b\rangle = \langle m\rangle$ より整数 a',b' を用いて $a = a'm, b = b'm$ と書ける．よって m は a と b の公約数である．d は a と b の最大公約数であったので，$m \leq d$ が成り立つ．以上より $m = d$ である． □

系 1.10. a,b を 0 でない整数とし，$d = \gcd(a,b)$ とする．このとき，ある整数 x,y で

$$ax + by = d$$

となるものが存在する．

Proof. $d \in \langle d\rangle$ と定理 1.9 から従う． □

この系を使って一つ命題を証明する．

命題 1.11. 0 でない整数 n と整数 a, b が $n|ab$ を満たすとする．もし n と a が互いに素なら $n|b$ が成り立つ．

Proof. $n|ab$ から整数 m を使って $ab = nm$ と書ける．仮定から n と a は互いに素，つまり $\gcd(n, a) = 1$ なので，系 1.10 より $nx + ay = 1$ を満たす整数解 (x, y) が存在する．この等式の両辺を b 倍すると

$$nbx + aby = b$$

であり，$ab = nm$ から $b = nbx + nmy = n(bx + my)$ となる．これより $n|b$ が従い証明が完了した． □

補足 1.12. 本来のイデアルの定義を書いておく．空でない $\mathbb{Z}$ の部分集合 I が**イデアル**であるとは，条件

(1) $a, b \in I$ ならば $a + b \in I$,

(2) $a \in I$ かつ $x \in \mathbb{Z}$ ならば $ax \in I$

を満たすときにいう．実は，どんなイデアル I もある整数 m を用いて $I = \langle m \rangle$ と書くことができる．イデアルはもともと環に対して定義される概念である．$\mathbb{Z}$ のように，どんなイデアルも 1 つの元で生成されるとき，その環は**単項イデアル整域（PID）**と呼ばれる．特に，ユークリッド整域は単項イデアル整域である．よって $\mathbb{Z}$ や $\mathbb{R}[x]$ は単項イデアル整域となっている．

1.3 ユークリッド互除法

例えば $\gcd(2, 3) = 1$ であるので，系 1.10 から $2x + 3y = 1$ は整数解をもつ．実際，$2 \cdot 2 + 3 \cdot (-1) = 1$ である．しかし，系 1.10 は解の存在は保証するが，具体的に解を求めることはできない．この解をユークリッド互除法を用いることで具体的に見つけることができる．まずはユークリッド互除法を紹介する．これは以下の定理を基本としたアルゴリズムである．

定理 1.13 (互除法の基本)**.** 整数 a を整数 $b(\neq 0)$ で割ったときの商と余りをそれぞれ q と r とする．つまり $a = bq + r$ で $0 \leq r < |b|$ である．このとき，

$$\gcd(a, b) = \gcd(b, r)$$

である．

Proof. $\gcd(a, b) = d_1, \gcd(b, r) = d_2$ とする．定義から $d_2|b$ かつ $d_2|r$ である．これと $a = bq + r$ から $d_2|a$ も従う．よって d_2 は a と b の公約数であるから，最大公約数の定義より $d_2 \leq d_1$ が成り立つ．同様に $d_1 \leq d_2$ も示すことができるので，$d_1 = d_2$ である． □

互除法の基本を繰り返して使うことで最大公約数を求めるアルゴリズムがユークリッド互除法である．

定理 1.14 (ユークリッド互除法)**.** 0 でない整数 a, b に対し，$\gcd(a, b)$ は，次のアルゴリズムによって，有限回のステップで計算することができる．

INPUT : a, b

OUTPUT : $d = \gcd(a, b)$

$(n, d) := (a, b)$

$r := n$ を d で割ったときの余り

WHILE $r \neq 0$ DO

　　$n := d$

　　$d := r$

　　$r := n$ を d で割ったときの余り

RETURN d

Proof. 証明すべきことはこのアルゴリズム有限回のステップで停止することと，停止したときに出力される d が $\gcd(a, b)$ となることである．今，WHILE が始まる前の (n, d, r) を (n_0, d_0, r_0) とし，WHILE が始まって i 回目の繰り返しが終わったときの (n, d, r) を (n_i, d_i, r_i) と書くことにする．r_0 は $n_0 = a$ を $d_0 = b$ で割った余りなので，$0 \leq r_0 < |b|$ が成り立つ．もし $r_0 \neq 0$ であれば，r_1 は $n_1 = d_0$ を $d_1 = r_0$ で割った余りなので $0 \leq r_1 < r_0 < |b|$ である．もし $r_1 \neq 0$ であれば，r_2 は $n_2 = d_1$ を $d_2 = r_1$ で割った余りなので $0 \leq r_2 < r_1 < r_0 < |b|$ である．これを繰り返すと，もし任意の k に対して $r_k \neq 0$ であれば，狭義単調減少する無限列

$$0 \leq \cdots < r_i < r_{i-1} < \cdots < r_2 < r_1 < r_0 < |b|$$

が構成できる．しかし $|b|$ より小さい自然数は有限個しか存在しないので，そのような無限列は存在しない．よってある k に対して $r_k = 0$ とならなければならない．したがって，アルゴリズムは有限回のステップで停止する．

今，定理 1.13 より

$$\gcd(a, b) = \gcd(b, r_0)$$

が成り立つ．$r_0 \neq 0$ なら再び定理 1.13 より

$$\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1)$$

である．アルゴリズムが $r_k = 0$ で停止したと仮定すると，同様の議論から等式

$$\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \cdots = \gcd(r_{k-1}, r_k) = \gcd(d_k, 0) = d_k$$

出力される値が $\gcd(a, b)$ であることがわかった． □

具体例でユークリッド互除法を使ってみよう．さらにここでは $ax + by = \gcd(a, b)$ の整数解 (x, y) の見つけ方も紹介する．

例 1.15. $a = 108, b = 57$ として $\gcd(a, b)$ を求める．

$$\underline{108}_a \div \underline{57}_b \to 108 = 1 \times 57 + \underline{51}_{r_0}$$
$$\underline{57}_b \div \underline{51}_{r_0} \to 57 = 1 \times 51 + \underline{6}_{r_1}$$
$$\underline{51}_{r_0} \div \underline{6}_{r_1} \to 51 = 8 \times 6 + \underline{3}_{r_2}$$
$$\underline{6}_{r_1} \div \underline{3}_{r_2} \to 6 = 2 \times 3 + \underline{0}_{r_3}$$

から

$$\gcd(108, 57) = \gcd(57, 51) = \gcd(51, 6) = \gcd(6, 3) = \gcd(3, 0) = 3$$

が得られる．よって $\gcd(108, 57) = 3$ である．

系 1.10 から $108x+57y=3$ を満たす整数解 (x,y) が存在することはわかっている．ユークリッド互除法の逆を辿ると少なくとも整数解を 1 つ見つけることができる．実際，上の式から

$$\underline{51}_{r_0} = \underline{108}_a - 1 \times \underline{57}_b$$
$$\underline{6}_{r_1} = \underline{57}_b - 1 \times \underline{51}_{r_0}$$
$$\underline{3}_{r_2} = \underline{51}_{r_0} - 8 \times \underline{6}_{r_1}$$

が得られる．2 つ目の式を 3 つ目の式の右辺に代入すると

$$3 = \underline{51}_{r_0} - 8 \times (\underline{57}_b - 1 \times \underline{51}_{r_0}) = (-8) \times \underline{57}_b + 9 \times \underline{51}_{r_0}.$$

1 つ目の式をこの式の右辺に代入すると

$$3 = (-8) \times \underline{57}_b + 9 \times (\underline{108}_a - 1 \times \underline{57}_b) = 9 \times \underline{108}_a + (-17) \times \underline{57}_b.$$

したがって，$108x+57y=3$ の整数解として $(x,y)=(9,-17)$ が得られた．

1 つ整数解を見つけることができれば解全体を求めることは可能である．実際，

$$\begin{cases} 108x+57y=3 \\ 108\cdot 9+57\cdot(-17)=3 \end{cases}$$

に対し，上式から下式を引くと

$$108(x-9)+57(y+17)=0$$

が得られる．$\gcd(108,57)=3$ からこの方程式の両辺を 3 で割って

$$36(x-9)+19(y+17)=0$$

つまり $36(x-9)=-19(y+17)$ である．これより，$36|(-19)(y+17)$ がわかる．特に，36 と -19 は互いに素なので，命題 1.11 から $36|y+17$ である．したがって，ある整数 k を用いて $y+17=36k$ と表せる．また

$$36(x-9)=-19\cdot 36k$$

から $x=-19k+9$ となる．よって $108x+57y=3$ の整数解全体の集合は

$$\{(-19k+9, 36k-17) : k\in\mathbb{Z}\}$$

である．

1.4 素因数分解

定義 1.16. p を 1 でない自然数とする．p の正の約数が 1 と p のみのとき，p を**素数**と呼ぶ．また p が素数でない，つまり，1 と p 以外の正の約数を持つとき，p を**合成数**と呼ぶ．

中学校で素因数分解を学んだと思うが，ここでは，0 でないどんな整数も素因数分解でき，しかもその表示は一意的であることを証明する．まずは次の命題を示す．

命題 1.17. 素数 p と整数 a,b に対し，$p|ab$ ならば $p|a$ または $p|b$ が成り立つ．

Proof. $p|ab$ のとき，$p\not|a$ を仮定する．このとき p が素数なので，a と p は互いに素である．よって命題 1.11 より $p|b$ が従い証明が完了した． □

この命題の p が素数という条件は必要である．実際，$6|12$ だが $6\not|3$ かつ $6\not|4$ である．それでは素因数分解に関する定理を証明する．

定理 1.18 (素因数分解の存在とその一意性)**.** n を $0, \pm 1$ でない整数とする．このとき，ある有限個の素数 $p_1, \ldots, p_s$（重複可）が存在して

$$n = \pm p_1 p_2 \cdots p_s$$

と書ける．ただし，符号は $n > 0$ のとき $+$，$n < 0$ のとき $-$ をとる．この表示を n の**素因数分解**という．また素因数分解は n に対して,（素数の順番を除いて）一意的である．

Proof. まずは存在を示す． $|n|$ が素数のときは $n = \pm|n|$ が欲しい表示であるので存在する．特に，$|n| = 2$ で成り立つ．次に，3 以上の整数 k に対し，$1 < |m| < k$ を満たす任意の整数 m が素因数分解を持つと仮定する．このとき $|n| = k$ を満たす整数 n が素因数分解を持つことを示す．k は合成数であると仮定してよい．つまり 1 でない自然数 a, b を使って $k = ab$，特に $n = \pm ab$ という表示を持つ．このとき $1 < a, b < k$ であるので，帰納法の仮定から a と b は素因数分解を持つ．それを $a = p_1 p_2 \cdots p_s, b = q_1 q_2 \cdots q_r$ とする．すると

$$n = \pm p_1 p_2 \cdots p_s q_1 q_2 \cdots q_r$$

となり，n は素因数分解を持つ．したがって，$|n|$ に関する帰納法より素因数分解の存在が示された．

次に一意性を示す．これは n が素因数分解の表示として

$$n = \pm p_1 p_2 \cdots p_s = \pm q_1 q_2 \cdots q_r$$

という 2 つの表示が与えられたとき，$s = r$ かつ適当に順番を並び替えることにより $p_1 = q_1, \ldots, p_s = q_s$ となるようにできることを言えばよい．これも $|n|$ に関する帰納法で示す．$|n|$ が素数のときは，$n = \pm|n|$ という表示が一意的であることは容易にわかる．特に，$|n| = 2$ で成り立つ．次に，3 以上の整数 k に対し，$1 < |m| < k$ を満たす任意の整数 m の素因数分解が一意的であると仮定する．このとき $|n| = k$ を満たす整数 n の素因数分解が一意的であることを示す．k は合成数であると仮定してよい．

$$n = \pm p_1 p_2 \cdots p_s = \pm q_1 q_2 \cdots q_r$$

という 2 つの素因数分解の表示が与えられたと仮定する．k が合成数であるので $s, r \geq 2$ である．$p_s | \pm q_1 q_2 \cdots q_r$ であるから，命題 1.17 を繰り返し使うことで，p_s は $q_1, \ldots, q_r$ のいずれかを割り切る．必要なら $q_1, \ldots, q_r$ の順番を並べ替えることで $p_s | q_r$ としてよい．このとき，$p_s = q_r$ である．一方，

$$\frac{n}{p_s} = \pm p_1 p_2 \cdots p_{s-1} = \pm q_1 q_2 \cdots q_{r-1}$$

となるが，$p_s > 1$ から $1 < \left|\dfrac{n}{p_s}\right| < k$ であるから，帰納法の仮定より整数 $\dfrac{n}{p_s}$ の素因数分解は一意的である．つまり，$s - 1 = r - 1$，つまり $s = r$ かつ適当に順番を並び替えることにより $p_1 = q_1, \ldots, p_{s-1} = q_{s-1}$ となるようにできる．よって $p_s = q_r$ と合わせることで n は一意的な素因数分解を持つ．したがって $|n|$ に関する帰納法より，素因数分解の一意性が示された． □

補足 1.19. 整数の素数を環に拡張した概念として**素元**というものがある．また掛け算に関して逆元を持つ元を**単元**という．例えば，$\mathbb{Z}$ では単元は ± 1 のみである．どんな 0 でも単元でもない元が素元の積として一意的に書ける環を**一意分解整域（UFD）**という．したがって，整数の集合 $\mathbb{Z}$ は環として見ると一意分解整域となっている．補足 1.12 で $\mathbb{Z}$ は単項イデアル整域になっていると説明したが，実は単項イデアル整域はいつでも一意分解整域となる．つまり

$$\text{ユークリッド整域} \Rightarrow \text{単項イデアル整域} \Rightarrow \text{一意分解整域}$$

である．したがって $\mathbb{R}[x]$ も一意分解整域である．このように概念を拡張することで，例えば $\mathbb{Z}$ の素因数分解の一意性や $\mathbb{R}[x]$ の因数分解の一意性は，本質的に同じということがわかる．特に，この性質は一番はじ

めに定義した「余りを考慮した割り算」が鍵となっている.

