代数学入門

§1. 整数の性質

§1.1. 割り算と余り

- $\mathbb{Z} = \{\cdots -3,-2,-1,0,1,2,\cdots\}$ 整数全体の集合, $\mathbb{N} = \{1,2,3,\cdots\}$: 自然数全体の集合
- $\mathbb{Z}$ においては, 足し算と掛け算が定義されている.
- 任意の整数 $a,b \in \mathbb{Z}$ に対して, $a \geqslant b$ または $b \geqslant a$ が成り立つ.
  また, $a \geqslant b$ かつ $b \geqslant a$ のとき, $a = b$ である.

定理 1.1.1 (割り算の定理): 任意の $a,b \in \mathbb{Z}$ $(b \neq 0)$ に対して,

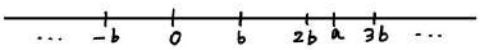
$$a = bq + r, \quad 0 \leqslant r < |b|$$

を満たす $q,r \in \mathbb{Z}$ が一意的に存在する.

q は**商**といい, r は**余り**という.

証明: まず, q,r の存在性を示す.

- $b > 0$ のとき　b の全ての倍数 $\{bk \mid k \in \mathbb{Z}\}$ を考える.



明かに, $k \in \mathbb{Z}$ が存在し, $bk \leqslant a < b(k+1)$ が成り立つ. よって, $0 \leqslant a - bk < b$ である.
$q = k$, $r = a - bk$ とおけば良い.

- $b < 0$ のとき　以上より, $a = (-b)q' + r'$ かつ $0 \leqslant r' < -b$ であるような $q', r' \in \mathbb{Z}$ が存在する. ゆえに, $q = -q'$, $r = r'$ とおけば良い.

次に q,r の一意性を証明する.

$a = bq_1 + r_1 = bq_2 + r_2$ かつ $0 \leqslant r_1, r_2 < |b|$ とする. このとき, $r_1 - r_2 = b(q_1 - q_2)$ である. ゆえに, $r_1 - r_2$ は b の倍数である. $|r_1 - r_2| < |b|$ であるので, $r_1 = r_2$ がいえる. よって, $q_1 = q_2$ であることも分かる. □

例 1.1.2 • $a = 59$, $b = -7$ とする.

$$59 = (-7) \times \underbrace{(-8)}_{q} + \underbrace{3}_{r}$$

• $a = -8$, $b = -3$ とする.

$$-8 = (-3) \times \underbrace{3}_{q} + \underbrace{1}_{r}$$

• $a = 8$, $b = -3$ とする

$$8 = (-3) \times \underbrace{(-2)}_{q} + \underbrace{2}_{r}$$

§1.2. 最大公約数・最小公倍数

$a, b \in \mathbb{Z}$ とする. $a = bc$ を満たす $c \in \mathbb{Z}$ が存在するとき,

「a が b で割り切れる」, または
「a が b の倍数である」, または
「b が a の約数である」

といい, $b \mid a$ と書く.

定義 1.2.1 $a, b \in \mathbb{Z}$ $(a \neq 0, b \neq 0)$ とする.

- a と b の最大公約数は $c \mid a$ かつ $c \mid b$ を満たす最大の自然数 c のことをいい, $\gcd(a, b)$ で表す.
- a と b の最小公倍数は $a \mid c$ かつ $b \mid c$ を満たす最小の自然数 c のことをいい, $\mathrm{lcm}(a, b)$ で表す.

§1.3 ユークリッドの互除法

a, b を自然数とする．有限数列 $\{a_n\}_n$ を次のように作る．

- $a_0 = a$, $a_1 = b$ とおく．
- 定理 1.1.1 によって，

$$a_0 = q_1 a_1 + a_2 \qquad (0 \leq a_2 < a_1)$$

と表すことができる．

- $a_2 \neq 0$ であるならば，

$$a_1 = q_2 a_2 + a_3 \qquad (0 \leq a_3 < a_2)$$

- と表すことができる．
- 以降，このプロセスを繰り返していく．つまり $0 \leq a_n < a_{n-1}$ まで得られたときに，$a_n \neq 0$ である限り

$$a_{n-1} = q_n a_n + a_{n+1} \qquad (0 \leq a_{n+1} < a_n)$$

と表すことができる．

補題 1.3.1. 上記のプロセスは有限回のステップで終止する．つまり，$N \geq 1$ が存在し，

$a_0 > a_1 > \cdots > a_{N-1} > a_N > a_{N+1} = 0$ である．

まとめると

$$(*) \begin{cases} a_0 = q_1 a_1 + a_2 \\ a_1 = q_2 a_2 + a_3 \\ \quad \vdots \\ a_{N-2} = q_{N-1} a_{N-1} + a_N \\ a_{N-1} = q_N a_N \end{cases}$$

が得られる．上の $(*)$ のプロセスは**ユークリッドの互除法**という．

定理 1.3.2.

(i) $a_N = \gcd(a, b)$

(ii) $r, s \in \mathbb{Z}$ を用いて, $a_N = ar + bs$ と書くことができる.

証明:

(i) $1 \leq n \leq N$ について, $a_{n-1} = q_n a_n + a_{n+1}$ である.
よって, a_{n-1} と a_n の公約数の集合は a_n と a_{n+1} の公約数の集合と一致する. とくに, $\gcd(a_{n-1}, a_n) = \gcd(a_n, a_{n+1})$ が成り立つ. ゆえに,

$$\gcd(a, b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_{N-1}, a_N) = a_N$$

($a_{N-1} = q_N a_N$)

(ii) 自然数 $0 \leq n \leq N$ に関する帰納法によって

「$a_n = ar_n + bs_n$ となる $r_n, s_n \in \mathbb{Z}$ が存在する」 (*)

を証明する.

- $n = 0$ のとき, $a_0 = a$ である. $r_0 = 1$, $s_0 = 0$ とおけば良い.
- $0 \leq n \leq N-1$ とし, 全ての $k \leq n$ に対して $a_k = ar_k + bs_k$ と書けることを仮定する. このとき,

$$\begin{aligned} a_{n+1} &= a_{n-1} - q_n a_n \\ &= (ar_{n-1} + bs_{n-1}) - q_n(ar_n + bs_n) \\ &= a(r_{n-1} - q_n r_n) + b(s_{n-1} - q_n s_n) \end{aligned}$$

$\begin{cases} r_{n+1} = r_{n-1} - q_n r_n \\ s_{n+1} = s_{n-1} - q_n s_n \end{cases}$ とおけば良い.

- したがって, 全ての $0 \leq n \leq N$ に対して (*) が成り立つ. とくに, $a_N = ar_N + bs_N$ と表すことができる. □

逆に，$\langle S \rangle \subset T$ を示す．まず，T が部分群であることを証明する．

$x = s_1^{k_1} \cdots s_n^{k_n}$ かつ $y = t_1^{r_1} \cdots t_m^{r_m}$ $(s_i, t_j \in S,\ k_i, r_j \in \mathbb{Z})$

とする．このとき

$$x y^{-1} = s_1^{k_1} \cdots s_n^{k_n} \left(t_1^{r_1} \cdots t_m^{r_m}\right)^{-1}$$
$$= s_1^{k_1} \cdots s_n^{k_n} t_m^{-r_m} \cdots t_1^{-r_1} \quad \in T \quad \text{である．}$$

補題 3.3.2 より T は G の部分群である．$S \subset T$ が成り立つので，$\langle S \rangle \subset T$ となる． □

定義 3.4.5 G を群とする．$G = \langle x \rangle$ となる $x \in G$ が存在するときに，G が巡回群であるという．また，このような x を G の生成元とよぶ．

命題 3.4.4 より

$$\langle x \rangle = \{ x^k \mid k \in \mathbb{Z} \}$$ である．

例 3.4.6 $n \in \mathbb{N}$ とする．$\mathbb{Z}/n\mathbb{Z}$ は $\overline{1}$ で生成されるので $\mathbb{Z}/n\mathbb{Z}$ は巡回群である．

∵ $\mathbb{Z}/n\mathbb{Z} = \{ \overline{0}, \overline{1}, \ldots, \overline{n-1} \}$ である．

また，$0 \leq k \leq n-1$ に対して $\overline{k} = k\overline{1} = \underbrace{\overline{1} + \cdots + \overline{1}}_{k\text{コ}}$

よって，$\langle \overline{1} \rangle = \mathbb{Z}/n\mathbb{Z}$ である．

命題 3.4.7 $n \in \mathbb{N}$ とし，$m \in \mathbb{Z}$ とする．以下の条件は互いに同値である．

(i) $\mathbb{Z}/n\mathbb{Z}$ は $\overline{m}$ で生成される．

(ii) $\gcd(n,m) = 1$

証明 (i) $\Rightarrow$ (ii)： $\mathbb{Z}/n\mathbb{Z} = \langle \overline{m} \rangle$ とする．とくに，$\overline{1} = k \cdot \overline{m} = \overline{km}$ となる $k \in \mathbb{Z}$ が存在する．ゆえに，$\overline{m}$ は $\mathbb{Z}/n\mathbb{Z}$ の可逆元である．命題 2.3.5 より $\gcd(n,m) = 1$

(ii) $\Rightarrow$ (i)： $\gcd(n,m) = 1$ とすると，$\overline{m}$ は可逆元である（命題 2.3.5）．よって，$\overline{1} = \overline{k} \cdot \overline{m} = k\overline{m}$ となる $k \in \mathbb{Z}$ が存在する．また，全ての $r = 1, \dots, n-1$ に対して

$$\overline{r} = r\overline{1} = (rk)\overline{m} \in \langle \overline{m} \rangle$$

である．

したがって $\langle \overline{m} \rangle = \mathbb{Z}/n\mathbb{Z}$ となる． □

例題 1.3.3 $a = 9006$, $b = 498$ とする.

ユークリッドの互除法により $\gcd(a,b)$ を求めよ. また, $\gcd(a,b) = ar + bs$ となる $r, s \in \mathbb{Z}$ を求めよ.

$a_0 = 9006$, $a_1 = 498$ とおく.

$$\begin{cases} \underbrace{9006}_{a_0=a} = 18 \times \underbrace{498}_{a_1=b} + \underbrace{42}_{a_2} \\ \underbrace{498}_{a_1=b} = 11 \times \underbrace{42}_{a_2} + \underbrace{36}_{a_3} \\ \underbrace{42}_{a_2} = 1 \times \underbrace{36}_{a_3} + \underbrace{6}_{a_4} \\ \underbrace{36}_{a_3} = 6 \times \underbrace{6}_{a_4} + 0 \end{cases}$$

$a_2 = a - 18b$

$a_3 = b - 11a_2 = -11a + 199b$

$a_4 = a_2 - a_3 = 12a - 217b$

よって,

$$\gcd(9006, 498) = 6$$
$$6 = 12 \times 9006 - 217 \times 498$$

§1.4 互いに素な整数

定義 1.4.1 $a, b \in \mathbb{Z}$ $(a \neq 0, b \neq 0)$ とする. $\gcd(a,b) = 1$ であるとき, a と b が**互いに素**であるという.

命題 1.4.2 $a, b \in \mathbb{Z}$ とする.

a と b が互いに素である $\iff \exists r, s \in \mathbb{Z},\ 1 = ar + bs$

証明:

($\Rightarrow$): $\gcd(a,b) = 1$ とする. 定理 1.3.2 (ii) より, $1 = ar + bs$ となる $r, s \in \mathbb{Z}$ が存在する.

($\Leftarrow$): $1 = ar + bs$ とし, $d \in \mathbb{N}$ を a と b の公約数とする.
$d \mid a$ かつ $d \mid b$ より, d が $ar + bs = 1$ の約数である. したがって, $d = 1$ となり, ゆえに $\gcd(a,b) = 1$ となる.

□

補題 1.4.3（ユークリッドの補題） $a, b, c \in \mathbb{Z}$ とし，$a \mid bc$ とする．
a と b が互いに素であれば，$a \mid c$ である．

証明：命題 1.4.2 より，$1 = ar + bs$ $(r, s \in \mathbb{Z})$ と書くことができる．
よって，$c = acr + bcs$ となる．$a \mid bc$ だから，$a \mid c$ となる．
□

補題 1.4.4：$a, b, c \in \mathbb{Z}$ とし，$\gcd(a, b) = \gcd(a, c) = 1$ とする．このとき，$\gcd(a, bc) = 1$ である．

証明：命題 1.4.2 より $\begin{cases} ar_1 + bs_1 = 1 \\ ar_2 + cs_2 = 1 \end{cases}$ となる $r_1, s_1, r_2, s_2 \in \mathbb{Z}$ が存在する．
よって，

$$\begin{aligned} 1 &= (ar_1 + bs_1)(ar_2 + cs_2) \\ &= a^2 r_1 r_2 + abs_1 r_2 + acr_1 s_2 + bcs_1 s_2 \\ &= a(ar_1 r_2 + bs_1 r_2 + cr_1 s_2) + bcs_1 s_2 \end{aligned}$$

したがって，$ar' + (bc)s' = 1$ となる $r', s' \in \mathbb{Z}$ が存在する．主張が従う．□

補題 1.4.5 $a, b, c \in \mathbb{Z}$ とし，$\gcd(a, b) = 1$ とする．
$a \mid c$ かつ $b \mid c$ ならば，$ab \mid c$ である．

証明：$c = ak$ となる $k \in \mathbb{Z}$ が存在する．$b \mid c$ かつ $\gcd(a, b) = 1$ より
$b \mid k$ となる（補題 1.4.3 参照）．よって，$k = bk'$ $(k' \in \mathbb{Z})$ と書くことができる．
ゆえに，$c = abk'$ となる．
□

§1.5. 素因数分解

$p \geq 2$ を自然数とする. p が**素数**であるとは, p が $\pm 1, \pm p$ 以外の約数をもたないことをいう.

定理 1.5.1.

任意の自然数 $n \geq 2$ は一意的に

$$n = p_1^{k_1} p_2^{k_2} \cdots p_d^{k_d} \quad (\text{ただし } p_1 < p_2 < \cdots < p_d \text{ は素数}, k_i \in \mathbb{N} \text{ である})$$

と表すことができる.

証明:

- 存在性: n に関する帰納法により証明する.

  n が素数であるときには主張が明らかである.

  n が素数でないとする. このとき, $n = ab$ $(1 < a, b < n)$ と表すことができる. 帰納法の仮定により, a と b は素数の積に分解できる.

  よって n も同様である.

- 一意性: n に関する帰納法により示す.

  $n = p_1^{k_1} \cdots p_d^{k_d}$ $(p_1 < \cdots < p_d$ は素数, $k_i \in \mathbb{N})$

  $= q_1^{r_1} \cdots q_m^{r_m}$ $(q_1 < \cdots < q_m$ は素数, $r_i \in \mathbb{N})$ とする.

  よって, $p_1 \mid q_1^{r_1} \cdots q_m^{r_m}$ である. 全ての $j = 1, \ldots, m$ に対して $p_1 \neq q_j$ であれば, p_1 と $n = q_1^{r_1} \cdots q_m^{r_m}$ は互いに素であり, $p_1 \mid n$ に矛盾する.

  よって $p_1 = q_j$ となる q_j が存在する. 同様に, $q_1 = p_s$ となる p_s が存在する.

  $j \neq 1$ とすると, $p_1 = q_j > q_1 = p_s$ となり, 矛盾する. よって $q_1 = p_1$ である.

  このことから $p_1^{k_1 - 1} p_2^{k_2} \cdots p_d^{k_d} = q_1^{r_1 - 1} q_2^{r_2} \cdots q_m^{r_m}$ である.

  帰納法の仮定により, $d = m$ かつ $p_i = q_i$, $k_i = r_i$ $(1 \leq \forall i \leq m)$ が分かる. □

§2. 合同式

§2.1 合同関係

$n \geq 1$ を自然数を固定する．2つの整数 a, b が n を法として合同であるとは，$a-b$ が n で割り切れることをいう．このとき，

$$a \equiv b \pmod{n}$$

という記号を用いる．

例 2.1.1

$$7 \equiv 1 \pmod{3}$$
$$7 \equiv 1 \pmod{2}$$
$$83 \equiv 13 \pmod{10}$$

$n \geq 1$ を固定する．2つの整数 $a, b \in \mathbb{Z}$ に対して

$$「a \sim b \overset{\text{def}}{\iff} a \equiv b \pmod{n}」$$

として，$\mathbb{Z}$ に同値関係 $\sim$ を入れる．

（$\sim$ が同値関係であるとは，任意の $a, b, c \in \mathbb{Z}$ に対して

- $a \sim a$ （反射性）
- $a \sim b$ ならば $b \sim a$ （対称性）
- $a \sim b$ かつ $b \sim c$ ならば $a \sim c$ （推移性）

が成り立つことをいう．）

補題 2.1.2 $\sim$ が $\mathbb{Z}$ 上の同値関係である.

証明: $a, b, c \in \mathbb{Z}$ とする.

- **反射性**: $a - a = 0$ が n で割り切れるので $a \equiv a \pmod{n}$ である.
- **対称性**: $a \equiv b \pmod{n}$ とする. よって, $a - b = nk$ $(k \in \mathbb{Z})$ と書くことができる. ゆえに, $b - a = -(a-b) = (-k) \cdot n$ であり, n で割り切れる.
  よって, $b \equiv a \pmod{n}$ である.
- **推移性**: $a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$ とする.
  このとき, $\begin{cases} a - b = n \cdot r \\ b - c = n \cdot s \end{cases}$ となる $r, s \in \mathbb{Z}$ が存在する.
  したがって, $a - c = (a-b) + (b-c) = nr + ns = n(r+s)$ である.
  以上より $a \equiv c \pmod{n}$ である. □

注意 2.1.3 $a \equiv b \pmod{n}$ とし, $k \in \mathbb{Z}$ とする. このとき,

$a + k \equiv b + k \pmod{n}$ かつ $a \cdot k \equiv b \cdot k \pmod{n}$ である.

整数 a の $\sim$ による同値類を $\overline{a}$ で表す. つまり,

$$\begin{aligned} \overline{a} &= \{ b \in \mathbb{Z} \mid a \equiv b \pmod{n} \} \\ &= \{ b \in \mathbb{Z} \mid b - a \text{ が } n \text{ で割り切れる} \} \end{aligned}$$

また, $b - a$ が n で割り切れる $\Leftrightarrow$ $b = a + nk$ $(k \in \mathbb{Z})$ である.

よって, $\overline{a}$ は以下のように表すことができる.

$$\overline{a} = \{ a + nk \mid k \in \mathbb{Z} \}$$

この集合を単に $a + n\mathbb{Z}$ で表す. つまり $\overline{a} = a + n\mathbb{Z}$ である.

= 商集合

同値関係 $\sim$ による同値類全体の集合を $\mathbb{Z}/n\mathbb{Z}$ で表す. すなわち,

$$\mathbb{Z}/n\mathbb{Z} = \{ \overline{a} \mid a \in \mathbb{Z} \}.$$

補題 2.1.4 $\mathbb{Z}/n\mathbb{Z}$ はちょうど n 個の元 $\overline{0}, \overline{1}, \dots, \overline{n-1}$ から構成されている:

$$\mathbb{Z}/n\mathbb{Z} = \{ \overline{0}, \overline{1}, \dots, \overline{n-1} \}$$

証明: まず, $\overline{0}, \overline{1}, \dots, \overline{n-1}$ が互いに異なることを示す.

$0 \leq a, b \leq n-1$ とし, $\overline{a} = \overline{b}$ とする. このとき, $|a-b| \leq n-1$ であり, さらに $n \mid a-b$ である. ゆえに $a = b$ となる.

したがって, $\overline{0}, \overline{1}, \dots, \overline{n-1}$ は互いに異なる.

次に, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ を示す. $a \in \mathbb{Z}$ とし, $\overline{a}$ を a の同値類とする.

割り算定理より $a = qn + r$ $(0 \leq r < n)$ と書くことができる.

よって, $n \mid a-r$ であり, $\overline{a} = \overline{r}$ となる. 主張が従う. □

$\sim$ が $\mathbb{Z}$ 上の同値関係であるので, $\mathbb{Z}$ は同値類に分割される:

$$\mathbb{Z} = \bigsqcup_{j=0}^{n-1} j + n\mathbb{Z}$$

(この記号 $\sqcup$ は互いに共通部分のない部分集合の和集合という意味である.)

§2.2 加法と乗法

自然数 n を固定する. 集合 $\mathbb{Z}/n\mathbb{Z}$ に加法と乗法を定義する.
$a, b \in \mathbb{Z}$ とし, $\overline{a} = a + n\mathbb{Z}$ と $\overline{b} = b + n\mathbb{Z}$ をそれぞれの同値類とする.

$$\begin{aligned} \overline{a} + \overline{b} &:= \overline{a+b} \\ \overline{a} \cdot \overline{b} &:= \overline{a \cdot b} \end{aligned} \qquad (*)$$

と定義する.

$(*)$ が well-defined であることを確認する.

$\overline{a} = \overline{a'}$ かつ $\overline{b} = \overline{b'}$ $(a, b, a', b' \in \mathbb{Z})$ のとき,

$$(**) \begin{cases} \overline{a+b} = \overline{a'+b'} \\ \overline{ab} = \overline{a'b'} \end{cases}$$ が成り立つことを示せば良い.

証明:

$\begin{cases} a - a' = n \cdot r \\ b - b' = n \cdot s \end{cases}$ となる $r, s \in \mathbb{Z}$ が存在する.

よって, $(a+b) - (a'+b') = (a-a') + (b-b') = nr + ns = n(r+s)$ である.

また, $\begin{aligned} ab - a'b' &= (ab - ab') + (ab' - a'b') \\ &= a(b-b') + b'(a-a') \\ &= ans + b'nr \\ &= n(as + b'r) \end{aligned}$ である.