2　合同式

情報数理 B で同値関係の例の一つとして合同式を学習した．合同式は簡単にいうと「余りの世界」で数を考えることである．この「余りの世界」における演算に着目する．

2.1　合同式の復習

合同式や同値関係の定義は情報数理 B で学習済みのため，ここでは簡単に復習する．

定義 2.1. 0 でない整数 m に対し，整数 a と b が m を**法**として**合同**であるとは，$a-b \in m\mathbb{Z}$ となるときにいう．つまり $m|a-b$ である．このとき，

$$a \equiv_m b \text{ または } a \equiv b \bmod m$$

と書く．この表示を**合同式**という．合同でないときは $a \not\equiv_m b$ や $a \not\equiv b \bmod m$ と書く．法 m が文脈から明らかのときは，単に $a \equiv b$ や $a \not\equiv b$ と書くこともある．

例えば，$7 \equiv_5 2$ や $7 \not\equiv_3 2$ である．合同式が何を意味するかというと，これは法 m で割ったときの余りが等しいということに他ならない．

命題 2.2. $a \equiv_m b$ であることと，a と b をそれぞれ m で割った余りが一致することは同値である．

Proof. a と b をそれぞれ m で割った商と余りをそれぞれ q, q' と r, r' とする．つまり，$a = mq+r, b = mq'+r'$ かつ $0 \le r, r' < |m|$ である．

（⇒）$a \equiv_m b$ であると仮定する．このとき，$a-b \in m\mathbb{Z}$ よりある整数 n を使って $a-b = mn$ と書ける．すると

$$a-b = (mq+r) - (mq'+r') = m(q-q') + (r-r') = mn$$

より $r-r' = m(n-(q-q'))$ となる．つまり，$r-r' \in m\mathbb{Z}$ である．余りの条件から，$0 \le |r-r'| < |m|$ であるので，これは $r-r' = 0$，つまり $r = r'$ を意味する．

（⇐）$r = r'$ を仮定する．このとき，

$$a-b = (mq+r) - (mq'+r') = m(q-q') + (r-r') = m(q-q') \in m\mathbb{Z}.$$

よって $a \equiv_m b$ である．　□

次に，同値関係の定義を復習する．

定義 2.3. X に対し，$X \times X$ の部分集合 R を X 上の**（二項）関係**と呼ぶ．R を X 上の二項関係 R とする．記法として，$(a,b) \in R$ のとき aRb と書く．

(1) R が**反射的**であるとは，任意の $x \in X$ に対して xRx であるときにいう．

(2) R が**対称的**であるとは，任意の $a, b \in X$ に対して aRb ならばいつでも bRa であるときにいう．

(3) R が**推移的**であるとは，任意の $a, b, c \in X$ に対して，aRb かつ bRc ならばいつでも aRc となるときをいう．

(4) 反射的，対称的かつ推移的な二項関係を**同値関係**と呼ぶ．同値関係には $\sim$ という記号がよく使われる．

同値関係は「何らかの意味で等しい」を意味する．もちろん通常の「等しい（$=$）」は同値関係である．合同式は「余りが等しい」を意味していたので，合同式も同値関係となる．

命題 2.4. 合同式 $\equiv_m$ を $\mathbb{Z}$ 上の二項関係としてみると，$\equiv_m$ は同値関係である．

Proof. 情報数理 B の 4 回目を参照. □

$m = \pm 1$ の場合，任意の整数 a, b に対して $a \equiv_m b$ である．この場合，合同式の世界では「全ての整数は等しい」ということになるので考えるべきことはほとんどない．以降，m は $|m| \geq 2$ を満たす整数とする．

2.2 合同式の演算

次に合同式の演算を見ていく．

命題 2.5. a, b, c, d を $a \equiv_m b$ かつ $c \equiv_m d$ を満たす整数とする．

(1) $a + c \equiv_m b + d$ かつ $ac \equiv_m bd$ である．

(2) 0 でない整数 n が $n|m$ を満たすとすると，$a \equiv_n b$ である．

Proof. 仮定より整数 k, ℓ を用いて $a - b = mk, c - d = m\ell$ と書ける．

(1)

$$(a + c) - (b + d) = (a - b) + (c - d) = mk - m\ell = m(k - \ell) \in m\mathbb{Z}$$

となるので $a + c \equiv_m b + d$ である．また

$$ac - bd = a(c - d) + ad - bd = a(c - d) + d(a - b) = am\ell + dmk = m(a\ell + dk) \in m\mathbb{Z}$$

から $ac \equiv_m bd$ である．

(2) 仮定より整数 t を用いて $m = nt$ と書ける．このとき，$a - b = (nt)k = n(tk) \in n\mathbb{Z}$ である．よって $a \equiv_n b$ である． □

系 2.6. a, b を $a \equiv_m b$ を満たす整数とする．このとき，任意の整数 c に対し，以下が成り立つ．

(1) $a + c \equiv_m b + c$,

(2) $a - c \equiv_m b - c$,

(3) $ac \equiv_m bc$.

これらの結果から $\equiv_m$ の世界では $+, -, \times$ は「$=$」と同じように計算ができる．ただし，$\div$ はできない．実際，$6 \equiv_4 2$ であるが，両辺を 2 で割ると $3 \not\equiv_4 1$ である．一方で，ある条件下だと $\div$ をすることができる．

命題 2.7. c を 0 でない整数，a, b を整数とし，$ac \equiv_m bc$ を満たすとする．このとき以下が成り立つ．

(1) $c|m$ ならば

$$a \equiv b \bmod \frac{m}{c}$$

である．

(2) c と m は互いに素，つまり $\gcd(c, m) = 1$ なら $a \equiv_m b$ が成り立つ．

Proof. 仮定から整数 n を用いて $ac - bc = mn$ と書ける．

(1) $c(a-b) = mn$ であり，両辺を c で割ると，

$$a - b = \frac{m}{c}n$$

となる．$c|m$ より $\dfrac{m}{c}$ は整数であるので，$a \equiv b \bmod \dfrac{m}{c}$ が成り立つ．

(2) $c(a-b) = mn$ から $m|c(a-b)$ である．c と m は互いに素なので命題 1.11 より $m|a-b$ である．よって $a \equiv_m b$ が成り立つ． □

定義 2.8. 整数 a が法 m に関して**可逆**であるとは，$ax \equiv_m 1$ を満たす整数 x が存在するときにいう．またこのとき，x を法 m に関する a の**逆元**という．

例えば，$2 \cdot 3 \equiv_5 1$ であるので，3 は 2 の法 5 に関する逆元であり，逆に 2 は 3 の法 5 に関する逆元である．よって 2 と 3 はともに法 5 に関して可逆である．逆元はいつでも存在するとは限らない．つまり，可逆であるとは限らない．例えば，2 は法 4 に関して逆元を持たない（理由を考えよ）．一方で，もし逆元が存在すれば，m を法として一意的に定まる．

命題 2.9. a を法 m に関して可逆な整数とする．x, y がともに a の法 m に関する逆元であれば，$x \equiv_m y$ である．

Proof. 仮定より，$ax \equiv_m ay \equiv_m 1$ であるから，

$$x \equiv_m x \cdot 1 \equiv_m x(ay) \equiv_m (ax)y \equiv_m 1 \cdot y \equiv_m y$$

が成り立つ． □

余りの世界では，通常の整数の積では起きない不思議な現象がある．実際，$2 \not\equiv_6 0$ かつ $3 \not\equiv_6 0$ であるが，$2 \cdot 3 \equiv_6 0$ となる．このような性質に名前をつけよう．

定義 2.10. 整数 a が法 m に関して**零因子**であるとは，$az \equiv_m 0$ かつ $z \not\equiv_m 0$ を満たす整数 z が存在するときにいう．

上の議論より，2 と 3 はともに法 6 に関する零因子である．また 0 は任意の法に関する零因子である．

今定義した，逆元と零因子は実は真逆の性質である．

定理 2.11. 整数 a に対して次は同値である．

(1) a, m は互いに素である．

(2) a は法 m に関して可逆である．

(3) a は法 m に関して零因子ではない．

Proof. ((1) $\Rightarrow$ (2)) $\gcd(a, m) = 1$ と系 1.10 から $ax + my = 1$ となる整数 x, y が存在する．このとき，$ax \equiv_m 1$ であるので，a は法 m に関して可逆である．

((2) $\Rightarrow$ (3)) 整数 x を a の法 m に関する逆元とする．つまり，$ax \equiv_m 1$ である．今，a が法 m に関して零因子であると仮定する．このとき，ある整数 z に関して $az \equiv_m 0$ かつ $z \not\equiv_m 0$ である．すると，

$$z \equiv_m 1 \cdot z \equiv_m (ax)z \equiv_m x(az) \equiv_m x \cdot 0 \equiv_m 0$$

となり，矛盾する．よって a は法 m に関して零因子ではない．

((3) ⇒ (1)) $d = \gcd(a, m)$ とおく．このとき，整数 a', m' を用いて $a = a'd, m = m'd$ と書ける．すると，

$$am' = (a'd)m' = a'(m'd) = a'm \equiv_m 0$$

となるが，仮定より a は法 m に関する零因子ではないので，$m' \equiv_m 0$ とならなければならない．つまり，$m' \in m\mathbb{Z}$ であるので，ある整数 c を用いて $m' = mc$ と書ける．すると，$m = m'd = mcd$ であるので，$cd = 1$，よって $d = 1$ となる． □

補足 2.12. 命題 2.7 (2) から m が素数であれば，$\equiv_m$ の世界では $+, -, \times, \div$ の四則演算ができることがわかる．逆に，四則演算ができるのは m が素数のときに限ることも示せる．

2.3 1 次合同方程式と連立 1 次合同方程式

1 次合同式とは 1 次方程式の合同式版である．つまり，$a \not\equiv_m 0$ を満たす整数 a と整数 b，および未知数 x に対し，式

$$ax \equiv_m b$$

を考える．この方程式を解くというのは，上の合同方程式を満たす x を（適切な法の下で）求めることである．また $ax \equiv_m b$ ならば，ある整数 y を使って，$ax - b = my$，よって $ax - my = b$ となるので，合同方程式を解くということはこの不定方程式を解くことに他ならない．

それでは，例として $2x \equiv_3 1$ を解いてみよう．系 2.6 より両辺を 2 倍してもよいので $4x \equiv_3 2$ である．また $4 \equiv_3 1$ から $4x \equiv_3 x$ も成り立つ．よって解 $x \equiv_3 2$ を得る．一方，合同方程式は解を持たない場合もある．例えば $2x \equiv_4 1$ とすると．両辺を 1 で引くと $2x - 1 \equiv_4 0$．しかし，$2x - 1$ は奇数なので 4 で割った余りは 0 になり得ない．よって $2x - 1 \not\equiv_4 0$ となり解が存在しないことがわかった．

そこで合同方程式はいつ解を持つのかを考えてみよう．

> **定理 2.13.** $a \not\equiv_m 0$ を満たす整数 a と整数 b に対し，合同方程式 $ax \equiv_m b$ が整数解を持つ必要十分条件は $d = \gcd(a, m)$ としたとき，$d|b$ となることである．

Proof. $\gcd(a, m) = d > 0$ より整数 a', m' を用いて $a = a'd, m = m'd$ と書ける．

（⇒）合同方程式が解 x を持つとすると，ある整数 k を用いて $ax - b = mk$ と書ける．すると，$b = ax - mk = a'dx - m'dk = d(a'x - m'k)$ であり，$ax' - m'k$ は整数なので，$d|b$ である．

（⇐）$d|b$ を仮定する．このとき $b \in \langle d \rangle$ である．すると定理 1.8 から $\langle a, m \rangle = \langle d \rangle \ni b$ である．したがってある整数 x, y を用いて $b = ax + my$ と書ける．よって $b \equiv_m ax$ であり，x が合同方程式の解となることがわかった． □

この定理から合同方程式に解が存在するかどうか判定することができるが，その解が同じ法に関して一意的に書けるかはわからない．実際，$2x \equiv_6 4$ を考えると，$\gcd(2, 6) = 2|4$ であるので，解を持つ．しかしその解は $x \equiv_6 2$ と $x \equiv_6 5$ の 2 通り出てくる．ただし，特別な状況であれば同じ法に関して解を一意的に書くことができる．

> **系 2.14.** 整数 a が $\gcd(a, m) = 1$ を満たすとする．このとき，任意の整数 b に対して合同方程式 $ax \equiv_m b$ は法 m で一意的な整数解を持つ．

Proof. 定理 2.13 より解の存在は従う．一意性を示すために，x_1, x_2 がともに $ax \equiv_m b$ の整数解とする．このとき，

$$ax_1 \equiv_m b \equiv_m ax_2$$

より $a(x_1 - x_2) \equiv_m 0$ が成り立つ．a と m が互いに素であるので，定理 2.11 より a は法 m に関して零因子を持たない．よって $x_1 - x_2 \equiv_m 0$ つまり $x_1 \equiv_m x_2$ でなければならなく，一意性が示された． □

次に連立 1 次合同方程式を考える．例えば，

$$\begin{cases} x \equiv_2 1 \\ x \equiv_3 2 \end{cases}$$

を解いてみよう．これは結局 x が整数 s,t を使って $x = 2s+1 = 3t+2$ と書けるので不定方程式 $2s-3t=1$ を解くことに帰着する．実際の解は整数 k を用いて $x = 6k+5$ と書ける．つまり，$x \equiv_6 5$ である．

定理 2.15 (中国式剰余定理)**.** m,n を 0 でない互いに素な $|m|,|n| \geq 2$ を満たす整数とする．このとき，任意の整数 a,b に対し，連立 1 次合同方程式

$$\begin{cases} x \equiv_m a \\ x \equiv_n b \end{cases}$$

は法 mn に関して一意的な解を持つ．

Proof. $\gcd(m,n) = 1$ と定理 1.9 より，$\langle m,n \rangle = \langle 1 \rangle = \mathbb{Z}$ である．よって $b-a \in \langle m,n \rangle$ となる．これはある整数を x_0, y_0 を使って $b-a = mx_0 + ny_0$ と書けることを意味する．今，$a + mx_0 = b - ny_0 = x$ とおく．このとき，

$$\begin{cases} x \equiv_m a \\ x \equiv_n b \end{cases}$$

が成り立つので，この x がこの連立合同方程式の解である．

次に一意性を示す．x_1, x_2 を連立合同方程式の整数解とする．このとき，ある整数 k_1, k_2 を用いて $x_1 - a = k_1 m, x_2 - a = k_2 m$ と書ける．すると $x_1 - x_2 = (k_1 - k_2)m$ より $x_1 - x_2$ は m の倍数である．同様に，$x_1 - x_2$ は n の倍数でもある．一方，m と n は 0 でない互いに素な整数であるので，その最小公倍数は mn である．したがって，$x_1 - x_2$ は mn の倍数となる．したがって，$x_1 - x_2 \equiv_{mn} 0$，つまり $x_1 \equiv_{mn} x_2$ となり，一意性が示された． □

2.4 フェルマーの小定理

この節では，合同式に関するある公式を証明する．

定理 2.16 (フェルマーの小定理)**.** p を素数とする．p と互いに素な整数 a に対して次の合同式が成り立つ：

$$a^{p-1} \equiv_p 1.$$

この定理の証明のために，補題を準備する．

補題 2.17. k を $0 < k < p$ を満たす整数とする．このとき $\binom{p}{k}$ は p の倍数である．ただし，$\binom{p}{k} = {}_p\mathrm{C}_k = \dfrac{p!}{k!(p-k)!}$ は二項係数である．

Proof. $\binom{p}{k} = \dfrac{p!}{k!(p-k)!} \in \mathbb{Z}$ であり，$0 < k < p$ から $0 < p-k < p$ であるので，約分したときに分子の p は生き残る．よって $\binom{p}{k}$ は p の倍数である． □

補題 2.18. 整数 $a_1, \ldots, a_n$ と素数 p に対して，

$$(a_1 + \cdots + a_n)^p \equiv_p a_1^p + \cdots + a_n^p$$

が成り立つ.

Proof. n に関する帰納法で示す．$n=1$ の時は明らか．$n\geq 2$ を仮定する．$x=a_1+\cdots+a_{n-1}$ として，二項展開すると

$$(a_1+\cdots+a_n)^p=(x+a_n)^p=\binom{p}{0}x^pa_n^0+\binom{p}{1}x^{p-1}a_n^1+\cdots+\binom{p}{p-1}x^1a_n^{p-1}+\binom{p}{0}x^0a_n^p$$

である．一方，補題 2.17 より $0<k<p$ に対して，$\binom{p}{k}\equiv_p 0$ である．よって

$$(x+a_n)^p\equiv_p x^p+a_n^p$$

が成り立つ．また帰納法の仮定より

$$x^p=(a_1+\cdots+a_{n-1})^p\equiv_p a_1^p+\cdots+a_{n-1}^p$$

である．以上より，

$$(x+a_n)^p\equiv_p x^p+a_n^p\equiv_p a_1^p+\cdots+a_{n-1}^p+a_n^p$$

が成り立つので，帰納法より主張が示された． □

補題 2.19. 整数 n と素数 p に対して，

$$n^p\equiv_p n$$

が成り立つ.

Proof. $n=0$ のときは明らかである．$n\geq 1$ とする．補題 2.18 で $a_1=\cdots=a_n=1$ の場合を考えると，

$$\underbrace{(1+\cdots+1)}_{n}{}^p\equiv_p \underbrace{1^p+\cdots+1^p}_{n}$$

となるから，$n^p\equiv_p n$ である．

次に $n<0$ とする．$k=-n$ とおくと，$k>0$ より上の証明から $k^p\equiv_p k$ である．すると

$$-n=k\equiv_p k^p\equiv_p(-n)^p\equiv_p(-1)^pn^p$$

となる．ここで，$(-1)^p\equiv_p -1$ が任意の素数 p で成り立つ（$p=2$ の場合のみ注意する）．よって $-n\equiv_p(-1)n^p$ である．この両辺に -1 をかけることで $n^p\equiv_p n$ を得る． □

以上よりフェルマーの小定理の証明の準備が終わった.