以上より, $(**)$ が従う. □

同様に引き算を定義する: $\bar{a} = a+n\mathbb{Z}$, $\bar{b} = b+n\mathbb{Z}$ $(a, b \in \mathbb{Z})$ について,

$$\bar{a} - \bar{b} = \overline{a-b}$$

と定める. この定義が well-defined である.

例 2.2.1 $n=5$ とする.

$$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

$\mathbb{Z}/5\mathbb{Z}$ の加法と乗法は以下のように定まる.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

§2.3 可逆元

$n \geq 1$ を固定する.

定義 2.3.1 $\mathbb{Z}/n\mathbb{Z}$ の元 $\overline{a} = a + n\mathbb{Z}$ $(a \in \mathbb{Z})$ が可逆元であるとは,

$$\overline{a} \cdot \overline{b} = \overline{1}$$

となる $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ $(b \in \mathbb{Z})$ が存在することをいう.

例 2.3.2 $n = 6$ とする. $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

×	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

よって, $\mathbb{Z}/6\mathbb{Z}$ の可逆元は $\overline{1}, \overline{5}$ である.

補題 2.3.3 $\overline{a}$ $(a \in \mathbb{Z})$ を $\mathbb{Z}/n\mathbb{Z}$ の可逆元とする. このとき,

$\overline{a}\,\overline{b} = \overline{1}$ となる $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ は一意的に存在する.

この元 $\overline{b}$ を $\overline{a}$ の**逆元**とよび, $\overline{b} = (\overline{a})^{-1}$ で表す.

証明：$\overline{a}\overline{b}=\overline{1}$ かつ $\overline{a}\overline{c}=\overline{1}$ とし，$\overline{b}=\overline{c}$ を示せば良い．

$\overline{a}\overline{b}=\overline{1}$ より $\overline{a}\overline{b}\overline{c}=\overline{c}$ である．また，$\overline{a}\overline{c}=\overline{1}$ だから，

$\overline{a}\overline{b}\overline{c}=\overline{1}\cdot\overline{b}=\overline{b}$ となる．ゆえに $\overline{b}=\overline{c}$ である．　□

注意 2.3.4

(i) $\overline{1}$ と $\overline{-1}=\overline{n-1}$ は常に可逆元である．なぜならば，

$$\begin{cases}\overline{1}\cdot\overline{1}=\overline{1}\\ \overline{-1}\cdot\overline{-1}=\overline{(-1)(-1)}=\overline{1}\end{cases}$$

が成り立つ．よって $(\overline{1})^{-1}=\overline{1}$ かつ $(\overline{-1})^{-1}=\overline{-1}$ である．

(ii) $\overline{0}$ は可逆元でない．なぜならば，全ての $\overline{b}\in\mathbb{Z}/n\mathbb{Z}$ に対して

$\overline{0}\cdot\overline{b}=\overline{0}$ である．よって $\overline{0}\cdot\overline{b}=\overline{1}$ となる $\overline{b}$ は存在しない．

(iii) $\overline{a}$ が可逆元であるならば，$(\overline{a})^{-1}$ も可逆元である．また，

$\overline{a}(\overline{a})^{-1}=\overline{1}$ より $((\overline{a})^{-1})^{-1}=\overline{a}$ が成り立つ．

命題 2.3.5　$\overline{a}\in\mathbb{Z}/n\mathbb{Z}$ について，以下が成り立つ．

$\overline{a}$ が可逆元である $\iff$ $\gcd(a,n)=1$

証明

($\Rightarrow$)：$\overline{a}$ を可逆元とする．$\overline{a}\overline{b}=\overline{1}$ となる $\overline{b}\in\mathbb{Z}/n\mathbb{Z}$ $(b\in\mathbb{Z})$ が存在する．よって，$ab\equiv 1 \pmod n$ であり，つまり $ab-1$ は n で割り切れる：$ab-1=nr$ $(r\in\mathbb{Z})$．よって $ab-nr=1$ となり，$\gcd(a,n)=1$ である．

($\Leftarrow$)：$\gcd(a,n)=1$ とする．このとき，$ar+ns=1$ となる $r,s\in\mathbb{Z}$ が存在する．よって，$ar\equiv 1 \pmod n$ である．

ゆえに $\overline{a}\overline{r}=\overline{ar}=\overline{1}$ であり，$\overline{a}$ は可逆元である．　□

系 2.3.6 p を素数とする．全ての $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ $(\overline{a} \neq \overline{0})$ は可逆元である．

証明： $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$ である．
$1, 2, \dots, p-1$ はそれぞれ p と互いに素であるので，主張が命題 2.3.5 から従う． □

§2.4 ウィルソンの定理・フェルマーの小定理

定理 2.4.1 (ウィルソンの定理) $n \geq 2$ を自然数とする．

n が素数である $\iff$ $(n-1)! \equiv -1 \pmod{n}$

が成り立つ．

証明

($\Rightarrow$) n が素数であるとする． $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ である．
$n=2$ のとき $(n-1)! = 1! = 1 \equiv -1 \pmod{2}$ である．よって，
$n \geq 3$ を仮定して良い．とくに，n は奇数である．
$\overline{0}$ 以外の元の積 $\overline{1} \cdot \overline{2} \cdots \overline{(n-1)}$ を計算する．系 2.3.6 より
全ての $\overline{a} \in \{\overline{1}, \dots, \overline{n-1}\}$ は可逆元である．

- $\overline{a} = \overline{1}$ のとき，$(\overline{1})^{-1} = \overline{1}$ である，
- $\overline{a} = \overline{n-1} = \overline{-1}$ のとき，$(\overline{n-1})^{-1} = \overline{n-1}$ である．
- $2 \leq a \leq n-2$ のとき，$(\overline{a})^{-1} \neq \overline{a}$ である．なぜならば，
  $(\overline{a})^{-1} = \overline{a}$ とすると，$\overline{a}^2 = \overline{1}$ となる．よって，$a^2 \equiv 1 \pmod{n}$ であり，

ゆえに $a^2-1=(a-1)(a+1)$ が n で割り切れる．n が素数であるので，$n \mid a-1$ または $n \mid a+1$ となり，矛盾する．したがって $(\overline{a})^{-1} \neq \overline{a}$ である．

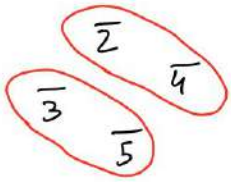
$\{\overline{2}, \cdots, \overline{n-2}\}$ の中で各元をその逆元とペアにして，$k=\frac{n-3}{2}$ 個のペアを作る．

例えば，$n=7$ の場合について考える．

$$\mathbb{Z}/7\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$$

$\overline{2}\cdot\overline{4}=\overline{8}=\overline{1}$ より $(\overline{2})^{-1}=\overline{4}$ かつ $(\overline{4})^{-1}=\overline{2}$ である．

$\overline{3}\cdot\overline{5}=\overline{15}=\overline{1}$ より $(\overline{3})^{-1}=\overline{5}$ かつ $(\overline{5})^{-1}=\overline{3}$ である．



← このようにペアを作る．

ゆえに，$\{\overline{2}, \cdots, \overline{n-2}\} = \{\overline{x_1}, (\overline{x_1})^{-1}, \overline{x_2}, (\overline{x_2})^{-1}, \cdots, \overline{x_k}, (\overline{x_k})^{-1}\}$

となる $2 \leq x_1, x_2, \cdots, x_k \leq n-2$ が存在する．よって，

（ペア）

$$\prod_{j=2}^{n-2} \overline{j} = \prod_{i=1}^{k} \overline{x_i}\cdot(\overline{x_i})^{-1} = \prod_{i=1}^{k} \overline{1} = \overline{1}$$ である．

したがって，$\prod_{j=1}^{n-1} \overline{j} = \overline{n-1} = \overline{-1}$ である．

このことから，$(n-1)! \equiv -1 \pmod{n}$ となる．

($\Longleftarrow$)：$(n-1)! \equiv -1 \pmod{n}$ とする．

$(n-1)! = -1 + n\cdot r$ となる $r \in \mathbb{Z}$ が存在する．よって，$2, \cdots, n-1$ のいずれも n と素であり，とくに n の約数でない．

以上より，n は素数である． □

例 2.4.2

- $n=5$ とする

  $(n-1)! = 1\times 2\times 3\times 4 = 24$ であり, $24 \equiv -1 \pmod 5$ である

- $n=6$ とする

  $(n-1)! = 120$ であり, $120 \equiv 0 \pmod 6$ である.

定理 2.4.3 (フェルマーの小定理) p を素数とする.

(i) $a \in \mathbb{Z}$ とし, a は p で割り切れないとする. このとき,

$$a^{p-1} \equiv 1 \pmod p$$ が成り立つ.

(ii) 任意の整数 a に対して,

$$a^p \equiv a \pmod p$$ が成り立つ.

証明

(i) を示す. $H = \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$ とおく.

claim: 写像 $\underset{\overline{x}}{H} \xrightarrow{\varphi} \underset{\overline{ax}}{H}$ は全単射である.

- φ は well-defined である: $\overline{x} \in H$ より, x は p で割り切れない. よって, ax も p で割り切れない. ゆえに $\overline{a}\,\overline{x} \neq \overline{0}$ であり, $\overline{a}\,\overline{x} \in H$ となる.
- φ は単射である: $\overline{a}\,\overline{x} = \overline{a}\,\overline{y}$ とする. 系 2.3.6 より $\overline{a}$ は可逆元である. 両辺に $(\overline{a})^{-1}$ をかけると $(\overline{a})^{-1}\overline{a}\,\overline{x} = (\overline{a})^{-1}\overline{a}\,\overline{y}$ となる. $(\overline{a})^{-1}\overline{a} = \overline{1}$ より, $\overline{x} = \overline{y}$ が分かる. よって, φ は単射である.
- φ は全射である: $\overline{y} \in H$ とする. $\overline{x} = (\overline{a})^{-1}\overline{y}$ と定めると, $\overline{a}\,\overline{x} = \overline{a}(\overline{a})^{-1}\overline{y} = \overline{1}\cdot\overline{y} = \overline{y}$ である. よって, φ は全射である.

$S = \prod_{\overline{x}\in H} \overline{x}$ と定義する. *claim* により

$$S = \prod_{\overline{x}\in H} \overline{a}\,\overline{x} = \overline{a}^{p-1} \prod_{\overline{x}\in H} \overline{x} = \overline{a}^{p-1} \cdot S$$

両辺に S^{-1} をかけることによって

$$\overline{1} = S^{-1}\cdot S = \overline{a}^{p-1} S^{-1} S = \overline{a}^{p-1}$$

が得られる．したがって，$a^{p-1} \equiv 1 \pmod{p}$ である．

(ii) $p \mid a$ のとき，$a^p \equiv a \equiv 0 \pmod{p}$ である．

$p \nmid a$ のとき，(i) より $a^{p-1} \equiv 1 \pmod{p}$ である．

よって $a^p \equiv a \pmod{p}$． □

例 2.4.4 $p = 13$ とする．$2^{12} \equiv 1 \pmod{13}$ が成り立つことを確認する．

$$2^4 = 16 \equiv 3 \pmod{13}$$

$$2^8 \equiv 3^2 \equiv 9 \pmod{13}$$

$$2^{12} \equiv 2^8 \times 2^4 \equiv 3 \cdot 9 \equiv 27 \equiv 1 \pmod{13}$$

§2.5 合同1次方程式

例題 2.5.1 次の合同式の解を求めよ．

(1) $2x \equiv 3 \pmod{5}$

(2) $4x \equiv 7 \pmod{10}$

(3) $4x \equiv 6 \pmod{10}$

解答

(1) $x_0 = 4$ とすると，x_0 は方程式を満たす $(\because\ 2 \cdot 4 = 8 \equiv 3 \pmod{5})$

任意の整数 x に対して

$$2x \equiv 3 \pmod{5} \iff 2x \equiv 2x_0 \pmod{5}$$

$$\iff 2(x - x_0) \equiv 0 \pmod{5}$$

$$\iff x - x_0 \equiv 0 \pmod{5}$$

2と5は互いに素である

よって，$2x \equiv 3 \pmod 5 \iff x \equiv 4 \pmod 5$ である．

方程式 (1) の全ての解は $x = 5k + 4 \ (k \in \mathbb{Z})$ である．

(2) $4x \equiv 7 \pmod{10}$ ならば，$4x = 7 + 10k$ となる $k \in \mathbb{Z}$ が存在する．$4x$ は偶数であり，$7 + 10k$ は奇数であるので，矛盾する．よって，方程式 (2) は解をもたない．

(3)
$$\begin{aligned} 4x \equiv 6 \pmod{10} &\iff 4x = 6 + 10k \quad (\exists k \in \mathbb{Z}) \\ &\iff 2x = 3 + 5k \quad (\exists k \in \mathbb{Z}) \\ &\iff 2x \equiv 3 \pmod 5 \\ &\iff x \equiv 4 \pmod 5 \end{aligned}$$
(1)

定理 2.5.2 $n \geq 1$ を自然数とし，a, b を整数とする．次の合同方程式を考える．

$$ax \equiv b \pmod n \qquad (*)$$

(1) $\gcd(a, n) = 1$ のとき，$(*)$ は解をもつ．また，$c \in \mathbb{Z}$ が存在し，任意の $x \in \mathbb{Z}$ に対して

$$x \text{ が } (*) \text{ を満たす} \iff x \equiv c \pmod n$$

が成り立つ．

(2) $d := \gcd(a, n) \geq 2$ とする．このとき，

$$(*) \text{ は解をもつ} \iff d \mid b$$

である．

(3) $d = \gcd(a, n) \geq 2$ とし，$d \mid b$ とする．$a = da'$，$n = dn'$，$b = db'$ と表しておく．このとき，$c' \in \mathbb{Z}$ が存在し，任意の $x \in \mathbb{Z}$ に対して

$$x \text{ が } (*) \text{ を満たす} \iff x \equiv c' \pmod{n'}$$

が成り立つ．

証明

(1) $\gcd(a,n)=1$ とする. $ar+ns=1$ となる $r,s\in\mathbb{Z}$ が存在する. よって,

$$ax\equiv b \pmod n \iff axr\equiv br \pmod n \quad \because \gcd(r,n)=1$$
$$\iff x\equiv br \pmod n \quad \because ar\equiv 1 \pmod n$$

$c=br$ とおけば良い. 例えば, $x=c$ は $(*)$ の解である.

(2) ($\Rightarrow$) $ax\equiv b \pmod n$ とする. $ax=b+nk$ となる $k\in\mathbb{Z}$ が存在する.

$d\mid a$ かつ $d\mid n$ より, $d\mid b$ となる.

($\Leftarrow$) $d\mid b$ とし, $a=da'$, $n=dn'$, $b=db'$ と表す. このとき,

$$ax\equiv b \pmod n \iff n\mid ax-b$$
$$\iff n'\mid a'x-b'$$
$$\iff a'x\equiv b' \pmod{n'}$$

である.

a' と n' は互いに素であるので, (1) より $(*)$ は解をもつ.

(3) (1) から従う. □

§2.6 中国の剰余定理

定理 2.6.1 (中国の剰余定理) $n_1, n_2, \dots, n_d$ を自然数とし，どの二つも互いに素であるとする（すなわち $i \neq j \Rightarrow \gcd(n_i, n_j) = 1$）．また，$a_1, a_2, \dots, a_d \in \mathbb{Z}$ とする．

このとき，以下の合同方程式を満たす整数 $x \in \mathbb{Z}$ が存在する．

$$(*) \quad \begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_d \pmod{n_d} \end{cases}$$

また，$n = n_1 n_2 \cdots n_d$ を法としては x が一意的に存在する．

証明・x の存在性：

$d \geq 1$ に関する帰納法により証明する．$d = 1$ のときに明らかである．

$d = 2$ とする．n_1 と n_2 が互いに素だから，$rn_1 + sn_2 = 1$ となる $r, s \in \mathbb{Z}$ が存在する．よって，$rn_1 \equiv 1 \pmod{n_2}$ かつ $sn_2 \equiv 1 \pmod{n_1}$ である．

$x = rn_1a_2 + sn_2a_1$ とおくと

$$\begin{cases} x \equiv sn_2a_1 \equiv a_1 \pmod{n_1} \\ x \equiv rn_1a_2 \equiv a_2 \pmod{n_2} \end{cases} \quad (A)$$

今，$d \geq 3$ として，$d-1$ までは主張が正しいと仮定をする．

仮定より，$y \equiv a_1 \pmod{n_1}, \dots, y \equiv a_{d-1} \pmod{n_{d-1}}$ を満たす $y \in \mathbb{Z}$ が存在する．$n' = n_1 n_2 \cdots n_{d-1}$ とおくと，n' と n_d が互いに素である．

$d = 2$ の場合より

$$\begin{cases} x \equiv y \pmod{n'} \\ x \equiv a_d \pmod{n_d} \end{cases}$$

となる $x \in \mathbb{Z}$ が存在する．

とくに $i = 1, 2, \dots, d-1$ に対して $x \equiv y \equiv a_i \pmod{n_i}$ が成り立つので，x の存在性が示せた．(B)

- n を法とした x の一意性

y を $(*)$ の他の解とする．このとき，全ての $i=1,2,\dots,d$ に対して

$x \equiv y \pmod{n_i}$ が成り立つ．よって，$x-y$ が $n_1, n_2, \dots, n_d$ で割り切れる．

$n_1, n_2, \dots, n_d$ は互いに素であるので，$n = n_1 n_2 \cdots n_d \mid x-y$ となる．

すなわち，$x \equiv y \pmod{n}$ である． □

例題 2.6.2. 以下の合同方程式の全ての解を求めよ．

$$(E) \begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 1 \pmod 5 \\ x \equiv 3 \pmod{12} \end{cases}$$

また，(E) を満たす最小の自然数を求めよ．

解答 $7, 5, 12$ は互いに素である．まず，合同方程式

$$(E') \begin{cases} y \equiv 2 \pmod 7 \\ y \equiv 1 \pmod 5 \end{cases}$$ を満たす y を探す．

$3\times 7 - 5\times 4 = 1$ である．(A) より $y = -5\times 4\times 2 + 3\times 7\times 1 = -19$ とおくと

y は (E') の解である．次に，以下の合同方程式を考える．

$$(E'') \begin{cases} x \equiv -19 \pmod{35} \\ x \equiv 3 \pmod{12} \end{cases}$$

$(-1)\times 35 + 3\times 12 = 1$ である．(A) より

$$\begin{aligned} x &= 3\times 12\times(-19) - 1\times 35\times 3 \\ &= -789 \end{aligned}$$

は (E'') の解である．また，(B) より x は (E) の解である．

定理 2.6.1 より，(E) の解全体の集合は

$$\mathcal{E} = \{ -789 + \underbrace{7\times 5\times 12}_{=840} k \mid k \in \mathbb{Z} \}$$

$\mathcal{E}$ の最小の自然数は $-789 + 840 = \boxed{51}$ である． □

$n_1, n_2 \in \mathbb{N}$ とし，$\gcd(n_1, n_2) = 1$ とする．次の写像を考える．

$$f : \mathbb{Z}/n_1n_2\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$
$$a + n_1n_2\mathbb{Z} \longmapsto (a + n_1\mathbb{Z},\ a + n_2\mathbb{Z})$$

- f は well-defined である： $a + n_1n_2\mathbb{Z} = a' + n_1n_2\mathbb{Z}$ $(a, a' \in \mathbb{Z})$ のとき
  $a + n_1\mathbb{Z} = a' + n_1\mathbb{Z}$ かつ $a + n_2\mathbb{Z} = a' + n_2\mathbb{Z}$ を確認しなければいけない．
  $a + n_1n_2\mathbb{Z} = a' + n_1n_2\mathbb{Z}$ とすると $a \equiv a' \pmod{n_1n_2}$ である．とくに $a \equiv a' \pmod{n_1}$
  かつ $a \equiv a' \pmod{n_2}$ となり，主張が従う．

- f は全射である： $a_1, a_2 \in \mathbb{Z}$ とする．定理 2.6.1 より
  $$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$
  を満たす $x \in \mathbb{Z}$ が存在する．よって，
  $$f(x + n_1n_2\mathbb{Z}) = (x + n_1\mathbb{Z},\ x + n_2\mathbb{Z}) = (a_1 + n_1\mathbb{Z},\ a_2 + n_2\mathbb{Z})$$

- f は単射である： $a, a' \in \mathbb{Z}$ とし，$f(a + n_1n_2\mathbb{Z}) = f(a' + n_1n_2\mathbb{Z})$ とする．
  このとき，$\begin{cases} a + n_1\mathbb{Z} = a' + n_1\mathbb{Z} \\ a + n_2\mathbb{Z} = a' + n_2\mathbb{Z} \end{cases}$ であり，ゆえに $\begin{cases} a \equiv a' \pmod{n_1} \\ a \equiv a' \pmod{n_2} \end{cases}$ である．
  定理 2.6.1 の「一意性」により $a \equiv a' \pmod{n_1n_2}$ が分かる．
  したがって $a + n_1n_2\mathbb{Z} = a' + n_1n_2\mathbb{Z}$ である．

より一般に，$n_1, n_2, \cdots, n_d \in \mathbb{N}$ とし，どの二つも互いに素であるとする．
$n = n_1 n_2 \cdots n_d$ とおく．次の写像を考える．

$$f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z}$$
$$a + n\mathbb{Z} \longmapsto (a + n_1\mathbb{Z}, a + n_2\mathbb{Z}, \cdots, a + n_d\mathbb{Z})$$

上と同様に，以下の命題が証明できる．

命題 2.6.3：f は全単射である．

§2.7 オイラーの φ 関数

$n \geq 1$ を自然数とし，a を整数とする．
命題 2.3.5 と 命題 1.4.2 より，以下の条件は互いに同値である．

(i) $\bar{a} = a + n\mathbb{Z}$ が $\mathbb{Z}/n\mathbb{Z}$ において可逆元である
(ii) $\gcd(a, n) = 1$
(iii) $ar + ns = 1$ となる $r, s \in \mathbb{Z}$ が存在する．

(*)

$\mathbb{Z}/n\mathbb{Z}$ の可逆元全体の集合を $(\mathbb{Z}/n\mathbb{Z})^\times$ で表す．すなわち，

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; \bar{a} \text{ は可逆元} \right\}$$
$$= \left\{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; \gcd(a, n) = 1 \right\}$$

注意 2.3.4 より，以下が常に成り立つ．

$\bar{0} \notin (\mathbb{Z}/n\mathbb{Z})^\times$
$\bar{1} \in (\mathbb{Z}/n\mathbb{Z})^\times$，$\overline{n-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$．

定義 2.7.1 与えられた自然数 n に対して，$(\mathbb{Z}/n\mathbb{Z})^\times$ の元の個数を $\varphi(n)$ で表す．つまり，

$$\varphi(n) = \left| (\mathbb{Z}/n\mathbb{Z})^\times \right| \quad \text{と定める．}$$

(*) より $\varphi(n) = \left\{ a \;\middle|\; 0 < a < n,\ \gcd(a, n) = 1 \right\}$ が成り立つ．

例 2.7.2 $n=8$ とする. $\mathbb{Z}/8\mathbb{Z} = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7}\}$

$(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1},\bar{3},\bar{5},\bar{7}\}$ である.