定理 2.16 の証明. 命題 2.7 と補題 2.19 より従う． □

2.5 剰余類

同値関係を扱うときは，同値類や商集合を用いることで，議論が進みやすくなる．一般の同値関係の同値類や商集合の話は後にして，ここでは合同式に対する同値類である剰余類について考える.

定義 2.20. m を自然数とする．整数 a に対し，$x\equiv_m a$ を満たす整数全体の集合を $a+m\mathbb{Z}$ で表し，法 m に関する a の**剰余類**という．つまり，

$$a+m\mathbb{Z}:=\{x\in\mathbb{Z}:x\equiv_m a\}\subset\mathbb{Z}$$

である．ここで $0+m\mathbb{Z}$ は $m\mathbb{Z}$ のことである．文脈から m が明らかな場合は，$\overline{a}$ と書くことが多い.

つまり，$\overline{a} = a + m\mathbb{Z}$ である．また剰余類全体の集合を $\mathbb{Z}/m\mathbb{Z}$ と書く．つまり，

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{a} : a \in \mathbb{Z}\}$$

である．

補足 2.21. 合同式 $\equiv_m$ を $\mathbb{Z}$ 上の同値関係としてみると，剰余類 $a + m\mathbb{Z}$ は同値類 $[a]_{\equiv_m}$ のことであり，$\mathbb{Z}/m\mathbb{Z}$ は商集合 $\mathbb{Z}/\equiv_m$ のことに他ならない．

例えば，$m = 3$ のとき，

$$\begin{aligned}\overline{-1} = -1 + 3\mathbb{Z} &= \{\ldots, -4, -1, 2, 5, \ldots\},\\ \overline{0} = 0 + 3\mathbb{Z} &= \{\ldots, -3, 0, 3, 6, \ldots\},\\ \overline{1} = 1 + 3\mathbb{Z} &= \{\ldots, -2, 1, 4, 7, \ldots\},\\ \overline{2} = 2 + 3\mathbb{Z} &= \{\ldots, -4, -1, 2, 5, \ldots\}\end{aligned}$$

となる．特に，$\overline{-1} = \overline{2}$ である．

剰余類の簡単な性質を見ていく．

命題 2.22. 自然数 m を固定する．整数 a, b について以下は同値である．

(1) $\overline{a} = \overline{b}$, (2) $\overline{a} \cap \overline{b} \neq \emptyset$, (3) $a \equiv_m b$, (4) $a \in \overline{b}$, (5) $b \in \overline{a}$.

Proof. (1), (2), (3) の同値性のみ示し，(4), (5) は演習問題とする．

((1)⇒(2)) 一般に，任意の整数 x に対し $x \in \overline{x}$ であるので $\overline{x} \neq \emptyset$ である．よって $\overline{a} = \overline{b}$ から $\overline{a} \cap \overline{b} = \overline{a} \cap \overline{a} = \overline{a} \neq \emptyset$ が従う．

((2)⇒(3)) $x \in \overline{a} \cap \overline{b}$ をとる．このとき，$x \equiv_m a$ かつ $x \equiv_m b$ であるので，$a \equiv_m b$ が従う．

((3)⇒(1)) $x \in \overline{a}$ を任意にとると，$x \equiv_m a$ である．すると $a \equiv_m b$ から $x \equiv_m b$ となるので，$x \in \overline{b}$ がわかる．よって $\overline{a} \subset \overline{b}$ である．同様に，$\overline{a} \supset \overline{b}$ もわかるので $\overline{a} = \overline{b}$ が従う． □

命題 2.22 からわかる通り，もとの整数は違えど，その剰余類が同じになることは多い．例えば，$-1+3\mathbb{Z} = 2+3\mathbb{Z}$ であった．この場合，$-1+3\mathbb{Z}$ か $2+3\mathbb{Z}$ のどちらかの表記に統一した方が便利である．こういった考え方が代表元である．

定義 2.23. m を自然数とする．$x \in \mathbb{Z}/m\mathbb{Z}$ に対して，$x = \overline{a}$ となる整数 a を x の**代表元**という．

$\mathbb{Z}/m\mathbb{Z}$ の各剰余類は代表元を 0 から $m-1$ の整数から選ぶことができる．

命題 2.24. m を自然数とすると，

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

である．特に，$|\mathbb{Z}/m\mathbb{Z}| = m$ である．

Proof.

$$\mathbb{Z}/m\mathbb{Z} \supset \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

は明らかなので逆の包含関係を示す．任意の剰余類 $x \in \mathbb{Z}/m\mathbb{Z}$ をとる．このとき，ある整数 a を使って $x = \overline{a}$ と書ける．a を m で割ったときの商と余りを q, r とする．つまり，$a = qm + r$ で $0 \leq r < m$ を

満たす．すると，$a - r = qm$ なので，$a \equiv_m r$ がわかる．よって，$x = \overline{a} = \overline{r}$ であり，$0 \leq r < m$ から $x \in \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ が従い， $\mathbb{Z}/m\mathbb{Z} \subset \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ が成り立つ．

また任意の整数 $0 \leq a < b \leq m-1$ に対して，$a \not\equiv_m b$ なので，$|\mathbb{Z}/m\mathbb{Z}| = m$ が従う． □

もちろん，$\mathbb{Z}/7\mathbb{Z} = \{\overline{-3}, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ のように書くこともできるが，重要なのは剰余類が 7 個だけということである．

次に特殊な剰余類の集合を考える．

定義 2.25. m を 2 以上の自然数とする．剰余類 $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ $(a \in \mathbb{Z})$ に対して，$\gcd(a, m) = 1$ を満たすものを，法 m の**既約剰余類**と呼ぶ．また既約剰余類の集合を

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^\times &= \{\overline{a} \in \mathbb{Z}/m\mathbb{Z} : a \in \mathbb{Z}, \gcd(a, m) = 1\} \\ &= \{\overline{a} \in \mathbb{Z}/m\mathbb{Z} : 0 \leq a \leq m-1, \gcd(a, m) = 1\}\end{aligned}$$

と書く．

例えば，$(\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{1}\}, (\mathbb{Z}/3\mathbb{Z})^\times = \{\overline{1}, \overline{2}\}$ であり，$(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}, \overline{5}\}$ である．この既約剰余類の個数を考えていく．

定義 2.26. 自然数 $m \geq 2$ に対し，$\phi(m)$ を m と互いに素な整数 $1 \leq a \leq m-1$ の個数を表す関数とする．つまり，$\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$ である．この関数 ϕ を**オイラー関数**という．

上の例から $\phi(2) = 1, \phi(3) = 2, \phi(6) = 2$ となっている．

一般にフェルマーの小定理は素数 p でなければ成り立たない場合がある．実際，

$$5^{6-1} \equiv_6 5 \not\equiv_6 1$$

である．つまり，フェルマーの小定理をそのまま整数 m に拡張することはできない．一方，素数 p に対し，$\phi(p) = p - 1$ が成り立つ．よってフェルマーの小定理は p と互い素な整数 a に対して

$$a^{\phi(p)} \equiv_p 1$$

が成り立つと見ることができる．実はこの表示として考えれば，より一般の自然数に対してフェルマーの小定理を拡張することができる．

定理 2.27 (オイラーの定理)**.** 自然数 $m \geq 2$ と m と互いに素な整数 a に対して，

$$a^{\phi(m)} \equiv_m 1$$

が成り立つ．

例えば，$\phi(6) = 2$ なので，

$$5^2 \equiv_6 1$$

である．

この定理は直接証明することができるが，群を学習した後に，その応用で証明することにする．

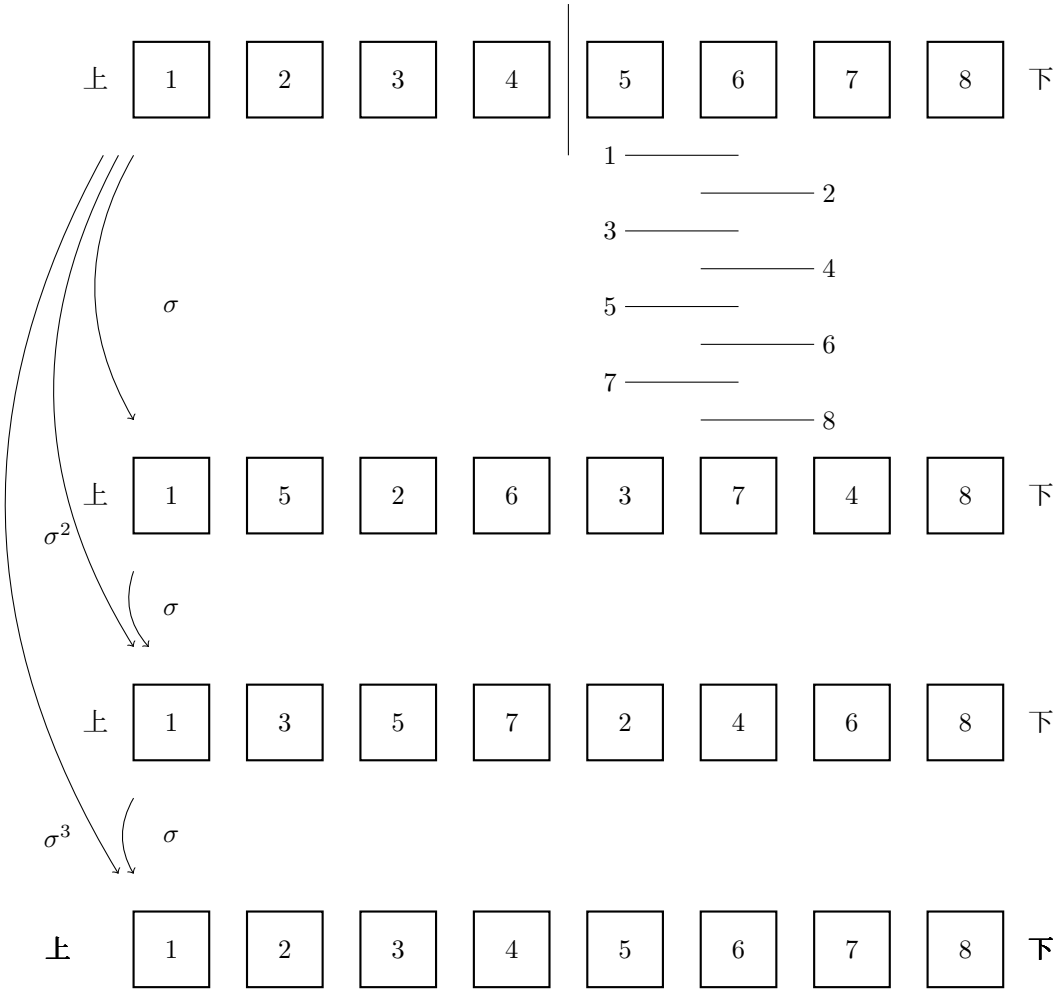
3　群の定義

3.1　イントロダクション

定義 3.1. X を空でない集合とする．X 上の**（二項）演算**とは写像 $f : X \times X \to X$ のことをいう．つまり，演算とは，2 つの要素から（同じ集合に属する）新しい要素を生み出す操作のことである．演算は $\circ, +, *, \ldots$ などを使い，$\circ(a, b)$ の代わりに $a \circ b$ と書くことが多い．こうするとこれまで知っている演算の形と思えるだろう．

例えば，整数の足し算や引き算，掛け算などは $\mathbb{Z}$ 上の演算である．演算といえば，こういった数に関する操作という認識があると思うが，どんな集合でも演算というものは考えられる．

例 3.2. 1 から 8 の数字が書かれたカードの山を準備し，この山を切る（混ぜる）ことを考える．例えば，下図のように，上下に半分に分け，上の山のそれぞれのカードの間に下の山のカードが 1 枚ずつ入るように切る．



カードの切り方全体の集合を X とする．このとき，X 上の演算を次のように定義する．カードの切り方 $\sigma_1, \sigma_2 \in X$ に対し，$\sigma_1 \circ \sigma_2$ を σ_2 で切った後に，σ_1 で切る操作として定義すると，この一連の流れももちろんカードの切り方の 1 つなので $\sigma_1 \circ \sigma_2 \in X$ であり，$\circ$ は X 上の演算となる．

集合 X とその集合上の演算 $\circ$ の対 $(X, \circ)$ を**代数系**という．様々な操作は代数系を使って数学的に表現できる．ここではこの代数系の最も基本となる群というものを考える．この群を考えることで様々な現象を群の性質を通して理解することができる．

例 3.3 (例 3.2 の続き)**.** カードの山を何度か同じ切り方をしていくと，必ずもとのカードの山の状態に戻るという事実がある．例えば，例 3.2 で考えた切り方 σ を 3 回すれば上図のように元に戻る．これは $\sigma^3 = 1$ を意味している．ここで 1 は何もしないという切り方である．したがって上の事実はどんな切り方 $\delta \in X$ に対してもある自然数 n で $\delta^n = 1$ となるものが存在することを意味している．これはカードの切り方の集合が有限群という代数構造を持つことから従う．

実はオイラーの定理も同様に証明できる．つまり，群を考えることで，一見全く違う集合の性質を統一的に証明することができる．このことを念頭に置いて群を学習していく．

3.2 群の定義

それでは群の定義を紹介する．

定義 3.4. G を空ではない集合，$\circ$ を G 上の演算とする．このとき，対 $(G, \circ)$ が**群** (group) であるとは，以下の条件を満たすときにいう．

(G1) （結合律）任意の a, b, c に対し，$(a \circ b) \circ c = a \circ (b \circ c)$ が成り立つ．

(G2) （単位元の存在）ある元 e で，任意の元 a に対して $a \circ e = e \circ a = a$ を満たすものが存在する．このとき e を G の $\circ$ に関する**単位元**という．

(G3) （逆元の存在）任意の a に対して，ある元 $h \in G$ が存在して $a \circ h = h \circ a = e$ を満たすものが存在する．このとき，h を a の $\circ$ に関する**逆元**という．また a の逆元を a^{-1} と書く．

演算が文脈から明らかなときは $(G, \circ)$ を単に G と書いて群とみなす．以降，断りがない限り，群 G の演算は $\circ$，単位元は e で表す．

補足 3.5. (1) もし $(G, \circ)$ が (G1) のみを満たすときは**半群** (semigroup) といい，(G1) と (G2) を満たすときは**モノイド** (monoid) という．

(2) 群の演算は基本的に「積」または「乗法」と呼ぶ．また $a \circ b$ を単に ab と書くこともある．さらに $n \in \mathbb{Z}$ に対し

$$a^n = \begin{cases} \underbrace{a \circ a \circ \cdots \circ a}_{n \text{ 個}} & (n > 0) \\ e & (n = 0) \\ \underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{-n \text{ 個}} & (n < 0) \end{cases}$$

と表記する．このとき，任意の整数 n, m に対し

$$a^n \circ a^m = a^{n+m}$$
$$a^{nm} = (a^n)^m$$

が成り立つことは簡単に証明できる．ただし，

$$(a \circ b)^n = a^n \circ b^n$$

は一般に成り立たないことに注意する（$a \circ b = b \circ a$ とは限らないから）．

(3) もし演算の記号として $+$ を使う場合，逆元は a^{-1} の代わりに $-a$ を使うことが多い．またこのとき，a^n の代わりに $n \cdot a$ と書き，$n \cdot a + m \cdot a = (n + m) \cdot a$ が成り立つ．

例 3.6. (1) $\mathbb{Z}$ 上の通常の和 $+$ を考えると，$(\mathbb{Z}, +)$ は群となる．実際，(G1) は明らか．(G2) は $e = 0$ とすると，任意の整数 a に対して，$a + 0 = 0 + a = a$ なので，単位元が存在する．(G3) は整数 a に対して，$-a$ を考えると $a + (-a) = (-a) + (a) = 0 = e$ となり a は逆元を持つ．