ゆえに $\varphi(8)=4$

補題 2.7.3 p を素数とし, $m \geq 1$ を自然数とする.

$$\varphi(p^n) = p^n - p^{n-1}$$ が成り立つ.

証明 $\varphi(p^n) = \left|\{a \in \{0,1,\dots,p^n-1\} \mid \gcd(a,p)=1\}\right|$

$= p^n - \left|\{a \in \{0,1,\dots,p^n-1\} \mid p \mid a\}\right|$ である.

$\{0,1,\dots,p^n-1\}$ の中で p の倍数は $\{p\cdot k \mid k=0,1,\dots,p^{n-1}-1\}$ である.

よって $\varphi(n) = p^n - p^{n-1}$ となる. □

n_1, n_2 を互いに素な自然数とする. 命題 2.6.3 より 写像

$$f: \mathbb{Z}/n_1n_2\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$
$$a+n_1n_2\mathbb{Z} \longmapsto (a+n_1\mathbb{Z}, a+n_2\mathbb{Z})$$

は全単射である.

補題 2.7.4 f は全単射 $(\mathbb{Z}/n_1n_2\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$ を引き起こす.

証明 $a+n_1n_2\mathbb{Z} \in (\mathbb{Z}/n_1n_2\mathbb{Z})^\times$ とすると, $\gcd(a,n_1n_2)=1$ である. とくに

$\gcd(a,n_1)=\gcd(a,n_2)=1$ となり, ゆえに $a+n_1\mathbb{Z} \in (\mathbb{Z}/n_1\mathbb{Z})^\times$ かつ $a+n_2\mathbb{Z} \in (\mathbb{Z}/n_2\mathbb{Z})^\times$ である. よって, f は写像 $(\mathbb{Z}/n_1n_2\mathbb{Z})^\times \xrightarrow{f'} (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$ を引き起こす. f が単射であるので, f' も単射である. また, f' が全射であることを示す. $a_1, a_2 \in \mathbb{Z}$ とし, $\gcd(a_1,n_1)=1$ かつ $\gcd(a_2,n_2)=1$ とする. f が全射なので

$$\begin{cases} a+n_1\mathbb{Z} = a_1+n_1\mathbb{Z} \\ a+n_2\mathbb{Z} = a_2+n_2\mathbb{Z} \end{cases}$$

を満たす $a \in \mathbb{Z}$ が存在する. $a+n_1n_2\mathbb{Z} \in \left(\mathbb{Z}/n_1n_2\mathbb{Z}\right)^\times$ を示せば良い.

$\gcd(a, n_1) = \gcd(a_1, n_1) = 1$ かつ $\gcd(a, n_2) = \gcd(a_2, n_2) = 1$ である.

補題 1.4.4 より $\gcd(a, n_1n_2) = 1$ となる. したがって, f' は全射である. □

命題 2.7.5 $n_1, n_2, \dots, n_d$ を自然数とし, どの2つも互いに素であるとする. また, $n = n_1n_2\cdots n_d$ とおく. このとき,

$$\varphi(n) = \varphi(n_1)\varphi(n_2)\cdots\varphi(n_d) \quad \text{が成り立つ.}$$

証明 まず $d = 2$ の場合を考える.

補題 2.7.4 より全単射 $\left(\mathbb{Z}/n_1n_2\mathbb{Z}\right)^\times \longrightarrow \left(\mathbb{Z}/n_1\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/n_2\mathbb{Z}\right)^\times$ が存在する. よって $\varphi(n_1n_2) = \left|\left(\mathbb{Z}/n_1n_2\mathbb{Z}\right)^\times\right| = \left|\left(\mathbb{Z}/n_1\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/n_2\mathbb{Z}\right)^\times\right| = \varphi(n_1)\varphi(n_2)$ となる.

よって $d = 2$ のとき主張は正しい. $d > 2$ のとき, 帰納法の仮定より $\varphi(n_1\cdots n_{d-1}) = \varphi(n_1)\cdots\varphi(n_{d-1})$ である. よって

$$\varphi(n_1\cdots n_d) = \varphi(n_1\cdots n_{d-1})\,\varphi(n_d) = \varphi(n_1)\cdots\varphi(n_{d-1})\varphi(n_d)$$

となり, 主張が従う. □

定理2.7.6 $n \geq 2$ を自然数とし，n の素因数分解を

$$n = p_1^{k_1} \cdots p_r^{k_r} \quad (p_1, \ldots, p_r : \text{互いに異なる素数}, \ k_1, \ldots, k_r \geq 1)$$

とする．このとき，

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

が成り立つ．

証明：命題2.7.5より $\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r})$ が成り立つ．

一方，補題2.7.3より $\varphi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i-1}$ である． □

§3. 群論の基礎

§3.1. 演算・モノイド

X を空でない集合とする．**X 上の演算**とは，写像 $f : X \times X \longrightarrow X$ のことをいう．

例えば $\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (x, y) & \longmapsto & x+y \end{array}$ は $\mathbb{Z}$ 上の演算である．

$x, y \in X$ のとき，$f(x,y)$ を単に $x \cdot y$ あるいは xy で表す場合がある．

定義 3.1.1 空でない集合 G に演算 $\cdot$ が与えられているとする．

任意の $x, y, z \in G$ に対して

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

が成り立つとき，$\cdot$ が**結合的**であるという．また，このとき $(G, \cdot)$ が**半群**とよばれる．

注意 3.1.2

演算 $\cdot$ が結合的であるとき，元 $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ を単に $x \cdot y \cdot z$ で表す．同様に，積 $x_1 \cdot x_2 \cdots x_n$ $(x_i \in G)$ はカッコの付け方に依らない．

$(G, \cdot)$ を半群とする．元 $e \in G$ が**単位元**であるとは，任意の $x \in G$ に対して

$$x \cdot e = e \cdot x = x$$

が成り立つことをいう．

補題 3.1.3 e と e' を半群 G の単位元とする．このとき $e = e'$ が成り立つ．

ゆえに単位元は高々一つ存在する．

証明　$e \overset{e'\text{:単位元}}{=} e \cdot e' \overset{e\text{:単位元}}{=} e'$ である．　□

定義 3.1.4　単位元をもつ半群はモノイドとよぶ．

例 3.1.5

- $(\mathbb{N}, +)$ はモノイドである．単位元は 0 である（∵ 全ての $n \in \mathbb{N}$ に対して $n+0 = 0+n = n$ である）．
- $(\mathbb{Z}, \times)$ はモノイドである．単位元は 1 である（∵ $k \times 1 = 1 \times k = k$, $\forall k \in \mathbb{Z}$）

§3.2 逆元，群

G をモノイドとし，G の単位元を e とおく．また，x を G の元とする．元 $y \in G$ が x の**逆元**であるとは，

$$x \cdot y = y \cdot x = e$$

が成り立つことをいう．逆元をもつ元は**可逆元**とよぶ．

補題 3.2.1　G をモノイドとし，$x \in G$ を可逆元とする．x の逆元は一意的に存在する．

証明：y と y' を x の逆元とする．

$y = y \cdot e = y \cdot (x \cdot y') = (y \cdot x) \cdot y' = e \cdot y' = y'$ である．　□

注意 3.2.2

(i) x が可逆元であるとき，x の逆元を x^{-1} で表す．

(ii) 単位元 e は常に可逆元であり，$e^{-1}=e$ が成り立つ．

(iii) x が可逆元ならば，x^{-1} も可逆元である．また，$(x^{-1})^{-1}=x$ である．

(iv) x と y が可逆元ならば，$x\cdot y$ も可逆元である．また，

$$(x\cdot y)^{-1}=y^{-1}\cdot x^{-1}$$

である．

例 3.2.3

- モノイド $(\mathbb{N},+)$ の可逆元全体の集合は $\{0\}$ である．
  （∵ $n+m=0$ を満たす $n,m\in\mathbb{N}$ は $n=m=0$ の場合に限る．）
- モノイド $(\mathbb{Z},\times)$ の可逆元全体の集合は $\{-1,1\}$ である．
  （∵ $n\times m=1 \Rightarrow n\in\{-1,1\}$ ）
- $M_n(\mathbb{C})$ を n 次複素正方行列の集合とする．行列の積に関して $M_n(\mathbb{C})$ はモノイドを公す．その単位元は単位行列である．行列 $M\in M_n(\mathbb{C})$ に対して，以下が成り立つ

M がモノイド $M_n(\mathbb{C})$ の可逆元である $\iff$ M が正則行列である．

定義 3.2.4 全ての元が可逆元であるようなモノイドは群とよぶ．

例 3.2.5

- $(\mathbb{Z}, +)$ は群である ($\because$ $n + (-n) = 0$ より n は可逆元である).
- $n \geqslant 1$ とする. 同様に, $(\mathbb{Z}/n\mathbb{Z}, +)$ は群である.
- $(GL_n(\mathbb{C}), \times)$ は群である ($\because$ $M \in GL_n(\mathbb{C})$ の逆元は M の逆行列である.)

定義 3.2.6 G_1, G_2 を群とする. $g_1, g_1' \in G_1$, $g_2, g_2' \in G_2$ に対して

$$(g_1, g_2) \cdot (g_1', g_2') \overset{\text{def}}{=} (g_1 \cdot g_1', g_2 \cdot g_2')$$

として, 直積集合 $G_1 \times G_2$ に演算を入れる. こうすると $G_1 \times G_2$ は群をなし, G_1 と G_2 の**直積**という.

補題 3.2.7 H をモノイドとし,

$$G = \{ x \in H \mid x \text{ は可逆元である} \}$$

とおく. このとき, G は H の演算に関して群をなす.

証明: 注意 3.2.2 (iv) より $x, y \in G \Rightarrow x \cdot y \in G$ である.

よって, H の演算 $H \times H \longrightarrow H$, $(x, y) \mapsto x \cdot y$ は G 上の演算 $G \times G \longrightarrow G$, $(x, y) \mapsto x \cdot y$ を引き起こす.

注意 3.2.2 (ii) より $e \in G$ である.

注意 3.2.2 (iii) より $x \in G \Rightarrow x^{-1} \in G$ である.

したがって, $(G, \cdot)$ は群である. □

例 3.2.8 $(\mathbb{Z}/n\mathbb{Z}, \times)$ はモノイドであり，その単位元は $\overline{1}$ である．このモノイドの可逆元全体の部分集合は $(\mathbb{Z}/n\mathbb{Z})^\times$ である．

補題 3.2.7 より

$\left((\mathbb{Z}/n\mathbb{Z})^\times, \times\right)$ は群である．

まとめると，

- $\mathbb{Z}/n\mathbb{Z}$ は加法 $+$ に関して群をなす．
- $(\mathbb{Z}/n\mathbb{Z})^\times$ は乗法 $\times$ に関して群をなす．

記号 G を群とする．$x \in G$，$n \in \mathbb{Z}$ について

$$x^n = \begin{cases} e & \text{if } n = 0 \\ \underbrace{x \cdots x}_{n\text{コ}} & \text{if } n > 0 \\ \underbrace{x^{-1} \cdots x^{-1}}_{n\text{コ}} & \text{if } n < 0 \end{cases}$$

例えば，$x^{-2} = x^{-1} \cdot x^{-1} = (x^{-1})^2 = (x^2)^{-1}$ である．

定義 3.2.9 G を群とする．任意の $x, y \in G$ に対して

$$x \cdot y = y \cdot x$$

が成り立つとき，G がアーベル群（または可換群）であるという．

例 3.2.10

- $(\mathbb{Z}/n\mathbb{Z}, +)$ と $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ はアーベル群である.
- $(\mathbb{C}^\times, \times)$ はアーベル群である.
- $(GL_2(\mathbb{C}), \times)$ はアーベル群でない ($\because$ $x = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ と $y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ とおくと
  $x \cdot y = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$ かつ $y \cdot x = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \neq x \cdot y$)

記号 アーベル群の演算を・の代わりに + で表す場合がある.
演算を + で表すときに, 合わせて

単位元	を	0	で,
x の逆元 x^{-1}	を	$-x$	で,
x の n 乗 x^n	を	nx	で
xy^{-1}	を	$x-y$	で表す.

§3.3 部分群

定義 3.3.1 G を群とし, $H \subset G$ を部分集合とする. H が G の部分群であるとは, 以下が成り立つことをいう.

(i) G の単位元が H に属する: $e \in H$.

(ii) H が演算に対して閉じている: $x, y \in H \Rightarrow x \cdot y \in H$.

(iii) H が逆元に対して閉じている: $x \in H \Rightarrow x^{-1} \in H$.

補題 3.3.2 Gを群とし，$H \subset G$を部分集合とする．次の条件は互いに同値である．

(i) HがGの部分群である．

(ii) $H \neq \emptyset$ かつ「$x, y \in H$ ならば $xy^{-1} \in H$」が成り立つ．

証明

(i) $\Rightarrow$ (ii) は簡単である．

(ii) $\Rightarrow$ (i) : $H \neq \emptyset$ より $x \in H$ がとれる．仮定より $x \cdot x^{-1} = e$ がHに属する．よって，任意の$x \in H$に対して，$e \cdot x^{-1} = x^{-1} \in H$ である．最後に，$x, y \in H$とする．$y^{-1} \in H$ より $x \cdot (y^{-1})^{-1} = xy \in H$ である．

以上より，HはGの部分群である．

注意 3.3.3 Gを群とする．$\{e\}$（単位元）と G は常にGの部分群である．

例題 3.3.4 以下のいずれの場合に，HがGの部分群であるかどうか判定せよ．

(i) $G = \mathbb{Z}$ (演算：加法)，$H = \mathbb{N}$．

(ii) $G = \mathbb{Q}^{\times}$ (演算：乗法)，$H = \mathbb{R}_{>0}$ (正の有理数全体の集合)．

(iii) $G = (\mathbb{Z}/7\mathbb{Z})^{\times}$ (演算：乗法)，$H = \{\overline{1}, \overline{2}, \overline{4}\}$．

(iv) $G = GL_2(\mathbb{R})$，$H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid (a, b) \in \mathbb{R}^2,\ (a, b) \neq (0, 0) \right\}$．

解答

(i) G の単位元は 0 である．$x=1$ とすると，x の逆元は -1 である．
$-1 \notin \mathbb{N}$ より $\mathbb{N}$ は $(\mathbb{Z},+)$ の部分群でない．

(ii) $x, y \in \mathbb{Q}_{>0}$ とする．このとき $xy^{-1} = \frac{x}{y} \in \mathbb{Q}_{>0}$ である．
よって $\mathbb{Q}_{>0}$ は $(\mathbb{Q}^{\times}, \times)$ の部分群である．

(iii) $\overline{2}\cdot\overline{4} = \overline{1}$ より $(\overline{2})^{-1} = \overline{4}$ かつ $(\overline{4})^{-1} = \overline{2}$ である．
また，$\overline{2}\times\overline{2} = \overline{4} \in H$
$\overline{4}\times\overline{4} = \overline{16} = \overline{2} \in H$ である．
よって，H は $\left((\mathbb{Z}/7\mathbb{Z})^{\times}, \times\right)$ の部分群である．

(iv) $\det\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2+b^2$ である．$(a,b)\neq(0,0)$ より $\det\begin{pmatrix} a & b \\ -b & a \end{pmatrix} > 0$
であり，ゆえに $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in GL_2(\mathbb{R})$ である．$(a_i, b_i) \neq (0,0)$ とする $(i=1,2)$

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}^{-1}\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} = \frac{1}{a_1^2+b_1^2}\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{a_1a_2+b_1b_2}{a_1^2+b_1^2} & \frac{a_1b_2-a_2b_1}{a_1^2+b_1^2} \\ \frac{a_2b_1-a_1b_2}{a_1^2+b_1^2} & \frac{a_1a_2+b_1b_2}{a_1^2+b_1^2} \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad \left(\text{ただし } a = \frac{a_1a_2+b_1b_2}{a_1^2+b_1^2},\ b = \frac{a_1b_2-a_2b_1}{a_1^2+b_1^2}\right)$$

したがって，H は G の部分群である．

§3.4 部分集合で生成される部分群

補題 3.4.1 H_1 と H_2 を群 G の部分群とする．このとき，
$H_1 \cap H_2$ は G の部分群である．

証明 $e \in H_1$ かつ $e \in H_2$ より $e \in H_1 \cap H_2$ である．$x, y \in H_1 \cap H_2$ とする．H_i が部分群なので $xy^{-1} \in H_i$ $(i=1,2)$ である．ゆえに $xy^{-1} \in H_1 \cap H_2$ となる．補題 3.3.2 より $H_1 \cap H_2$ は G の部分群である． □

より一般的に，$\mathcal{F} \neq \emptyset$ を G の部分群からなる集合とする（例えば $\mathcal{F} = \{H_1, H_2, \dots, H_n\}$，$H_i$：$G$ の部分群）．このとき，

$$\bigcap_{H \in \mathcal{F}} H \quad \text{は } G \text{ の部分群である．} \qquad (\not\Rightarrow)$$

定義 3.4.2 G を群とし，$S \subset G$ を部分集合とする．

$$\mathcal{F} = \left\{ H \;\middle|\; \begin{array}{l} H \text{ は } G \text{ の部分群である．} \\ S \subset H \end{array} \right\} \quad \text{とおく．}$$

S で生成される部分群 は $\langle S \rangle$ で表し，

$$\langle S \rangle = \bigcap_{H \in \mathcal{F}} H \qquad \text{と定義される．}$$

つまり，$\langle S \rangle$ は S を含む G の部分群全体の共通部分として定義される．

注意 3.4.3

(i) 定義 3.4.2 の $\mathcal{F}$ について $G \in \mathcal{F}$ が成り立つので，
$\mathcal{F}$ は空でない．

(ii) (*) より $\langle S \rangle$ は G の部分群である．

(iii) $\langle S \rangle$ は S を含む G の部分群の中で最小のものである．
つまり，G の任意の部分群 H に対して，$S \subset H$ であるならば $\langle S \rangle \subset H$
が成り立つ．なぜならば，

$$S \subset H \Rightarrow H \in \mathcal{F} \Rightarrow \langle S \rangle \subset H .$$

($\mathcal{F}$：定義 3.4.2 の $\mathcal{F}$)

(iv) $S = \{x_1, x_2, \cdots, x_n\}$ $(x_i \in G)$ のとき，$\langle S \rangle$ を単に $\langle x_1, \cdots, x_n \rangle$ で表す．

(v) $G = \langle S \rangle$ のとき，**G が S で生成される** という．

命題 3.4.4 G を群とし，$S \subset G$ を空でない部分集合とする．このとき，

$$\langle S \rangle = \left\{ s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n} \;\middle|\; n \geq 1,\ s_i \in S,\ k_i \in \mathbb{Z} \right\} \quad (*)$$

が成り立つ．

証明 (*) で定まる集合を T とおき，$\langle S \rangle = T$ を示す．
H は部分群で，$S \subset H$ とする．$s_i \in S$, $k_i \in \mathbb{Z}$ $(i = 1, \cdots, n)$ に対して，$s_1^{k_1} \cdots s_n^{k_n} \in H$ である．よって，$T \subset \bigcap_{\substack{S \subset H \\ H:\text{部分群}}} H = \langle S \rangle$.

§3.5 $\mathbb{Z}$ の部分群

$m \in \mathbb{Z}$ とすると，$\mathbb{Z}$ において m で生成される部分群は

$$\langle m \rangle = m\mathbb{Z} = \{ mk \mid k \in \mathbb{Z} \}$$

である．

定理 3.5.1 $H \subset \mathbb{Z}$ を部分群とする．このとき，$H = m\mathbb{Z}$ となる $m \in \mathbb{Z}$ $(m \geq 0)$ が存在する．

証明 $H = \{0\}$ のとき $m = 0$ とおけばよい．

$H \neq \{0\}$ とする．$k \in H$ ならば $\pm k \in H$ であるので，集合 $H \cap \mathbb{N}$ は空でない．m を $H \cap \mathbb{N}$ の最小元とし，$H = m\mathbb{Z}$ を示す．$m \in H$ より $m\mathbb{Z} \subset H$ である．

逆に，$k \in H$ とする．$k = qm + r$ $(0 \leq r < m-1)$ を満たす整数 q, r が存在する．

$$r = \underbrace{k}_{\in H} - \underbrace{qm}_{\in H}$$ が成り立つ．

H は部分群なので，$r \in H$ となる．m の最小性より $r = 0$ が分かる．よって $k = qm \in m\mathbb{Z}$ である． □

補題 3.5.2 $m, n \in \mathbb{Z}$ とする．

$$m \mid n \iff n\mathbb{Z} \subset m\mathbb{Z}$$ が成り立つ．

証明 ($\Rightarrow$) $n = mk$ $(k \in \mathbb{Z})$ とする. $r \in \mathbb{Z}$ とすると $nr = mkr \in m\mathbb{Z}$ である.
よって $n\mathbb{Z} \subset m\mathbb{Z}$ となる.