(2) $(\mathbb{Z}, \cdot)$ は (G3) が成り立たないので群ではない．実際，$e = 1$ が $\cdot$ に関する単位元となるが，$a = 2$ に対して，$a \cdot b = b \cdot a = 1$ を満たす整数 $b \in \mathbb{Z}$ は存在しない．つまり，2 は逆元を持たないので (G3) が成り立たない．一方，(G1) と (G2) は満たすので，$(\mathbb{Z}, \cdot)$ はモノイドとなる．

(3) $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ とし，$\mathbb{R}^\times$ 上の通常の積 $\cdot$ を考えると，$(\mathbb{R}^\times, \cdot)$ は群となる．(G1) は明らか．(G2) は $e = 1$ とすると，任意の $a \in \mathbb{R}^\times$ に対して，$a \cdot 1 = 1 \cdot a = a$ なので，単位元が存在する．(G3) は $a \in \mathbb{R}^\times$ に対して，$\dfrac{1}{a}$ を考えると $a \cdot \dfrac{1}{a} = \dfrac{1}{a} \cdot a = 1 = e$ となり a は逆元を持つ．

(4) $(\mathbb{N}, +)$ は 0 を自然数とすればモノイド，0 が自然数でないとすれば半群となる．

以降，断らない限り，$\mathbb{Z}$ を群として扱うときは群 $(\mathbb{Z}, +)$ を考える．

定義 3.7. G を群とする．G が**アーベル群** (abelian group) または**可換群** (commutative group) であるとは，条件

(G4)（交換律）任意の $a, b \in G$ に対し $a \circ b = b \circ a$

を満たすときにいう．

群 $(\mathbb{Z}, +)$ や $(\mathbb{R}^\times, \cdot)$ は交換律が成り立つのでアーベル群である．それではアーベル群ではない群の例を見る．

例 3.8. 正則な，つまり逆行列を持つ 2 次正方行列全体の集合を $\mathrm{GL}_2(\mathbb{R})$ と書く．通常の行列の積 $\cdot$ を考えると $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ は群となる（確かめよ）．しかし，(G4) を満たさないのでアーベル群ではない．実際，

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 3 & -2 \end{pmatrix}$$

とすると，$A, B \in \mathrm{GL}_2(\mathbb{R})$ であるが，$AB \neq BA$ である．

3.3 群の基本的性質

次に群の定義の (G1)，(G2)，(G3) から導かれる群の基本的な性質を証明する．

命題 3.9 (単位元と逆元の一意性)**.** G を群とする．

(1) $a, b \in G$ が $a \circ b = a$ (または $b \circ a = b$) を満たすとする．このとき，$b = e$ (または $a = e$) である．特に，G の単位元は一意である．

(2) 任意の $a \in G$ に対し，a の逆元は一意である．

Proof. (1) $a \circ b = a$ の両辺に左から a^{-1} を掛けると，

$$b = e \circ b = a^{-1} \circ a \circ b = a^{-1} \circ a = e$$

である．$b \circ a = b$ の場合は右から b^{-1} を掛けると $a = e$ が従う．

(2) h, h' が a の逆元であるとする．このとき，

$$\begin{cases} a \circ h = h \circ a = e \\ a \circ h' = h' \circ a = e \end{cases}$$

であるので，

$$h = h \circ e = h \circ (a \circ h') = (h \circ a) \circ h' = e \circ h' = h'$$

となり，a の逆元は一意である． □

命題 3.10. G を群とする． このとき，$a, b, c \in G$ に対し以下が成り立つ．

(1) $a \circ b = c$ ならば $a = c \circ b^{-1}$ かつ $b = a^{-1} \circ c$ である．

(2) $a \circ b = a \circ c$ ならば $b = c$ である．

(3) $a \circ c = b \circ c$ ならば $a = b$ である．

(4) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ である．

(5) $(a^{-1})^{-1} = a$ である．

Proof. (1) $a \circ b = c$ の両辺の右から b^{-1} を掛けると

$$\begin{aligned}
(a \circ b) \circ b^{-1} &= c \circ b^{-1} \\
a \circ (b \circ b^{-1}) &= c \circ b^{-1} && ((\mathrm{G1}) \text{ より}) \\
a \circ e &= c \circ b^{-1} && ((\mathrm{G3}) \text{ より}) \\
a &= c \circ^{-1} b && ((\mathrm{G1}) \text{ より})
\end{aligned}$$

となる．同様に，左から a^{-1} を掛けることで $b = a^{-1} \circ c$ を得る．

(2) と (3) は (1) と同様に証明できる．

(4) 示すべきことは $a \circ b$ の逆元が $b^{-1} \circ a^{-1}$ となることである．

$$\begin{aligned}
(a \circ b) \circ (b^{-1} \circ a^{-1}) &= a \circ (b \circ (b^{-1} \circ a^{-1})) && ((\mathrm{G1}) \text{ より}) \\
&= a \circ ((b \circ b^{-1}) \circ a^{-1}) && ((\mathrm{G1}) \text{ より}) \\
&= a \circ (e \circ a^{-1}) && ((\mathrm{G3}) \text{ より}) \\
&= a \circ a^{-1} && ((\mathrm{G2}) \text{ より}) \\
&= e && ((\mathrm{G3}) \text{ より})
\end{aligned}$$

となる．同様に，$(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$ も示せるので，$(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ が成り立つ．

(5) a^{-1} の定義から $a \circ a^{-1} = a^{-1} \circ a = e$ である．これは a が a^{-1} の逆元であることも意味するので，$(a^{-1})^{-1} = a$ である． □

3.4 有限群

定義 3.11. G を群とする．もし G が有限集合なら G を**有限群**という．またこのとき，$|G|$ を G の**位数**という．G が無限集合のときは G を**無限群**という．

G が有限群の場合，$a \circ b$ の計算結果を表にした乗法表（積表）を書くと便利である．つまり，以下のような表である．

$\circ$	$\cdots$	b	$\cdots$
$\vdots$			
a		$a \circ b$	
$\vdots$			

ここまでの群の例はすべて無限群である．有限群の例として最も単純な群を紹介する．

例 3.12. 1 元集合 $G = \{e\}$ を考える．このとき G 上の演算 $\circ$（で表される式）は $e \circ e = e$ しかない．つまり，乗法表は以下のようになる．

$\circ$	e
e	e

このとき，$(G, \circ)$ は群となる（確かめよ）．このような 1 元からなる群を**自明群**という．

例 3.13. 自明群の次に単純な群を見ていく．つまり，$G = \{e, g\}$ という 2 元集合とその演算 $\circ$ を考える．e を単位元とすると，$e \circ g = g \circ e = g$ と $e \circ e = e$ は自動的に決まる．よって $g \circ g = e$ または $g \circ g = g$ となるが，g に逆元が存在しないといけないので，$g \circ g = e$ となる．よって演算 $\circ$ の対応が自動的に決まった．実際，乗法表は以下の通りとなる．

$\circ$	e	g
e	e	g
g	g	e

したがって，位数 2 の有限群は「本質的には」この群しかない．

実は位数 3 の有限群も本質的には 1 つしかない．

例 3.14. $G = \{e, g, h\}$ という 3 元集合とその演算 $\circ$ を考える．e を単位元とする．逆元の一意性から乗法表の各行および各列にはちょうど 1 個 e が入らなければならない．よってもし $g^2 = e$ ならば $h^2 = e$ となる（下図参照）．

$\circ$	e	g	h
e	e	g	h
g	g	e	$\times$
h	h	$\times$	e

しかし，単位元の一意性から $g \circ h \neq g, h$ であるので，乗法表が定まらない．したがって，G の乗法表の可能性は以下の 1 通りのみである．

$\circ$	e	g	h
e	e	g	h
g	g	h	e
h	h	e	g

したがって，位数 3 の有限群は「本質的には」この群しかない．

位数 4 で「本質的に」異なる有限群が現れる．

例 3.15. $G = \{e, a, b, c\}$ という 4 元集合とその演算 $\circ$ を考える．e を単位元とすると．G の乗法表は「本質的には」以下の 2 種類が存在する（$\circ_1$ と $\circ_2$ で分けて書く）．

$\circ_1$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\circ_2$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

違いがわかりにくいかもしれないが，右の表だと $a^2 = b^2 = c^2 = e^2 = e$ となっているが，左の表は $a^2 \neq e$ である．よってこの 2 つの乗法表で定義される群 $(G, \circ_1)$ と $(G, \circ_2)$ は「本質的には」違う有限群である．

「本質的には」同じ群や違う群と表現しているが，この意味は後の章で説明する．

次に代表的な有限アーベル群の例を紹介する．m を 2 以上の自然数とし，$\mathbb{Z}/m\mathbb{Z}$ 上の演算 $+$ を

$$\begin{array}{rccc} +: & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ & \cup & & \cup \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a} + \overline{b} := \overline{a +_{\mathbb{Z}} b} \end{array}$$

で定義する．ただし $+_{\mathbb{Z}}$ は $\mathbb{Z}$ 上の加法である（以降は単に $+$ と書くがどの集合での演算か意識しておこう）．ここで「定義する」と書いたが「矛盾なく」定義できていることを確かめないといけない．実際，この演算は剰余類の代表元に依存した演算となっている．例えば，$m = 3$ のとき，$\overline{-1} = \overline{2}$ であるので $\overline{-1} + \overline{1} = \overline{2} + \overline{1}$ でないといけない．つまり，代表元を入れ替えても答えが変わらないようにうまく定義できているか確認する必要がある．こういった性質を **well-defined 性**という．

命題 3.16. $\mathbb{Z}/m\mathbb{Z}$ 上の演算 $+$ は well-defined である．

Proof. 示すべきことは，任意の剰余類 $\overline{a} = \overline{a'}$ と $\overline{b} = \overline{b'}$ に対し，$\overline{a} + \overline{b} = \overline{a'} + \overline{b'}$ が成り立つことである．$+$ の定義から $\overline{a} + \overline{b} = \overline{a + b}$ かつ $\overline{a'} + \overline{b'} = \overline{a' + b'}$ である．仮定から $a \equiv_m a'$ かつ $b \equiv_m b'$ であるので，この両片を足すと $a + b \equiv_m a' + b'$ が得られる．これは $\overline{a + b} = \overline{a' + b'}$ を意味するので．$\overline{a} + \overline{b} = \overline{a'} + \overline{b'}$ が成り立つ．よって $+$ は well-defined である． □

それではこの演算に対して $\mathbb{Z}/m\mathbb{Z}$ がアーベル群であることを見る．

命題 3.17. $(\mathbb{Z}/m\mathbb{Z}, +)$ は有限アーベル群である．またその位数は m である．

Proof. (G1) 任意の $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/m\mathbb{Z}$ に対し，

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a + b} + \overline{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \overline{a} + (\overline{b + c}) = \overline{a} + (\overline{b} + \overline{c})$$

より結合律が成り立つ．

(G2) $e = \overline{0}$ とすると，任意の $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ に対し，

$$\overline{a} + \overline{0} = \overline{a + 0} = \overline{a} = \overline{0 + a} = \overline{0} + \overline{a}$$

なので，単位元が存在する．

(G3) 任意の $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ に対し，$\overline{-a}$ を考えると，

$$\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0} = \overline{(-a) + a} = \overline{-a} + \overline{a}$$

なので，逆元が存在する．

(G4) 任意の $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$ に対し，

$$\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a}$$

であるので交換律が成り立つ．

また $|\mathbb{Z}/m\mathbb{Z}| = m$ であるので，以上より $(\mathbb{Z}/m\mathbb{Z}, +)$ は位数 m の有限アーベル群である． □

以降，断りがない限り，$\mathbb{Z}/m\mathbb{Z}$ で群 $(\mathbb{Z}/m\mathbb{Z}, +)$ を意味する．

次に $(\mathbb{Z}/m\mathbb{Z})^\times$ を考える．$\mathbb{Z}/m\mathbb{Z}$ と同様に $+$ が定義できそうだが実はできない．実際，$m = 3$ とすると，$(\mathbb{Z}/3\mathbb{Z})^\times = \{\overline{1}, \overline{2}\}$ であるが，$\overline{1} + \overline{2} = \overline{0} \notin (\mathbb{Z}/m\mathbb{Z})^\times$ となる．つまり，演算の結果が同じ集合に属さないの

である．演算の結果がいつでも同じ集合に属するのも well-defined 性では必要となる．そこで，演算 $\cdot$ を考える．$(\mathbb{Z}/m\mathbb{Z})^\times$ 上の演算 $\cdot$ を以下で定義する．

$$\begin{array}{rccc} \cdot : & (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^\times \\ & \cup & & \cup \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a} \cdot \overline{b} := \overline{a \cdot_{\mathbb{Z}} b} \end{array}$$

で定義する．ただし $\cdot_{\mathbb{Z}}$ は $\mathbb{Z}$ 上の乗法である（以降は単に $\cdot$ と書く）．

命題 3.18. $(\mathbb{Z}/m\mathbb{Z})^\times$ 上の演算 $\cdot$ は well-defined である．

Proof. $\overline{a}, \overline{b} \in (\mathbb{Z}/m\mathbb{Z})^\times$ に対して $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ が $(\mathbb{Z}/m\mathbb{Z})^\times$ に属することを示す．これは $a \cdot b$ と m が互いに素であることを意味する．これは a と m が互いに素かつ b と m が互いに素であることから従う．よって $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/m\mathbb{Z})^\times$ である．

次に任意の既約剰余類 $\overline{a} = \overline{a'}$ と $\overline{b} = \overline{b'}$ に対し，$\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b'}$ が成り立つことを示す．$\cdot$ の定義から $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ かつ $\overline{a'} \cdot \overline{b'} = \overline{a' \cdot b'}$ である．仮定から $a \equiv_m a'$ かつ $b \equiv_m b'$ であるので，この両片を掛けると $a \cdot b \equiv_m a' \cdot b'$ が得られる．これは $\overline{a \cdot b} = \overline{a' \cdot b'}$ を意味するので．$\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b'}$ が成り立つ．

以上より $\cdot$ は well-defined である．

□

命題 3.19. $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ は有限アーベル群である．またその位数は $\phi(m)$ である．

Proof. (G1), (G2), (G4) の証明は演習問題とする．ここで単位元は $\overline{1}$ である．

(G3) 任意の $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ をとる．このとき，$\gcd(a, m) = 1$ であるので，$ax + my = 1$ を満たす整数 x, y が存在する．この x に対し，$\gcd(x, m) = 1$ である．実際，$\gcd(x, m) =: d \geq 2$ だと，$ax + my = 1$ の左辺が d の倍数となり，右辺が 1 なので矛盾である．したがって $\overline{x} \in (\mathbb{Z}/m\mathbb{Z})^\times$ である．特に，$ax \equiv_m 1$ であるので，$\overline{a} \cdot \overline{x} = \overline{ax} = \overline{1}$ となることから，$\overline{x}$ は $\overline{a}$ の逆元である．

また $|(\mathbb{Z}/m\mathbb{Z})^\times| = \phi(m)$ であるので，以上より $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ は位数 $\phi(m)$ の有限アーベル群である． □

以降，断りがない限り，$(\mathbb{Z}/m\mathbb{Z})^\times$ で群 $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ を意味する．

3.5 対称群

写像の性質についていくつか復習する．

定義 3.20. 空でない集合 X, Y と写像 $f : X \to Y$ を考える．

(1) f が**単射** (injective) であるとは，任意の $a, b \in X$ に対し，$f(a) = f(b)$ ならば $a = b$ を満たすときにいう．

(2) f が**全射** (surjective) であるとは，任意の $y \in Y$ に対し，$f(x) = y$ を満たす $x \in X$ が存在するときにいう．

(3) f が単射かつ全射のとき，f は**全単射** (bijective) であるという．

空でない集合 X, Y, Z と写像 $f : X \to Y, g : Y \to Z$ に対し，写像 $g \circ f : X \to Z$ を $x \mapsto g(f(x))$ で定義する．このとき，$g \circ f$ を写像 f, g の**合成写像**という．