($\Leftarrow$) $n\mathbb{Z} \subset m\mathbb{Z}$ とすると $n \in m\mathbb{Z}$ であり, ゆえに $n = mk$ $(k \in \mathbb{Z})$ と表せる. □

$m, n \in \mathbb{Z}$ とする. 命題 3.4.4 より, 部分集合 $\{m, n\}$ で生成された部分群は以下のように表される

$$\langle m, n \rangle = \mathbb{Z}m + \mathbb{Z}n = \left\{ am + bn \mid a, b \in \mathbb{Z} \right\}$$

定理 3.5.3 $m, n \in \mathbb{Z}$ とする. 以下が成り立つ.

(i) $\mathbb{Z}m + \mathbb{Z}n = \gcd(n, m)\mathbb{Z}$

(ii) $\mathbb{Z}m \cap \mathbb{Z}n = \mathrm{lcm}(n, m)\mathbb{Z}$

証明

(i) 定理 3.5.1 より $\mathbb{Z}m + \mathbb{Z}n = d\mathbb{Z}$ となる $d \in \mathbb{Z}$ が存在する.
また, $d\mathbb{Z} = (-d)\mathbb{Z}$ より, $d \geq 0$ を仮定して良い. d' を n と m の公約数とする.
$n\mathbb{Z} \subset d\mathbb{Z}$ かつ $m\mathbb{Z} \subset d\mathbb{Z}$ より $d \mid n$ かつ $d \mid m$ がいえる. よって,
$d \mid d'$ となる. また, $n\mathbb{Z} \subset d'\mathbb{Z}$ かつ $m\mathbb{Z} \subset d'\mathbb{Z}$ であるので,

$$n\mathbb{Z} + m\mathbb{Z} \subset d'\mathbb{Z}$$

となる. ゆえに $d\mathbb{Z} \subset d'\mathbb{Z}$ である. つまり $d' \mid d$ が成り立つ. 以上より
$d = d' = \gcd(n, m)$ が分かる.

(ii) $\mathbb{Z}m \cap \mathbb{Z}n$ は $\mathbb{Z}$ の部分群なので，$n\mathbb{Z} \cap m\mathbb{Z} = l\mathbb{Z}$ となる $l \in \mathbb{Z}$ が存在する．また，$l \geq 0$ を仮定して良い．l' を n と m の公倍数とする．$l\mathbb{Z} \subset n\mathbb{Z}$ かつ $l\mathbb{Z} \subset m\mathbb{Z}$ より $n \mid l$ かつ $m \mid l$ である．よって $l' \leq l$ である．$l'\mathbb{Z} \subset n\mathbb{Z}$ かつ $l'\mathbb{Z} \subset m\mathbb{Z}$ が成り立つので，

$$l'\mathbb{Z} \subset n\mathbb{Z} \cap m\mathbb{Z}$$

となり，ゆえに $l'\mathbb{Z} \subset l\mathbb{Z}$ である．つまり $l \mid l'$ である．したがって $l = l' = \mathrm{lcm}(n,m)$ が分かる． □

注意 3.5.4 定理 3.5.3 より，任意の $n, m \in \mathbb{Z}$ に対して

$$\gcd(n,m) = 1 \iff n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$$ が成り立つ．

§4 ラグランジュの定理

§4.1 部分群による剰余類

G を群とし，$H \subset G$ を部分群とする．また，$g \in G$ とする．集合

$$gH = \{ g \cdot h \mid h \in H \}$$
$$Hg = \{ h \cdot g \mid h \in H \}$$

はそれぞれ（H による）**左剰余類**，**右剰余類** とよぶ．

$g_1, g_2 \in G$ に対して

$$g_1 \sim g_2 \iff g_2 = g_1 h \text{ となる } h \in H \text{ が存在}$$
$$g_1 \sim' g_2 \iff g_2 = h g_1 \text{ となる } h \in H \text{ が存在}$$

として，G 上の2項関係 $\sim$ と $\sim'$ をそれぞれ定義する．

補題 4.1.1 $\sim$ と $\sim'$ はそれぞれ同値関係である．

証明 $\sim$ が同値関係であることを示す（$\sim'$ の場合は同様である）．

- 反射性：$g \in G$ とすると，$g = g \cdot e$（$e \in H$）より $g \sim g$ である．
- 対称性：$g_1 \sim g_2$ とする（$g_1, g_2 \in G$）．このとき $g_2 = g_1 \cdot h$（$h \in H$）と表せる．
  よって $g_2 \cdot h^{-1} = (g_1 \cdot h) \cdot h^{-1} = g_1 \cdot (h \cdot h^{-1}) = g_1 \cdot e = g_1$ となり，$g_2 \sim g_1$ が成り立つ．（$h^{-1} \in H$）
- 推移性：$g_1 \sim g_2$ かつ $g_2 \sim g_3$ とする（$g_1, g_2, g_3 \in G$）．このとき，
  $g_2 = g_1 \cdot h$ かつ $g_3 = g_2 \cdot h'$ となる $h, h' \in H$ が存在する．よって
  $$g_3 = g_2 \cdot h' = (g_1 \cdot h) \cdot h' = g_1 \cdot (h \cdot h')$$
  （$h \cdot h' \in H$）
  よって $g_1 \sim g_3$ である．

□

補題 4.1.2 $g \in G$ とする.

(i) 同値関係 $\sim$ による同値類で, g を含むものは左剰余類 gH と一致する

(ii) ―― $\sim'$ ―― 右剰余類 Hg ――

証明 (i) を示す ((ii) は同様である). g を含む同値類は

$\{ g' \in G \mid g' \sim g \}$ である. $g' \sim g \Leftrightarrow \exists h \in H,\ g' = g \cdot h \Leftrightarrow g' \in gH$. □

記号

G/H : H による左剰余類全体の集合.

$H\backslash G$: H による右剰余類全体の集合.

2つの元 $g_1, g_2 \in G$ に対して, 以下が成り立つ.

$$g_1 H = g_2 H \Leftrightarrow g_1 \sim g_2 \Leftrightarrow g_2 = g_1 \cdot h \quad (\exists h \in H)$$

$$H g_1 = H g_2 \Leftrightarrow g_1 \sim' g_2 \Leftrightarrow g_2 = h \cdot g_1 \quad (\exists h \in H)$$

補題 4.1.3 以下の写像は well-defined であり, 全単射である.

$$G/H \longrightarrow H\backslash G$$

$$gH \longmapsto Hg^{-1}$$

証明

- well-defined 性 : $g_1H = g_2H$ とすると $g_2 = g_1 \cdot h$ $(h \in H)$ と表せる.
  よって $g_2^{-1} = h^{-1} \cdot g_1^{-1}$ であり, ゆえに $Hg_2^{-1} = Hg_1^{-1}$ である.
- 単射 : $Hg_1^{-1} = Hg_2^{-1}$ とすると $g_2^{-1} = h \cdot g_1^{-1}$ となる $h \in H$ が存在する.
  よって $g_2 = g_1 \cdot h^{-1}$ となり, $g_2H = g_1H$ が成り立つ.
- 全射 : 明かである. □

$\{g_i\}_{i \in I}$ を同値関係 $\sim$ についての完全代表系とする.
G が同値類に分割されるので

$$G = \bigsqcup_{i \in I} g_i H$$

同様に, G が右剰余類に分割される.

§4.2 位数

定義 4.2.1 G を群とする.

(i) G が有限であるとき, G の元の個数を **G の位数** という.
G が無限であるとき, G の **位数が無限** であるという.

(ii) $g \in G$ とする. **g の位数** とは, $\langle g \rangle$ の位数のことをいう.
g の位数を $\mathrm{ord}(g)$ で表す $(\mathrm{ord}(g) \in \mathbb{N} \cup \{\infty\})$

定理 4.2.2 G を群とし，$g \in G$ とする．

(i) $\mathrm{ord}(g)$ が有限 $\iff$ $g^n = e$ となる整数 $n \geq 1$ が存在．

(ii) $\mathrm{ord}(g)$ が有限であるとし，$m = \mathrm{ord}(g)$ とおく．このとき

$$m = \min \{ k \geq 1 \mid g^k = e \}$$

が成り立つ．

証明

(i) ($\Rightarrow$) を示す．$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \}$ である．$\langle g \rangle$ が有限であるので $g^{n_1} = g^{n_2}$ となる $n_1 \neq n_2$ が存在する．$n_1 > n_2$ を仮定して良い．g^{-n_2} を両辺にかけて $g^{n_1 - n_2} = g^{n_2 - n_2} = e$ が分かる．$n = n_1 - n_2$ とおけば良い．

($\Leftarrow$) を示す．$g^n = 1$ $(n \geq 1)$ とする．このとき，

(*) $\langle g \rangle = \{ e, g, \cdots, g^{n-1} \}$ を示す．

「つ」は明かである．

逆に，$k \in \mathbb{Z}$ とし，g^k を考える．割り算の定理より $k = nq + r$ (ただし $0 \leq r < n-1$) となる $q, r \in \mathbb{Z}$ が存在する．

ゆえに $g^k = g^{nq+r} = (g^n)^k \cdot g^r = e^k \cdot g^r = g^r \in \{ e, g, \cdots, g^{n-1} \}$ である．

(ii) $n = \min \{ k \geq 1 \mid g^k = e \}$ とおき，$m = n$ を示す．(*) より $\langle g \rangle = \{ e, g, \cdots, g^{n-1} \}$ である．また，$e, g, \cdots, g^{n-1}$ が互いに異なることを確認する．$0 \leq a, b \leq n-1$ とし $g^a = g^b$ とする．

$a \geq b$ を仮定して良い. g^{-b} をかけて, $g^{a-b} = g^{b-b} = e$ が得られる.
$0 \leq a-b < n-1$ だから, n の最小性より $a-b=0$ であり,
$a=b$ である. よって, $e, g, \cdots, g^{n-1}$ は互いに異なる.
したがって,

$$m = |\langle g \rangle| = |\{e, g, \cdots, g^{n-1}\}| = n$$

となる □

例題 4.2.3 $G = GL_2(\mathbb{R})$ とし, $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ とおく.
a, b, $a \cdot b$ のそれぞれの位数を求めよ.

解答

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

よって $ord(a) = 4$ である.

$b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, $b^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

よって $ord(b) = 3$ である.

$a \cdot b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ である. 帰納法で $(a \cdot b)^n = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ が成り立つ.

よって $ord(a \cdot b) = \infty$ である.