命題 3.21. 空でない集合 X, Y, Z と写像 $f : X \to Y, g : Y \to Z$ を考える．

(1) f, g がともに単射であれば，$g \circ f$ も単射である．

(2) f, g がともに全射であれば，$g \circ f$ も全射である．

(3) f, g がともに全単射であれば，$g \circ f$ も全単射である．

Proof. (1) 任意の $a, b \in X$ で $(g \circ f)(a) = (g \circ f)(b)$ を満たすものをとる．このとき，$g(f(a)) = g(f(b))$ であり，g の単射性から $f(a) = f(b)$ が成り立つ．また f の単射性から $a = b$ が成り立つ．よって $g \circ f$ は単射である，

(2) 任意の $z \in Z$ をとる．このとき，g の全射性から $z = g(y)$ となる $y \in Y$ が存在する．さらに f の全射性から $y = f(x)$ となる $x \in X$ が存在する．よって

$$z = g(y) = g(f(x)) = (g \circ f)(x)$$

となるので，$z = (g \circ f)(x)$ を満たす $x \in X$ が存在することがわかったので，$g \circ f$ は全射である．

(3) (1) と (2) から従う． □

空でない集合 X に対し，写像

$$\mathrm{id}_X : X \to X$$

を $x \mapsto x$ で定義する．この写像 id_X を X の**恒等写像**という．また写像 $f : X \to Y$ に対し，写像 $g : Y \to X$ で

$$g \circ f = \mathrm{id}_X, \qquad f \circ g = \mathrm{id}_Y$$

を満たすものが存在するとき，g を f の**逆写像**といい，f^{-1} と書く．

命題 3.22. 空でない集合 X, Y と写像 $f : X \to Y$ を考える．このとき，f が全単射である必要十分条件は f の逆写像が存在することである．特に，逆写像は全単射である．

Proof. （⇒）f が全単射であるとする．任意の $y \in Y$ をとる．f が全射であるので $f(x_y) = y$ を満たす $x_y \in X$ が存在する．さらに f が単射であるので，この x_y は y に対して一意に定まる．すると，$y \mapsto g(y) = x_y$ という対応で写像 $g : Y \to X$ が定義できる．このとき，任意の x に対し $f(x_{f(x)}) = f(x)$ であり，f が単射なので $x_{f(x)} = x$ である．特に，

$$(g \circ f)(x) = g(f(x)) = x_{f(x)} = x$$

であるので，$g \circ f = \mathrm{id}_X$ となる．また任意の $y \in Y$ に対し，

$$(f \circ g)(y) = f(g(y)) = f(x_y) = y$$

であるので $f \circ g = \mathrm{id}_Y$ となる．よって f は逆写像 g を持つ．

（⇐）f が逆写像 f^{-1} を持つとする．任意の $a, b \in X$ で $f(a) = f(b)$ となるものをとる．すると，

$$a = \mathrm{id}_X(a) = (f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(f(b)) = (f^{-1} \circ f)(b) = \mathrm{id}_X(b) = b$$

であるので f は単射である．次に任意の $y \in Y$ をとる．$x = f^{-1}(y) \in X$ とする．このとき，

$$f(x) = f(f^{-1})(y) = (f \circ f^{-1})(y) = \mathrm{id}_Y(y) = y$$

となるので，$f(x) = y$ を満たす $x \in X$ が存在するので f は全射である．よって f は全単射である． □

空でない集合 X に対し，$\mathfrak{S}_X$ を X から X への全単射写像全体の集合とする．つまり

$$\mathfrak{S}_X := \{ f : X \to X \mid f \text{ は全単射} \}$$

このとき，命題 3.21 から写像の合成 $\circ$ は $\mathfrak{S}_X$ 上の演算を定義する．

命題 3.23. $(\mathfrak{S}_X, \circ)$ は群である．この群 $\mathfrak{S}_X$ を X の**対称群** (symmetric group) とよぶ.

Proof. 写像の合成は結合律を満たすので (G1) が従う．恒等写像 id_X が単位元となるので (G2) が従う．任意の $\sigma \in \mathfrak{S}_X$ に対し，$\sigma^{-1} \in \mathfrak{S}_X$ であり，これが逆元であるので (G3) が従う．以上より，$(\mathfrak{S}_X, \circ)$ は群である． □

補足 3.24. $\mathfrak{S}_X$ を考える際，全単射写像 $\sigma \in \mathfrak{S}_X$ を X の**置換**とも呼ぶ．また恒等写像や逆元をそれぞれ**恒等置換**や**逆置換**と呼ぶ．さらに合成写像を**置換の積**ともいう.

一般に写像の合成は可換ではない．つまり $\sigma \circ \tau \neq \tau \circ \sigma$ となるときがある．よって一般には対称群はアーベル群とはならない.

以降，X が有限集合の場合を考える．$X = \{1, 2, \ldots, n\}$ とし，$\mathfrak{S}_X$ を $\mathfrak{S}_n$ と書く．このとき $\mathfrak{S}_n$ を n **次対称群**と呼ぶ．$\sigma \in \mathfrak{S}_n$ をとると，$\sigma(1), \ldots, \sigma(n)$ の中には $1, \ldots, n$ がちょうど 1 度ずつ現れる．つまり，$\sigma(1), \ldots, \sigma(n)$ は $1, \ldots, n$ の並び替え（置換）だと思うことができる．数列 $1, \ldots, n$ を数列 $\sigma(1), \ldots, \sigma(n)$ に移すことを

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

と表すことにして，σ と同一視する．また列を入れ替えたものは同じ置換を表すとする．例えば,

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

である．こうすることで，σ の逆置換は

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

となることがわかる.

例 3.25. $n = 3$ の場合を考える．このとき,

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

となる．置換の積 $\tau \circ \sigma$ は結局 σ で数字を入れ替えた後に τ で数字を入れ替えることを意味する．例えば,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 2 & 1 & 3 \end{pmatrix}$$

とすると $\tau \circ \sigma$ は

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

となる．一方,

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

であるので，$\tau \circ \sigma \neq \sigma \circ \tau$ となる．よって $(\mathfrak{S}_3, \circ)$ は非可換な有限群である.

例 3.2 と 3.3 でカードの山を切ることを考えた．結局カードを切るということはカードの順番を並び替えることに他ならないので,

$$8 \text{ 枚のカードの切り方全体の集合} = \mathfrak{S}_8$$

となることがわかる．したがってカードの山を切るという操作を置換であると認識することで，群の中で扱うことが可能となる.

3.6 直積群

2 つの群から新たに群を構成することができる．$(G_1, \circ_1)$ と $(G_2, \circ_2)$ を単位元をそれぞれ e_1 と e_2 とする群とする．今，直積 $G_1 \times G_2$ 上の演算 $\circ$ を以下で定義する．

$$\circ : (G_1 \times G_2) \times (G_1 \times G_2) \to G_1 \times G_2; ((a_1, b_1), (a_2, b_2)) \mapsto (a_1 \circ_1 a_2, b_1 \circ_2 b_2).$$

命題 3.26. $(G_1 \times G_2, \circ)$ は単位元を (e_1, e_2) とする群である．

Proof. 演習問題とする． □

例 3.27. 直積群 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ を考える．ただし，演算の記号として $+$ を使う．これは以下の乗法表で定義される群である．

$+$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$

$\longleftrightarrow$

$\circ_2$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

今，$(\overline{0},\overline{0}) = e, (\overline{1},\overline{0}) = a, (\overline{0},\overline{1}) = b, (\overline{1},\overline{1}) = c$ とすると，$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ は例 3.15 で考えた $(G, \circ_2)$ に他ならない．一方で，同様に乗法表を比べることで $(G, \circ_1)$ は $\mathbb{Z}/4\mathbb{Z}$ と同一視することができる．したがって，例 3.15 で説明していたことは，$\mathbb{Z}/4\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が「本質的には」違う有限群であるということである．しかし，実は $\mathbb{Z}/6\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ は「本質的には」同じ有限群である．つまり，この 2 つの群の乗法表は同じ形をしている．より詳しい説明は後の節で行う．

4　部分群と巡回群

4.1　部分群の定義

$(G,\circ)$ を群とする．G の空でない部分集合 H に対し，写像

$$\circ|_H : H\times H\to G, (a,b)\mapsto a\circ b$$

を定義する．つまり，G の演算 $\circ$ を H の元のみで考えてることになるが，$a\circ b\notin H$ となる可能性もあるので $\circ|_H$ が H 上の演算になるとは限らない．もし $\circ|_H$ が H 上の演算となる，つまり $\circ|_H : H\times H\to H$ として定義でき，$(H,\circ|_H)$ が群となるとき，H を G の**部分群** (subgroup) という．まず，部分群 H の単位元や逆元が G から引き継がれることを見る．

補題 4.1. G を群とし，H を G の部分群とする．

(1) e と e' をそれぞれ G と H の単位元とする．このとき，$e=e'$ である．特に $e\in H$ である．

(2) 任意の $a\in H$ に対し，a^{-1} と a' をそれぞれ G と H の中での a の逆元とする．このとき，$a^{-1}=a'$ である．特に，$a^{-1}\in H$ である．

Proof. (1) e' が H の単位元であるので，ある（任意の）$h\in H\subset G$ に対し，

$$a=a\circ|_H e'=a\circ e'$$

が成り立つ．よって G の単位元の一意性から $e=e'$ が従う．

(2) (1) から

$$e=a\circ|_H a'=a\circ a'$$

である．G の逆元の一意性から $a^{-1}=a'$ が従う． □

この補題を使うことで以下の命題が示せる．この命題を部分群の定義と思ってもよい．

命題 4.2. G を群とする．このとき，空でない部分集合 $H\subset G$ が G の部分群である必要十分条件は以下の条件を満たすときにいう．

(H1)（逆元に関して閉じている）任意の $a\in H$ に対し，$a^{-1}\in H$ である．

(H2)（演算に関して閉じている）任意の $a,b\in H$ に対し，$a\circ b\in H$ である．

Proof.（⇒）$(H,\circ|_H)$ が G の部分群であるとする．このとき，$\circ|_H$ が H 上の演算となるので，任意の $a,b\in H$ に対し $a\circ|_H b\in H$ となる．よって (H2) を満たす．また補題 4.1 から (H1) が従う．

（⇐）(H1)，(H2) を満たすとする．(H2) は $\circ|_H$ が H 上の演算として定義できることを意味している．このとき，$(H,\circ|_H)$ が (G1)，(G2)，(G3) を満たすことを言えばよい．$\circ$ は結合律を満たすので，制限した $\circ|_H$ も結合律を満たす．よって (G1) が従う．また $H\neq\emptyset$ より $a\in H$ がとれる．このとき，(H1) から $a^{-1}\in H$ である．さらに，(H2) から $a\circ a^{-1}=e\in H$ である．e が G の単位元であることから，e が H の単位元になっていることが従う．よって (G2) が満たされる．再び (H1) より (G3) も満たされる．以上から $(H,\circ|_H)$ は群となる．よって H は G の部分群である． □

系 4.3. G を群とする．このとき，空でない部分集合 $H\subset G$ が G の部分群である必要十分条件は以下の条件を満たすときにいう．

(H) 任意の $a,b\in H$ に対し，$a\circ b^{-1}\in H$ である．

Proof. (H1)，(H2) を満たすなら (H) を満たすことは明らか．(H) を満たすと仮定する．(H) の $a = b$ のときを考えると，$a \circ a^{-1} = e \in H$ である．よって $a = e$ を考えると任意の $b \in H$ に対し $b^{-1} = e \circ b^{-1} \in H$ であるので (H1) を満たす．さらに，任意の $a, b^{-1} \in H$ に対し，$a \circ b = a \circ (b^{-1})^{-1} \in H$ であるので (H2) も満たす． □

以降，H が群 $(G, \circ)$ の部分群のとき，H 上の演算 $\circ|_H$ を単に $\circ$ と書くことにする．

例 4.4. G を群とする．このとき，$\{e\}$ は明らかに G の部分群である．また自分自身 G ももちろん G の部分群である．この 2 つの部分群を G の**自明な部分群**という．

例 4.5. 群 $(\mathbb{Z}, +)$ を考える．

(1) 任意の整数 n に対し，$n\mathbb{Z}$ は $\mathbb{Z}$ の部分群である．実際， (H) 任意の $nx, ny \in n\mathbb{Z}$ $(x, y \in \mathbb{Z})$ に対し，$nx + (-ny) = n(x - y) \in n\mathbb{Z}$ である．

(2) 部分集合 $H = \{2x + 1 : x \in \mathbb{Z}\} \subset \mathbb{Z}$ は $\mathbb{Z}$ の部分群ではない．これは H が (H1)，(H2) のいずれかの一つでも満たさないことを見ればよい．実際，$1, 3 \in H$ だが $1 + 3 = 4 \notin H$ なので (H2) を満たさない．

4.2 巡回群

命題 4.6. 群 G と $a \in G$ に対し，集合

$$\langle a \rangle := \{a^n : n \in \mathbb{Z}\} \subset G$$

を考える．このとき，$\langle a \rangle$ は G の部分群である．

Proof. 任意の $x, y \in \langle a \rangle$ をとる．このとき，整数 n, m を使って，$x = a^n, y = a^m$ と書ける．y の逆元は $y^{-1} = a^{-m}$ である．このとき，

$$x \circ y^{-1} = a^n \circ a^{-m} = a^{n-m}$$

であり，$n - m \in \mathbb{Z}$ なので $x \circ y^{-1} \in \langle a \rangle$ となる．よって (H) を満たすので，$\langle a \rangle$ は G の部分群である． □

定義 4.7. 群 G が**巡回群** (cyclic group) であるとは，ある元 $a \in G$ で

$$G = \langle a \rangle$$

となるものが存在するときにいう．このとき，a を巡回群 G の**生成系**という．

例 4.8. 群 $\mathbb{Z}/4\mathbb{Z}$ と群 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ を考える．ここで，$\overline{a} \in \mathbb{Z}/4\mathbb{Z}$ に対し，

$$\langle \overline{a} \rangle = \{n \cdot \overline{a} : n \in \mathbb{Z}\} \subset \mathbb{Z}/4\mathbb{Z}$$

であることに注意する．まず $\mathbb{Z}/4\mathbb{Z}$ は $\overline{1}$ を生成系とする巡回群である．実際,

$$\mathbb{Z}/4\mathbb{Z} = \{0 \cdot \overline{1}, 1 \cdot \overline{1}, 2 \cdot \overline{1}, 3 \cdot \overline{1}\} = \langle \overline{1} \rangle$$

である．また $\overline{3}$ も $\mathbb{Z}/4\mathbb{Z}$ の巡回群としての生成系となる．実際,

$$1 \cdot \overline{3} = \overline{3},$$
$$2 \cdot \overline{3} = \overline{2},$$
$$3 \cdot \overline{3} = \overline{1},$$
$$4 \cdot \overline{3} = \overline{0}$$

なので，

$$\mathbb{Z}/4\mathbb{Z} = \{1\cdot\overline{3}, 2\cdot\overline{3}, 3\cdot\overline{3}, 4\cdot\overline{3}\} = \langle\overline{3}\rangle$$

である．これらから巡回群の生成系は一意的でないことがわかる．

一方，$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ は巡回群ではない．これを確かめる．整数 $n\in\mathbb{Z}$ と元 $(\overline{a},\overline{b})\in\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ に対し，

$$n\cdot(\overline{a},\overline{b}) := (n\cdot\overline{a}, n\cdot\overline{b})$$

と表記する．すると，

$$\langle(\overline{a},\overline{b})\rangle = \{n\cdot(\overline{a},\overline{b}) : n\in\mathbb{Z}\} \subset \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$$

と表される．このとき，

$$2\cdot(\overline{0},\overline{0}) = 2\cdot(\overline{1},\overline{0}) = 2\cdot(\overline{0},\overline{1}) = 2\cdot(\overline{1},\overline{1}) = (\overline{0},\overline{0})$$

であるので，$n\cdot(\overline{1},\overline{0}) = (\overline{0},\overline{1})$ を満たす整数 n は存在しない．よって $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \neq \langle(\overline{1},\overline{0})\rangle$ である．同様に，$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \neq \langle(\overline{0},\overline{1})\rangle$ と $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \neq \langle(\overline{1},\overline{1})\rangle$ もわかるので，$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ は巡回群ではない．

$\mathbb{Z}/4\mathbb{Z}$ は巡回群であったが $\mathbb{Z}/m\mathbb{Z}$ はいつでも巡回群である．

命題 4.9. $\mathbb{Z}/m\mathbb{Z}$ は巡回群である．

Proof. 整数 n に対して，$n\cdot\overline{1} = \overline{n}$ なので，

$$\mathbb{Z}/m\mathbb{Z} = \{n\cdot\overline{1} : n\in\mathbb{Z}\} = \langle\overline{1}\rangle$$

となるから $\mathbb{Z}/m\mathbb{Z}$ は $\overline{1}$ を生成系とする巡回群である． □

一方で，$(\mathbb{Z}/m\mathbb{Z})^\times$ は巡回群になるとは限らない．

例 4.10. $(\mathbb{Z}/8\mathbb{Z})^\times$ を考える．このとき，$(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1},\overline{3},\overline{5},\overline{7}\}$ である．$\overline{1}^2 = \overline{3}^2 = \overline{5}^2 = \overline{7}^2 = \overline{1}$ となっているので，例 4.8 と同様に考えると $(\mathbb{Z}/8\mathbb{Z})^\times$ は巡回群にならないことがわかる．

4.3 元の位数

定義 4.11. G を群とする．元 $a\in G$ に対し，$a^n = e$ を満たす最小の自然数 n を a の**位数**といい，$\mathrm{ord}(a)$ と書く．もしそのような自然数が存在しない場合，$\mathrm{ord}(a) = \infty$ と書くことにする．逆に存在する場合は $\mathrm{ord}(a) < \infty$ と表現する．

補足 4.12. 元 a の位数は巡回群 $\langle a\rangle$ の位数として定義してもよい．つまり，

$$\mathrm{ord}(a) = |\langle a\rangle|$$

である．

例えば，群 $(\mathbb{Z},+)$ において，$\mathrm{ord}(2) = \infty$ である．実際，任意の自然数 n に対して $2n > 0$ である．一方，$((\mathbb{Z}/5\mathbb{Z})^\times,\cdot)$ において，$\mathrm{ord}(\overline{2}) = 4$ や $\mathrm{ord}(\overline{4}) = 2$ となる（確かめよ）．

簡単な位数の性質を見ていく．

命題 4.13. G を群とし，元 $a\in G$ の位数が n，つまり $\mathrm{ord}(a) = n < \infty$ とする．このとき，整数 m に対し，$a^m = e$ である必要十分条件は $n|m$ である．特に，$\mathrm{ord}(a^{-1}) = n$ である．

Proof. （⇒）m を n で割った商と余りを q, r とする．つまり，$m = nq + r$ で $0 \leq r < n$ である．すると仮定より，

$$e = a^m = a^{nq+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = e \cdot a^r = a^r$$

となる．このとき，$\mathrm{ord}(a) = n$ から $r = 0$ でなければならない．実際，$0 < r < n$ で $a^r = e$ となれば $r < n$ で a の位数より小さい自然数で $a^r = e$ となってしまい矛盾する．よって $m = nq$ なので，$n|m$ が従う．

（⇐）$n|m$ からある整数 k を用いて $m = nk$ と書ける．すると

$$a^m = a^{nk} = (a^n)^k = e^k = e$$

である．

$-n|n$ より $(a^{-1})^n = a^{-n} = e$ となることから，$\mathrm{ord}(a^{-1}) \leq n = \mathrm{ord}(a)$ である．よって $\mathrm{ord}(a^{-1}) < \infty$ より，同様に考えると，$\mathrm{ord}(a^{-1}) \geq \mathrm{ord}(a) = n$ が言えるので，$\mathrm{ord}(a^{-1}) = n$ が従う． □

例えば，$((\mathbb{Z}/5\mathbb{Z})^\times, \cdot)$ において $\mathrm{ord}(\overline{2}) = 4$ だったので，$\overline{2}^{10} = \overline{2}^8 \cdot \overline{2}^2 = \overline{1} \cdot \overline{4} = \overline{4}$ のように計算でき，$\overline{2}^{-1} = \overline{3}$ なので，$\mathrm{ord}(\overline{3}) = 4$ もわかる．

無限群では位数が無限となる元が存在したが，有限群ではどの元の位数も有限である．

命題 4.14. G を有限群とする．このとき，任意の $a \in G$ に対し，$\mathrm{ord}(a) < \infty$ である．

Proof. G が有限群であるので，無限列

$$a, a^2, a^3, a^4, \ldots$$

の中で同じ 2 つの元が存在する．それを a^n, a^m $(n < m)$ とする．$a^n = a^m$ の両辺の左から a^{-n} を掛けると

$$e = a^0 = a^{-n} \circ a^n = a^{-n} \circ a^m = a^{m-n}$$

となり，$m - n > 0$ であるので，$\mathrm{ord}(a) \leq m - n < \infty$ が成り立つ． □

さて，例 3.3 で，カードの山を何度か同じ切り方をしていくと，必ず元のカードの山の状態に戻るという事実があると紹介した．これまでの結果からこれが証明できる．実際，n 枚のカードの山の切り方全体の集合というのは n 次対称群と思うことができた．あるカードの切り方を何度か繰り返すというのは，$\sigma \in \mathfrak{S}_n$ を使って σ^r と表現できる．$\mathfrak{S}_n$ は有限群なので命題 4.14 から $\sigma^r = \mathrm{id}_n$ となる自然数 r が存在する．これは σ を r 回繰り返せば元の状態に戻ることを意味するので事実が確かめられた．後の章で，$\mathrm{ord}(a)$ は有限だけでなく，もう少し性質がわかることを示し，オイラーの定理の証明へ繋ぐ．

最後に元の位数を計算するのに便利な命題を証明する．

命題 4.15. G を群とし，元 $a \in G$ の位数が n，つまり $\mathrm{ord}(a) = n < \infty$ とする．このとき，自然数 k に対し，

$$\mathrm{ord}(a^k) = \frac{n}{\gcd(n, k)}$$

が成り立つ．

Proof. $\gcd(n, k) = d$ とおくと，整数 n', k' を用いて $n = n'd, k = k'd$ と書ける．このとき，$\gcd(n', k') = 1$ である．示すことは $\mathrm{ord}(a^k) = n'$ である．まず，

$$(a^k)^{n'} = (a^k)^{\frac{n}{d}} = (a^n)^{\frac{k}{d}} = e^{k'} = e$$

であるから，$\mathrm{ord}(a^k) \leq n'$ である．$\mathrm{ord}(a^k) = m$ とすると，$e = (a^k)^m = a^{km}$ と命題 4.13 から $n|km$ である．すると $n'd|k'dm$ であるので，$n'|k'm$ となるが，$\gcd(n', k') = 1$ から $n'|m$ である．よって $n' \leq m$ であるので，$n' \leq m = \mathrm{ord}(a^k) \leq n'$ となり，$\mathrm{ord}(a^k) = n'$ がわかる． □

5　準同型写像と同型

ここまで群が「本質的に」同じといった表現をしていたが，正確な定義を述べていく．

5.1　準同型写像

一般に，2 つの集合を比べるとき，その集合間の写像を考えることは基本である．しかし，単なる集合ではなく，群として比べたいときは，特別な写像を考える．

定義 5.1. $(G_1, \circ_1), (G_2, \circ_2)$ を群とする．写像 $f : G_1 \to G_2$ が（群）**準同型写像** (homomorphism) であるとは，任意の $a, b \in G_1$ に対し，

$$f(a \circ_1 b) = f(a) \circ_2 f(b)$$

を満たすときにいう．

乗法表で見ると，準同型写像というのは，写像で移る前の演算の対応と，移った先の演算の結果が一致しているということである．

$\circ_1$	$\cdots$	b	$\cdots$
$\vdots$			
a		$a \circ_1 b$	
$\vdots$			

$\xrightarrow{f}$

$\circ_2$	$\cdots$	$f(b)$	$\cdots$
$\vdots$			
$f(a)$		$f(a \circ_1 b)$?	
$\vdots$			

したがって，準同型写像というのはもと群の群構造を保つ写像ということがわかる．以降，断りがない限り，G_1 と G_2 の演算をそれぞれ $\circ_1, \circ_2$，単位元をそれぞれ e_1, e_2 で表す．
例を見る前に，準同型写像の大事な性質として，単位元や逆元が保たれていることを見る．

命題 5.2. G_1, G_2 を群とし，$f : G_1 \to G_2$ を準同型写像とする．このとき，以下が成り立つ．

(1) $f(e_1) = e_2$ である．

(2) 任意の $a \in G_1$ に対し，$f(a^{-1}) = f(a)^{-1}$ である．

Proof. (1) $e_1 \circ_1 e_1 = e_1$ より，

$$f(e_1) = f(e_1 \circ_1 e_1) = f(e_1) \circ_2 f(e_1)$$

である．したがって G_2 における単位元の一意性から $f(e_1) = e_2$ となる．
(2) 示すべきことは $f(a)$ の逆元が $f(a^{-1})$ となることである．これは

$$f(a) \circ_2 f(a^{-1}) = f(a \circ_1 a^{-1}) = f(e_1) = e_2$$
$$f(a^{-1}) \circ_2 f(a) = f(a^{-1} \circ_1 a) = f(e_1) = e_2$$

から従う． □

それでは準同型写像の例をいくつか見ていこう．

例 5.3. (1) 群 G_1, G_2 に対し，$f : G_1 \to G_2$ を $g \mapsto e_2$ で定義する．つまり，全ての元が G_2 の単位元に移るような写像を考える．すると任意の $a, b \in G_1$ に対し，

$$f(a \circ_1 b) = e_2 = e_2 \circ_2 e_2 = f(a) \circ_2 f(b)$$

が成り立つので，f は準同型写像である．これを自明な準同型写像という．

(2) 2 倍写像 $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto 2x$ を考えよう．任意の $x, y \in \mathbb{Z}$ に対し，

$$f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$$

であるので，f は準同型写像である．

(3) 写像 $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto x + 2$ を考える．このとき，

$$f(1+1) = f(2) = 2 + 2 = 4 \neq (1+2) + (1+2) = f(1) + f(1)$$

より，任意の $x, y \in \mathbb{Z}$ に対し，$f(x+y) = f(x) + f(y)$ が成り立つとは限らない．よって f は準同型写像ではない．

(4) 正則な 2 次正方行列全体の集合 $\mathrm{GL}_2(\mathbb{R})$ は行列の積に関して群であった．また $(\mathbb{R}^\times, \cdot)$ も群であった．写像 $f : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^\times$ を $A \mapsto \det A$ で定義する．ここで $\det A$ は A の行列式を表す．このとき，任意の $A, B \in \mathrm{GL}_2(\mathbb{R})$ に対し，$\det AB = \det A \cdot \det B$ であったことを思い出すと，

$$f(AB) = \det AB = \det A \cdot \det B = f(A) \cdot f(B)$$

が成り立つので，f は準同型写像である．

写像 $f : G_1 \to G_2$ があったとき，元 $x \in G_1$ に対し，$f(x) \in G_2$ を x の f に関する**像** (image) と呼ぶ．また像全体の集合

$$\mathrm{Im}(f) := \{f(x) \in G_2 : x \in G_1\}$$

を f の**像**と呼ぶ．一般に G_1, G_2 が群であったとしても $\mathrm{Im}(f)$ が群になるとは限らない．しかし，f が準同型写像であればいつでも $\mathrm{Im}(f)$ は群となる．

命題 5.4. G_1, G_2 を群とし，$f : G_1 \to G_2$ を準同型写像とする．このとき $\mathrm{Im}(f)$ は G_2 の部分群である．

Proof. 任意の $f(x), f(y) \in \mathrm{Im}(f)$ $(x, y \in G_1)$ をとる．このとき，

$$f(x) \circ_2 f(y)^{-1} = f(x) \circ_2 f(y^{-1}) = f(x \circ y^{-1}) \in \mathrm{Im}(f)$$

であるので，$\mathrm{Im}(f)$ は G_2 の部分群である． □

したがって $f : G_1 \to G_2$ が準同型写像であれば，$\mathrm{Im}(f)$ は G_1 の群構造を「ある程度」引き継いだ G_2 の部分群であることがわかる．特に，$\mathrm{Im}(f)$ はもとの群 G_1 の性質を引き継ぐことが多い．例えば，以下のような性質がある．

命題 5.5. G_1, G_2 を群とし，$f : G_1 \to G_2$ を準同型写像とする．このとき，G_1 が巡回群であれば，$\mathrm{Im}(f)$ も巡回群である．

Proof. 任意の $x \in G_1$ と整数 n に対して，f の準同型性から

$$f(x^n) = (f(x))^n$$

となることがわかる．今，$a \in G_1$ を使って $G_1 = \langle a \rangle$ と書けるとする．すると，

$$\mathrm{Im}(f) = \{f(x) : x \in G_1\} = \{f(a^n) : n \in \mathbb{Z}\} = \{(f(a))^n : n \in \mathbb{Z}\} = \langle f(a) \rangle$$

となり，$\mathrm{Im}(f)$ が巡回群であることがわかった． □

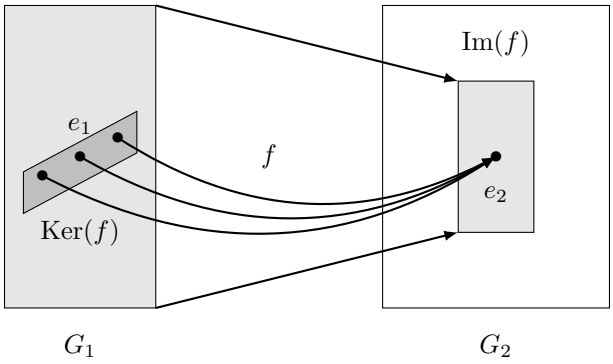
準同型写像 $f : G_1 \to G_2$ に対して，$\mathrm{Im}(f)$ は G_1 の群構造を「ある程度」引き継ぐといったが，これは一部の群構造が「潰れる」ときがあるのでこのように表現した．実際，自明な準同型写像を考えると，全てが単位元に飛ぶので群構造がほとんど「潰れる」のがわかるだろう．この「潰れる」元全体の集合を考える．

定義 5.6. G_1, G_2 を群とし，$f : G_1 \to G_2$ を準同型写像とする．このとき，集合

$$\mathrm{Ker}(f) := \{x \in G_1 : f(x) = e_2\} \subset G_1$$

を f の**核** (kernel) という．

下図のように，$\mathrm{Ker}(f)$ とは単位元 1 点に圧縮される集合のことである．



実は $\mathrm{Ker}(f)$ も群構造を持つ．

命題 5.7. G_1, G_2 を群とし，$f : G_1 \to G_2$ を準同型写像とする．このとき $\mathrm{Ker}(f)$ は G_1 の部分群である．

Proof. 任意の $x, y \in \mathrm{Ker}(f)$ をとる．このとき $f(x) = f(y) = e_2$ である．また $f(y^{-1}) = f(y)^{-1} = e_2^{-1} = e_2$ である．すると

$$f(x \circ_1 y^{-1}) = f(x) \circ_2 f(y^{-1}) = e_2 \circ_2 e_2 = e_2$$

であるので，$x \circ_1 y^{-1} \in \mathrm{Ker}(f)$ が従う．よって $\mathrm{Ker}(f)$ は G_1 の部分群である． □

f が準同型写像の場合，$\mathrm{Ker}(f)$ を調べることで f が単射かどうか判定できる．

命題 5.8. 準同型写像 $f : G_1 \to G_2$ が単射である必要十分条件は $\mathrm{Ker}(f) = \{e_1\}$ である．

Proof. （⇒）$x \in \mathrm{Ker}(f)$ とすると，

$$f(x) = e_2 = f(e_1)$$

である．f が単射であるので，$x = e_1$ が成り立ち，$\mathrm{Ker}(f) = \{e_1\}$ が従う．
（⇐）任意の $x, y \in G_1$ で $f(x) = f(y)$ を満たすものをとる．このとき，f の準同型性より

$$e_2 = f(x) \circ_2 f(x^{-1}) = f(y) \circ_2 f(x^{-1}) = f(y \circ_1 x^{-1})$$

である．よって $y \circ_1 x^{-1} \in \mathrm{Ker}(f) = \{e_1\}$ が成り立つので，$y \circ_1 x^{-1} = e_1$ となり，$y = x$ を得る．よって f は単射である． □

この命題から，$\mathrm{Im}(f)$ が潰れないことと f が単射であることが同値であることがわかる．

5.2　同型写像と同型

準同型写像 $f : G_1 \to G_2$ により G_2 の中で，G_1 の群構造をある程度引き継いだ部分群 $\mathrm{Im}(f)$ を見つけることができる．ということは，$\mathrm{Im}(f)$ が潰れずに，それが G_2 全体，つまり，$\mathrm{Im}(f) = G_2$ となれば，G_1 と G_2 が同じ群構造を持つと思うことができる．命題 5.8 からこれは f が全単射であることと同値である．こういった状況を群が「本質的に同じ」と考える．それでは正式な用語を使いこれらを定義する．

定義 5.9. 群 G_1, G_2 と準同型写像 $f : G_1 \to G_2$ を考える．f が**同型写像** (isomorphism) であるとは，f が全単射となるときにいう．また G_1 から G_2 への同型写像が存在するとき，G_1 は G_2 と**同型** (isomorphic) であるといい，$G_1 \cong G_2$ と書く．

命題 5.10. $f : G_1 \to G_2$ が同型写像であれば，その逆写像も同型写像である．したがって，G_1 が G_2 に同型ならば，G_2 は G_1 に同型である．よって単に G_1 と G_2 は同型であるといってよい．

Proof. 示すべきことは，$f^{-1} : G_2 \to G_1$ が準同型写像であることである．任意の $a, b \in G_2$ をとる．$f \circ f^{-1} = \mathrm{id}_{G_2}$ および f が準同型写像であることから

$$f(f^{-1}(a) \circ_1 f^{-1}(b)) = (f \circ f^{-1})(a) \circ_2 (f \circ f^{-1})(b) = a \circ_2 b = (f \circ f^{-1})(a \circ_2 b) = f(f^{-1}(a \circ_2 b))$$

が成り立つ．よって f が単射であることから

$$f^{-1}(a) \circ_1 f^{-1}(b) = f^{-1}(a \circ_2 b)$$

が従う．よって f^{-1} は準同型写像である． □

それでは例を見ていこう．

例 5.11. 群 $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ と $(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ に対して，写像 $f : \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/5\mathbb{Z})^\times$ を

$$\overline{0} \mapsto \overline{1}, \overline{1} \mapsto \overline{2}, \overline{2} \mapsto \overline{4}, \overline{3} \mapsto \overline{3},$$

で定義する．手計算により f が準同型写像であることがわかる．また定義から明らかに f は全単射である．よって f は同型写像であるので，$\mathbb{Z}/4\mathbb{Z}$ と $(\mathbb{Z}/5\mathbb{Z})^\times$ は同型となることがわかった．実際，この 2 つの群の乗法表を書いてみると，全く同じ法則になっていることがわかる．これが同型の意味である．

$\mathbb{Z}/4\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$(\mathbb{Z}/5\mathbb{Z})^\times$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{4}$

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

次に位相が小さい群について見ていこう．

命題 5.12. G を位数 2 の有限群とする．このとき，

$$G \cong \mathbb{Z}/2\mathbb{Z}$$

である．

Proof. $G = \{e, g\}$ とする．G の例 3.13 の乗法表で定義されていることを思い出そう．写像 $f : \mathbb{Z}/2\mathbb{Z} \to G$ を $\overline{0} \mapsto e$ と $\overline{1} \mapsto g$ で定義する．このとき，f は同型写像である．実際，全単射性は定義から明らかで，準同型性は 4 通りを全て考えればよい． □

この命題は，位数 2 の群構造はただ 1 つしかないことを意味する．したがって，位数 2 の群を考えるときは $\mathbb{Z}/2\mathbb{Z}$ として考えても問題ないことになる．

同様に以下の命題も簡単に示せる．

命題 5.13. G を位数 3 の有限群とする．このとき，

$$G \cong \mathbb{Z}/3\mathbb{Z}$$

である．

Proof. 演習問題とする． □

位数が違えば，集合間に全単射写像は存在しないのでもちろん同型ではない．しかし，位数が同じであっても同型にならない群が存在する．それが $\mathbb{Z}/4\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ である．この 2 つの群が同型でないことを定義通り見るためには $\mathbb{Z}/4\mathbb{Z}$ から $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ への同型写像がないことを示せばよい．今回の場合は位数が小さい有限群なのですべての可能性（写像）を考えればよいが，もっと大きい群の場合，この方法は現実的ではない．同型というのは群として同じということだった．つまり，２つの群が違う性質を持てば同型でないことは想像できるだろう．実際，$\mathbb{Z}/4\mathbb{Z}$ は巡回群であり，$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ は巡回群でなかった．実は，この事実から，この 2 つの群が同型でないことがわかる．

命題 5.14. G_1 と G_2 が同型な群であるとする．このとき，G_1 が巡回群であることと，G_2 が巡回群であることは同値である．

Proof. $f : G_1 \to G_2$ を同型写像とする．このとき，$\mathrm{Im}(f) = G_2$ である．よって命題 5.5 より G_1 が巡回群であれば G_2 も巡回群である．f^{-1} を考えれば逆も示せる． □

系 5.15. $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ である．

6　剰余類と剰余群

群 $\mathbb{Z}$ とその部分群 $m\mathbb{Z}$ から剰余類 $\mathbb{Z}/m\mathbb{Z}$ が構成できた．この概念を一般の群に拡張する．

6.1　剰余類

商集合の性質を少し復習する．集合 X とその同値関係 $\sim$ に対し，$a \in X$ の同値類 $[a]_\sim$ というのは，a と同値な X の元全体の集合，つまり，$\{b \in X : a \sim b\}$ であった．これは，a と何らかの意味で等しいものでグループを作るということである．そのグループを集めた集合が商集合 $X/\sim$ であった．つまり，$X/\sim$ は集合 X を $\sim$ でグループ分けするという操作になる．これを集合 X の分割といった．正確に定義すると，分割は以下で定義される．

定義 6.1. 集合 X の**分割**とは，X の部分集合族 $\{X_\lambda : \lambda \in \Lambda\}$ で以下の条件を満たすものである．

(1) $X = \bigcup_{\lambda\in\Lambda} X_\lambda$,

(2) 任意の $\lambda \in \Lambda$ に対し，$X_\lambda \neq \emptyset$ である．

(3) 任意の異なる $\lambda, \nu \in \Lambda$ に対し，$X_\lambda \cap X_\nu = \emptyset$ である．

このとき，$X = \bigsqcup_{\lambda\in\Lambda} X_\lambda$ と表現する．

命題 6.2. 集合 X とその同値関係 $\sim$ に対し，商集合 $X/\sim$ は X の分割となる．つまり，S を $X/\sim$ の完全代表系とすれば，

$$X = \bigsqcup_{a\in S} [a]_\sim$$

となる．

Proof. 情報数理 B の 5 回目を参照. □

それでは群とその部分群から同値関係を定義する．G を群とし，H を G の部分群とする．このとき，G 上の関係 $\equiv_l$ を以下のように定義する．

$$\begin{aligned} a \equiv_l b &\underset{\text{def}}{\iff} b^{-1} \circ a \in H \\ &\iff a = b \circ h \text{ を満たす } h \in H \text{ が存在する．} \end{aligned}$$

また G 上の関係 $\equiv_r$ を以下のように定義する．

$$\begin{aligned} a \equiv_r b &\underset{\text{def}}{\iff} a \circ b^{-1} \in H \\ &\iff a = h \circ b \text{ を満たす } h \in H \text{ が存在する．} \end{aligned}$$

命題 6.3. $\equiv_l$ と $\equiv_r$ はともに G 上の同値関係である．

Proof. $\equiv_l$ の場合のみ証明する．

（反射律）任意の $a \in G$ に対し，$a^{-1} \circ a = e \in H$ であるので $a \equiv_l a$ である．よって $\equiv_l$ は反射的である．

（対称律）任意の $a, b \in G$ で $a \equiv_l b$ となるものをとる．このとき，$b^{-1} \circ a \in H$ である．H が部分群であるので

$$a^{-1} \circ b = (b^{-1} \circ a)^{-1} \in H$$

が従う．よって $b \equiv_l a$ となり $\equiv_l$ は対称的である．

（推移律）任意の $a, b, c \in G$ で $a \equiv_l b$ かつ $b \equiv_l c$ となるものをとる．このとき，$b^{-1} \circ a \in H$ かつ $c^{-1} \circ b \in H$ である．すると，H が部分群であるので

$$c^{-1} \circ a = c^{-1} \circ e \circ a = c^{-1} \circ (b \circ b^{-1}) \circ a = (c^{-1} \circ b) \circ (b^{-1} \circ a) \in H$$

が従う．よって $a \equiv_l c$ となり $\equiv_l$ は推移的である．

以上より $\equiv_l$ は同値関係である． □

定義 6.4. G を群，H をその部分群とする．$a \in G$ に対し，同値類

$$[a]_{\equiv_l} = \{g \in G : a \equiv_l g\}$$

を H に関する a の属する**左剰余類**といい，aH で表す．同様に，同値類

$$[a]_{\equiv_r} = \{g \in G : a \equiv_r g\}$$

を H に関する a の属する**右剰余類**といい，Ha で表す．

命題 6.5. G を群とする．$a \in G$ に対し

$$aH = \{a \circ h : h \in H\},$$
$$Ha = \{h \circ a : h \in H\}$$

となる．特に，$eH = He = H$ である．

Proof. $A = \{a \circ h : h \in H\}$ とし，$aH = A$ の場合のみ証明する．$g \in G$ に対し，

$$\begin{aligned} g \in aH &\iff a \equiv_l g \\ &\iff g \equiv_l a \\ &\iff \exists h \in H, g = a \circ h \\ &\iff g \in A \end{aligned}$$

が成り立つ．よって $aH = A$ である． □

補足 6.6. G がアーベル群の場合は $aH = Ha$ であるので左と右の区別をする必要がない．この場合，単に**剰余類**と呼ぶことにする．

定義 6.7. 群 G とその部分群 H に対し，G の $\equiv_l$ に関する商集合を G/H と書き，$\equiv_r$ に関する商集合を $H \setminus G$ と書く．つまり，

$$G/H = \{aH : a \in H\},$$
$$H\backslash G = \{Ha : a \in H\}$$

である．G/H と $H\backslash G$ をそれぞれ G の H に関する**左商集合**と**右商集合**と呼ぶ．また L と R をそれぞれ G/H と $H\backslash G$ の完全代表系としたとき，$G = \bigsqcup_{a \in L} aH$ と $G = \bigsqcup_{a \in R} Ha$ をそれぞれ G の**左剰余類分割**と**右剰余類分割**と呼ぶ．

ここで集合の濃度について復習する．有限とは限らない集合 X と Y に対し，X と Y の濃度が同じ（$|X| = |Y|$ と書く）とは，集合 X と Y の間に全単射写像が存在するときにいう．

命題 6.8. G を群とし，H を G の部分群とする．

(1) 任意の $a, b \in G$ に対し，$|aH| = |bH|$ である．特に，$|aH| = |H|$ である．

(2) 任意の $a, b \in G$ に対し，$|Ha| = |Hb|$ である．特に，$|Ha| = |H|$ である．

(3) $|G/H| = |H\backslash G|$ である．

Proof. (1) 写像

$$f : aH \to bH; x \mapsto b \circ a^{-1} \circ x, \qquad g : bH \to aH; y \mapsto a \circ b^{-1} \circ y$$

を定義する．まず f が well-defined であること，つまり $b \circ a^{-1} \circ x \in bH$ を確かめる．$x \in aH$ より $h \in H$ を用いて $x = a \circ h$ と書ける．すると

$$b \circ a^{-1} \circ x = b \circ a^{-1} \circ a \circ h = b \circ e \circ h = b \circ h \in bH$$

であるので，f は well-defined である．同様に g も well-defined である．このとき，任意の $x \in aH$ に対し，

$$(g \circ f)(x) = g(f(x)) = g(b \circ a^{-1} \circ x) = a \circ b^{-1} \circ (b \circ a^{-1} \circ x) = x$$

であるので，$g \circ f = \mathrm{id}_{aH}$ である．同様に $f \circ g = \mathrm{id}_{bH}$ であるので g は f の逆写像である．よって f が全単射となるので $|aH| = |bH|$ が従う．また $eH = H$ が容易にわかるので，

(2) (1) と同様である．

(3) 写像 $\phi : G/H \to H\backslash G$ を $\phi(aH) = Ha^{-1}$ で定義する．この写像が well-defined であることを見る．$aH = bH$ とする．これは $a \equiv_l b$ を意味する．このとき $Ha^{-1} = Hb^{-1}$ となればよい．つまり $a^{-1} \equiv_r b^{-1}$ を確かめればよい．$a \equiv_l b$ から $b^{-1} \circ a \in H$ である．H が部分群であるので，

$$a^{-1} \circ (b^{-1})^{-1} = a^{-1} \circ b = (b^{-1} \circ a)^{-1} \in H$$

となる．よって $a^{-1} \equiv_r b^{-1}$ であるので，ϕ は well-defined である．同様に，写像 $\psi : H\backslash G \to G/H$ を $\phi(Ha) = a^{-1}H$ で定義すると，これは well-defined である．このとき，$\psi \circ \phi = \mathrm{id}_{G/H}$ と $\phi \circ \psi = \mathrm{id}_{H\backslash G}$ となることが容易に確かめられるので，ψ は ϕ の逆写像である．よって ϕ が全単射となるので $|G/H| = |H\backslash G|$ が従う． □

定義 6.9. 群 G と部分群 H に対し，商集合の位数 $|G/H| = |H\backslash G|$ を G における H の**指数**といい，$(G : H)$ で表す．

指数 $(G : H)$ は有限とは限らない．一方で G が有限群の場合は，$(G : H)$ も有限となる．特に，次の定理が成り立つ．

定理 6.10 (ラグランジュの定理)**.** 有限群 G とその部分群 H に対し，

$$|G| = (G : H) \cdot |H|$$

が成り立つ．特に，部分群 H の位数は，もとの群 G の位数の約数となる．

Proof. G の H による左剰余類分割 $G = \bigsqcup_{i=1}^{(G:H)} a_i H$ を考えると，

$$|G| = \sum_{i=1}^{(G:H)} |a_i H|$$

となる．このとき，$|a_iH| = |H|$ であったので，

$$|G| = \sum_{i=1}^{(G:H)} |H| = (G:H) \cdot |H|$$

が従う． □

系 6.11. G を有限群とする．このとき，任意の $a \in G$ に対し，$\mathrm{ord}(a)$ は $|G|$ の約数である．

Proof. $\mathrm{ord}(a) = |\langle a \rangle|$ より従う． □

この系を使ってオイラーの定理が証明できる．

定理 6.12 (オイラーの定理)**.** 自然数 $m \geq 2$ と m と互いに素な整数 a に対して，

$$a^{\phi(m)} \equiv_m 1$$

が成り立つ．

Proof. 群 $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ とその元 $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ を考える．示すことは，

$$\overline{a}^{\phi(m)} = \overline{1}$$

となることである．$|(\mathbb{Z}/m\mathbb{Z})^\times| = \phi(m)$ であるから，$\mathrm{ord}(a) | \phi(m)$ である．よって命題 4.13 から

$$\overline{a}^{\phi(m)} = \overline{1}$$

が従う． □

6.2 正規部分群と剰余群

群 $\mathbb{Z}$ とその部分群 $m\mathbb{Z}$ の剰余類 $\mathbb{Z}/m\mathbb{Z}$ は群となっていた．同様に，群 G とその部分群 H の剰余類 G/H や $H\backslash G$ に群構造を入れたい．しかし，一般の H ではうまく演算を定義できないことがある．これは群の演算が一般に非可換である弊害である．そこで特別な部分群を定義し，その問題を解消し，この場合に群構造を入れることを考える．

定義 6.13. G を群とし，N をその部分群とする．任意の $x \in N$ と任意の $a \in G$ に対して

$$a \circ x \circ a^{-1} \in N$$

が成り立つとき，N を G の**正規部分群** (normal subgroup) という．

補足 6.14. N が G の部分群のとき，任意の $x \in N$ と任意の $a \in N \subset G$ に対して

$$a \circ x \circ a^{-1} \in N$$

が成り立つため，N が正規部分群かどうか判定するときは，$a \in G \setminus N$ の場合のみチェックすればよい．

具体例を見てみよう．

例 6.15. 3 次対称群 $\mathfrak{S}_3$ とその部分群

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

を考える．このとき，$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in H$ と $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_3$ に対し，

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \notin H \end{aligned}$$

となるので，H は正規部分群ではない．一方で，部分群

$$N = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

は正規部分群である（確かめよ）．

以下の命題の条件を正規部分群の定義と思ってもよい．

命題 6.16. G を群とし，N をその部分群とする．このとき，N が G の正規部分群である必要十分条件は任意の $a \in G$ に対し，$aN = Na$ が成り立つことである．

Proof. （⇒）任意の $a \in G$ と $a \circ x \in aN$ $(x \in N)$ をとる．N が G の正規部分群であるので，$a \circ x \circ a^{-1} \in N$ が成り立つ．よって

$$a \circ x = (a \circ x \circ a^{-1}) \circ a \in Na$$

となるので $aN \subset Na$ が従う．同様に，$Na \subset aN$ が示せるので，$aN = Na$ が成り立つ．

（⇐）任意の $x \in N$ と $a \in G$ をとる．このとき，$aN = Na$ なので，$a \circ x = y \circ a$ を満たす $y \in N$ が存在する．この両辺の右から a^{-1} を掛けると，

$$a \circ x \circ a^{-1} = y \circ a \circ a^{-1} = y \in N$$

となる．よって N は G の正規部分群である． □

系 6.17. G がアーベル群であれば，G の任意の部分群は正規部分群となる．

N を G の正規部分群とし，左商集合 G/N 上に演算を次のように定義する．

$$\bar{\circ} : G/N \times G/N \to G/N, (aN, bN) \mapsto (a \circ b)N.$$

ここで G 上の演算 $\circ$ と区別するために $\bar{\circ}$ と書いている．

命題 6.18. G/N 上の演算 $\bar{\circ}$ は well-defined である．

Proof. $aN = a'N$ と $bN = b'N$ をとる．このとき，$(a \circ b)N = (a' \circ b')N$ を示せばよい．$(a \circ b) \circ x \in (a \circ b)N$ $(x \in N)$ を任意にとる．$bN = b'N$ と N が正規部分群であることから $bN = b'N = Nb'$ が成り立つ．よっ

て $b \circ x = y \circ b'$ を満たす $y \in N$ が存在する．同様の議論を $a \circ y \in aN$ ですると，$a \circ y = z \circ a'$ を満たす $z \in N$ が存在する．よって

$$(a \circ b) \circ x = a \circ (y \circ b') = (z \circ a') \circ b' = z \circ (a' \circ b') \in N(a' \circ b') = (a' \circ b')N$$

が従う．したがって，$(a \circ b)N \subset (a' \circ b')N$ が得られる．同様に，$(a \circ b)N \supset (a' \circ b')N$ が示せるので，$(a \circ b)N = (a' \circ b')N$ となり，$\bar{\circ}$ が well-defined であることがわかった． □

命題 6.19. 群 G とその正規部分群 N に対し，$(G/N, \bar{\circ})$ は群となる．特に，単位元は N，aN の逆元は $a^{-1}N$ である．この群 $(G/N, \bar{\circ})$ を G の N に関する**剰余群**という．

Proof. (G1) $\bar{\circ}$ の結合律は $\circ$ が結合律を満たすことから従う．

(G2) 任意の $aN \in G/N$ に対し，$aN \bar{\circ} N = (a \circ e)N = aN$ である．同様に，$N \bar{\circ} aN = aN$ であるので，単位元 $N \in G/N$ が存在する．

(G3) 任意の $aN \in G/N$ に対し，$a^{-1}N \in G/N$ を考えると，

$$aN \bar{\circ} a^{-1}N = (a \circ a^{-1})N = N = a^{-1}N \bar{\circ} aN$$

となるので，逆元 $a^{-1}N \in G/N$ が存在する．

以上より，$(G/N, \bar{\circ})$ は群である． □

G/N と同様に，右商集合 $N\backslash G$ 上の演算を

$$\bar{\circ}' : N\backslash G \times N\backslash G \to N\backslash G; (Na, Nb) \mapsto N(a \circ b)$$

と定義することで，剰余群 $(N\backslash G, \bar{\circ}')$ も考えることができるが，この 2 つの剰余群は全く同じである．

命題 6.20. 群 G とその正規部分群 N に対し，$(G/N, \bar{\circ}) = (N\backslash G, \bar{\circ}')$ である．

Proof. 任意の $a \in G$ に対し，$aN = Na$ から $G/N = N\backslash G$ である．また任意の $aN, bN \in G/N$ に対し，

$$aN \bar{\circ} bN = (a \circ b)N = N(a \circ b) = Na \bar{\circ}' Nb$$

より $\bar{\circ}$ と $\bar{\circ}'$ は同じ写像（演算）である．したがって，$(G/N, \bar{\circ}) = (N\backslash G, \bar{\circ}')$ である.. □

よって剰余群を考えるときは基本 G/N を考える．

6.3 準同型定理

一般に群 G_1 と G_2 の間の準同型写像 $f : G_1 \to G_2$ を与えたとき，f は同型写像にならない．そこで G_1, G_2 と f を加工することで，G_1 と G_2 の「同型な部分」を見つける定理が準同型定理である．

まず G_1 を加工する．$\mathrm{Ker}(f)$ は G_1 の部分群であったが，実は正規部分群となる．

命題 6.21. $\mathrm{Ker}(f)$ は G_1 の正規部分群である．

Proof. 任意の $a \in G_1$ と $n \in \mathrm{Ker}(f)$ に対して，$f(n) = e_2$ であるので，

$$f(a \circ_1 n \circ_1 a^{-1}) = f(a) \circ_2 f(n) \circ_2 f(a^{-1}) = f(a) \circ_2 e_2 \circ_2 f(a^{-1}) = f(a) \circ_2 f(a^{-1}) = e_2$$

となり，$a \circ_1 n \circ_1 a^{-1} \in \mathrm{Ker}(f)$ が成り立つので，$\mathrm{Ker}(f)$ は正規部分群である． □

したがって，剰余群 $G/\mathrm{Ker}(f)$ が定義できる．これが $\mathrm{Im}(f)$ と同型となることを準同型定理という．

定理 6.22 (準同型定理)．G_1, G_2 を群とする．任意の群準同型写像 $f : G_1 \to G_2$ に対し，

$$\overline{f} : G_1/\mathrm{Ker}(f) \to \mathrm{Im}(f);\ a\mathrm{Ker}(f) \mapsto f(a)$$

は well-defined な同型写像である．特に，f が全射の場合，$G_1/\mathrm{Ker}(f) \cong G_2$ が成り立つ．

Proof. $N = \mathrm{Ker}(f)$ とする．まず well-defined 性を見る．$aN = bN$ となる $aN, bN \in G_1/N$ をとる．このとき，$f(a) = f(b)$ を示せばよい．$a = a \circ_1 e_1$ から $a = b \circ_1 x$ となる $x \in N$ が存在する．すると

$$f(a) = \overline{f}(aN) = \overline{f}((b \circ_1 x)N) = f(b \circ_1 x) = f(b) \circ_2 f(x) = f(b) \circ_2 e_2 = f(b)$$

となり，$\overline{f}$ が well-defined であることがわかる．

また，任意の $aN, bN \in G_1/N$ に対し，

$$\overline{f}(aN\ \overline{\circ_1}\ bN) = \overline{f}((a \circ_1 b)N) = f(a \circ_1 b) = f(a) \circ_2 f(b) = \overline{f}(aN) \circ_2 \overline{f}(bN)$$

が成り立つので $\overline{f}$ は準同型である．

最後に $\overline{f}$ が全単射であることを見ればよい．任意の $f(x) \in \mathrm{Im}(f)$（$x \in G_1$）に対し，$\overline{f}(xN) = f(x)$ であるから，f は全射である．$aN \in \mathrm{Ker}(\overline{f})$ をとる．すると，

$$\overline{f}(aN) = f(a) = e_2$$

となるので，$a \in N$ である．これは $aN = N$ を意味する．したがって，$\mathrm{Ker}(\overline{f}) = \{N\}$ となるので，$\overline{f}$ は単射である．

以上より，$\overline{f}$ は同型写像である． □

6.4 中国式剰余定理

最後に準同型定理を使って群論の言葉での中国式剰余定理を証明する．

定理 6.23 (中国式剰余定理 (群版))．m, n を互いに素な自然数とする．このとき，

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

である．

Proof. 写像 $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ を $f(x) = (x + m\mathbb{Z}, x + n\mathbb{Z})$ で定義する．このとき f は準同型である．実際，任意の $x, y \in \mathbb{Z}$ に対し，$f(x+y) = (x+y+m\mathbb{Z}, x+y+n\mathbb{Z})$ であるが，$(x+m\mathbb{Z})+(y+m\mathbb{Z}) = x+y+m\mathbb{Z}$ かつ $(x + n\mathbb{Z}) + (y + n\mathbb{Z}) = x + y + n\mathbb{Z}$ であるので，

$$\begin{aligned} f(x + y) &= (x + y + m\mathbb{Z}, x + y + n\mathbb{Z}) \\ &= ((x + m\mathbb{Z}) + (y + m\mathbb{Z}), (x + n\mathbb{Z}) + (y + n\mathbb{Z})) \\ &= (x + m\mathbb{Z}, x + n\mathbb{Z}) \circ (y + n\mathbb{Z}, y + n\mathbb{Z}) = f(x) \circ f(y) \end{aligned}$$

となる．ただし，$\circ$ は $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ 上の演算である．

f が全射であることを示す．任意の $(a + m\mathbb{Z}, b + n\mathbb{Z}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ をとる．m, n は互いに素なので $mx + ny = 1$ を満たす整数 x, y が存在する．$c = mxb + nya$ とおく．このとき，

$$\begin{aligned} c &= mxb + (1 - mx)a = a + mx(b - a), \\ c &= (1 - ny)b + nya = b + ny(a - b) \end{aligned}$$

であるので，

$$f(c) = (c + m\mathbb{Z}, c + n\mathbb{Z}) = (a + mx(b-a) + m\mathbb{Z}, b + ny(a-b) + n\mathbb{Z}) = (a + m\mathbb{Z}, b + n\mathbb{Z})$$

が従う．よって f は全射である．

$\mathrm{Ker}(f) = mn\mathbb{Z}$ を示す．$\mathrm{Ker}(f) \supset mn\mathbb{Z}$ は明らか．$a \in \mathrm{Ker}(f)$ をとる．このとき，

$$f(a) = (a + m\mathbb{Z}, a + n\mathbb{Z}) = (m\mathbb{Z}, n\mathbb{Z})$$

である．これは $a \equiv_m 0$ と $a \equiv_n 0$ を意味する．また m, n は互いに素なので，これより $a \equiv_{mn} 0$ が従う．よって $a \in mn\mathbb{Z}$ となる．したがって，$\mathrm{Ker}(f) \subset mn\mathbb{Z}$ なので，$\mathrm{Ker}(f) = mn\mathbb{Z}$ がわかる．

以上より，準同型定理から

$$\mathbb{Z}/mn\mathbb{Z} = \mathbb{Z}/\mathrm{Ker}(f) \cong \mathrm{Im}(f) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

を得る． □

既約剰余類に関しても中国式剰余定理が成り立つ．

定理 6.24 (中国式剰余定理 (既約剰余類版))**.** m, n を互いに素な自然数とする．このとき，

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

である．

Proof. 定理 6.23 の証明で定義した写像 $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ から同型写像

$$\overline{f} : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}; x + mn\mathbb{Z} \mapsto f(x) = (x + m\mathbb{Z}, x + n\mathbb{Z})$$

が得られる．この写像を $(\mathbb{Z}/mn\mathbb{Z})^\times$ に制限すると，その像は $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ に含まれる．実際，$x + mn\mathbb{Z} \in (\mathbb{Z}/mn\mathbb{Z})^\times$ をとると，これは $\gcd(x, mn) = 1$ であるので，$\gcd(x, m) = \gcd(x, n) = 1$ である．よって，$(x + m\mathbb{Z}, x + n\mathbb{Z}) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ となる．そこで，写像 F を

$$F : (\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times; x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

で定義する．この写像 F が同型写像であることを示せばよい．

（準同型写像）F と $\overline{f}$ の定義は同じだが，群の演算が $+$ ではなく $\cdot$ なので準同型写像であることを確かめる必要がある．任意の $x+mn\mathbb{Z}, y+mn\mathbb{Z} \in (\mathbb{Z}/mn\mathbb{Z})^\times$ をとる．このとき，$(x+mn\mathbb{Z})\cdot(y+mn\mathbb{Z}) = xy+mn\mathbb{Z}$ であった．すると

$$\begin{aligned} F((x + mn\mathbb{Z}) \cdot (y + mn\mathbb{Z})) &= F(xy + mn\mathbb{Z}) = (xy + m\mathbb{Z}, xy + n\mathbb{Z}) \\ &= ((x + m\mathbb{Z}) \cdot (y + m\mathbb{Z}), (x + n\mathbb{Z}) \cdot (y + n\mathbb{Z})) \\ &= (x + m\mathbb{Z}, x + n\mathbb{Z}) \circ (y + m\mathbb{Z}, y + n\mathbb{Z}) \\ &= F(x + mn\mathbb{Z}) \circ F(y + mn\mathbb{Z}) \end{aligned}$$

である．ただし，$\circ$ は $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ 上の演算である．よって F は準同型写像である．

（単射性）$\overline{f}$ が単射なので F も単射である．

（全射性）任意の $(a+m\mathbb{Z}, b+n\mathbb{Z}) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ をとる．このとき，$\gcd(a, m) = \gcd(b, n) = 1$ である．定理 6.23 の証明と同様に c をとると，$\overline{f}(c+mn\mathbb{Z}) = (a+m\mathbb{Z}, b+n\mathbb{Z})$ である．特に，$c \equiv_m a$ かつ $c \equiv_n b$ である．すると，$\gcd(a, m) = \gcd(b, n) = 1$ から $\gcd(c, mn) = 1$ が得られる．実際，$\gcd(m, n) = 1$ から $\gcd(c, mn) = \gcd(c, m)\gcd(c, n)$ である．$c \equiv_m a$ から整数 q を用いて $c - a = mq$，つまり $c = mq + a$ と書けるが，

$$\gcd(c, m) = \gcd(a + mq, m) = \gcd(a, m) = 1$$

であり，同様に $\gcd(c,n)=1$ も示せるので $\gcd(c,mn)=1$ である．よって，$c+mn\mathbb{Z}\in(\mathbb{Z}/mn\mathbb{Z})^\times$ が成り立ち，$F(x+mn\mathbb{Z})=(a+m\mathbb{Z},b+n\mathbb{Z})$ であるので，F は全射である． □

この定理を使うと次のオイラー関数の公式が得られる．

系 6.25. m,n を互いに素な自然数とする．このとき，

$$\phi(mn)=\phi(m)\phi(n)$$

である．