§4.3 指数

定義 4.3.1 G を群とし, $H \subset G$ を部分群とする. G/H の元の個数は G における H の指数といい, $[G : H]$ で表す. すなわち,

$$[G : H] = |G/H| \quad \left(= |H \backslash G| \right)$$

と定める.

↑ 補題 4.1.3

定理 4.3.2 G を有限群とする.

$$|G| = [G : H] \cdot |H|$$ が成り立つ.

証明 $\{g_1H, \dots, g_mH\}$ を H による左剰余類全体の集合（ただし，g_iH が互いに異なるとする）．

$$G = g_1H \sqcup g_2H \sqcup \dots \sqcup g_mH$$

が成り立つ．また，任意の $g \in G$ に対して

$$\boxed{|gH| = |H|}$$

であることを示す．次の写像は全単射である．　$\varphi : H \longrightarrow gH,\ h \longmapsto g \cdot h$

- 単射：$g \cdot h_1 = g \cdot h_2 \xRightarrow{g^{-1}\text{をかけて}} h_1 = h_2$．
- 全射：明か．

したがって，$|G| = \sum_{i=1}^{m} |g_iH| = m \cdot |H| = [G:H] \cdot |H|$ である　□

系 4.3.3　G を有限群とし，H を部分群とする．
このとき，$|H|$ が $|G|$ の約数である．

定理 4.3.4（ラグランジュの定理）　G を有限群とし，その位数を n とおく．このとき，全ての $g \in G$ に対して

$$\boxed{g^n = e}$$

が成り立つ．

証明　$H = \langle g \rangle$ とおき，$m = ord(g) = |H|$ とおく．
$r = [G:H]$ とおくと $n = m \cdot r$ である．よって

$$g^n = g^{m \cdot r} = (g^m)^r = e^r = e$$

である　□

命題 4.3.5 n を自然数とし，$m \in \mathbb{Z}$ とする．$\gcd(n,m)=1$ のとき，

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$ が成り立つ．

証明 $G=(\mathbb{Z}/n\mathbb{Z})^\times$ とする．G の位数は $\varphi(n)$ である．
$\gcd(n,m)=1$ とし，$\overline{m} = m+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ を考える．
定理 4.3.4 より $\overline{m^{\varphi(n)}} = \overline{m}^{\varphi(n)} = \overline{1}$ である．主張が従う． □

例 4.3.6 $n=12$ とする．$\varphi(12)=\varphi(3\times 4)=\varphi(3)\times\varphi(4)=2\times 2=4$.
ゆえに，$\gcd(12,m)=1$ であるような m に対して $m^4 \equiv 1 \pmod{12}$ である．

§5 準同型写像

§5.1 定義

定義 5.1.1 G_1, G_2 を群とし，$f: G_1 \longrightarrow G_2$ を写像とする．
f が群準同型であるとは，

$$f(x\cdot y) = f(x)\cdot f(y) \quad (x,y \in G_1)$$

が成り立つことをいう．

補題 5.1.2 $f : G_1 \longrightarrow G_2$ を群準同型とする.

(i) $f(e_1) = e_2$ (ただし e_i は G_i の単位元である)

(ii) $f(g^{-1}) = f(g)^{-1}$ $(g \in G_1)$ が成り立つ.

証明

(i) $f(e_1) = f(e_1 \cdot e_1) = f(e_1) \cdot f(e_1)$ である. $f(e_1)^{-1}$ を両辺にかけて, $e_2 = f(e_1)$ が得られる.

(ii) $e_2 = f(e_1) = f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1})$ である. よって $f(g^{-1}) = f(g)^{-1}$ が成り立つ. □

例 5.1.3

- $\det : GL_n(\mathbb{C}) \longrightarrow \mathbb{C}^*$ は群準同型である.

  $\left[\because \det(AB) = \det(A)\det(B) \right]$

- $f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ は群準同型である.

  $k \longmapsto \overline{k} = k + n\mathbb{Z}$

  $\left[\because f(k_1+k_2) = \overline{k_1+k_2} = \overline{k_1} + \overline{k_2} = f(k_1) + f(k_2) \right]$

- $\mathrm{sgn} : \mathfrak{S}_n \longrightarrow \{\pm 1\}$ は群準同型である.

  $\sigma \longmapsto \mathrm{sgn}(\sigma)$

  $\left[\because \mathrm{sgn}(\sigma_1\sigma_2) = \mathrm{sgn}(\sigma_1)\,\mathrm{sgn}(\sigma_2) \right]$

§5.2 核・像

定義 5.2.1 $f : G_1 \longrightarrow G_2$ を群準同型とする.

(i) f の**核**: $\mathrm{Ker}(f) = \{ x \in G_1 \mid f(x) = e_2 \}$ (ただし, e_2 は G_2 の単位元である)

(ii) f の**像**: $\mathrm{Im}(f) = \{ f(x) \mid x \in G_1 \} = f(G_1)$

補題 5.2.2 $f : G_1 \longrightarrow G_2$ を群準同型とする.

(i) $\mathrm{Ker}(f)$ は G_1 の部分群である.

(ii) $\mathrm{Im}(f)$ は G_2 の部分群である.

証明

(i) $f(e_1) = e_2$ (e_i : G_i の単位元) より $e_1 \in \mathrm{Ker}(f)$ が成り立つ.

$x, y \in \mathrm{Ker}(f)$ とすると, $f(x \cdot y^{-1}) = f(x) f(y^{-1}) = \underbrace{f(x)}_{e_2} \underbrace{f(y)^{-1}}_{e_2} = e_2$ である.

よって $x \cdot y^{-1} \in \mathrm{Ker}(f)$ となる. 補題 3.3.2 より, $\mathrm{Ker}(f)$ は G_1 の部分群である.

(ii) $f(e_1) = e_2$ より $e_2 \in \mathrm{Im}(f)$ である. また, $x, y \in \mathrm{Im}(f)$ とすると $f(a) = x$, $f(b) = y$ となる $a, b \in G_1$ が存在する. よって

$$x y^{-1} = f(a) f(b)^{-1} = f(a) f(b^{-1}) = f(a b^{-1}) \in \mathrm{Im}(f).$$

したがって, $\mathrm{Im}(f)$ は G_2 の部分群である. □

注意 5.2.3 $f : G_1 \longrightarrow G_2$ を群準同型とする.

- $H_1 \subset G_1$ が部分群ならば, $f(H_1) \subset G_2$ は G_2 の部分群である.
- $H_2 \subset G_2$ が部分群ならば, $f^{-1}(H_2) = \{ g \in G_1 \mid f(g) \in H_2 \}$ は G_1 の部分群である ($H_2 = \{e_2\}$ とした場合に $f^{-1}(\{e_2\}) = \mathrm{Ker}(f)$).

§5.3 正規部分群

定義 5.3.1 Gを群とし，$H \subset G$を部分群とする．Hが**正規部分群**であるとは，任意の$g \in G$, $h \in H$に対して

$$ghg^{-1} \in H$$

が成り立つことをいう．

注意 5.3.2

- HがGの正規部分群であるとき$H \lhd G$で表す．
- $\{e\}$とGは常にGの正規部分群である．
- Gをアーベル群とする．Gの全ての部分群が正規部分群である
  $(\because\ ghg^{-1} = gg^{-1}h = e \cdot h = h \in H)$

補題 5.3.3 $H \subset G$を部分群とする．以下の条件は互いに同値である．

(i) $H \lhd G$

(ii) 任意の$g \in G$に対して$gH = Hg$である．

証明

(i)$\Rightarrow$(ii) $H \lhd G$とし，$g \in G$, $h \in H$とする．このとき$ghg^{-1} = h'$となる$h' \in H$が存在するので$gh = h'g \in Hg$である．ゆえに$gH \subset Hg$が成り立つ．

同様に$g^{-1}hg = h''$となる$h'' \in H$が存在する．よって$hg = gh'' \in gH$

である．ゆえに $Hg \subset gH$ となる．以上より $gH = Hg$ が成り立つ．

(ii) $\Rightarrow$ (i) 任意の $g \in G$ に対して $gH = Hg$ とする．$g \in G, h \in H$ のとき，

$gh \in gH = Hg$ より $gh = h'g$ となる $h' \in H$ が存在する．よって

$ghg^{-1} = h' \in H$ となる． □

命題 5.3.4 $f : G_1 \longrightarrow G_2$ を群準同型とする．このとき，

$\mathrm{Ker}(f) \lhd G_1$ である．

証明 $g \in G_1$，$x \in \mathrm{Ker}(f)$ とする．このとき，

$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)\underbrace{f(x)}_{=e_2}f(g)^{-1}$ である．

よって $f(gxg^{-1}) = f(g)f(g)^{-1} = e_2$ であり，ゆえに $gxg^{-1} \in \mathrm{Ker}(f)$

が成り立つ． □

G を群とし，$H \lhd G$ とする．このとき，集合 G/H に演算を入れる．

$g, g' \in G$ に対して

$$gH \cdot g'H \overset{\text{def}}{=} gg'H \qquad (*)$$

と定める．

定理 5.3.5.

(i) 上記の (*) で定まる演算は well-defined である．

(ii) この演算に関して G/H は群をなす．

(iii) 写像 $\pi : G \longrightarrow G/H$，$g \longmapsto gH$ は群準同型であり，$\mathrm{Ker}(\pi) = H$ が成り立つ．

π は**自然な射影**とよばれる．

証明

(i) $g_1, g_1', g_2, g_2' \in G$ とし，$g_1H = g_2H$ かつ $g_1'H = g_2'H$ とする．

このとき，$g_1g_1'H = g_2g_2'H$ を示せば良い．

$$g_1g_1'H = g_1(g_1'H) = g_1(g_2'H) \overset{(=)}{\uparrow} g_1(Hg_2') = (g_1H)g_2' = g_2(Hg_2') \overset{(=)}{\uparrow} g_2(g_2'H) = g_2g_2'H$$

正規性　　正規性

(ii) 明かに，この演算が結合的であり，$eH = H$ が単位元である．

また，$g \in G$ のとき $(gH)\cdot(g^{-1}H) = gg^{-1}H = H$ である．同様に

$(g^{-1}H)\cdot(gH) = H$ である．ゆえに G/H の全ての元が可逆元である．

以上より G/H は群をなす．

(iii) $g, g' \in G$ に対して

$$\pi(gg') = gg'H = (gH)\cdot(g'H) = \pi(g)\cdot\pi(g')$$ である．

また，$g \in \mathrm{Ker}(\pi) \Leftrightarrow gH = H \Leftrightarrow g \in H$ が成り立つ．　□

§5.4 準同型定理

定義 5.4.1 $f: G_1 \longrightarrow G_2$ を群準同型とする. f が全単射であるときに f が**群同型**であるという.

命題 5.4.2 $f: G_1 \longrightarrow G_2$ が群同型であるならば, 逆写像 $f^{-1}: G_2 \longrightarrow G_1$ も群同型である.

証明 f^{-1} は全単射であるので, f^{-1} が群準同型であることを示せば十分である. $x, y \in G_2$ とする.

$$f(f^{-1}(xy)) = xy = f(f^{-1}(x))\,f(f^{-1}(y)) = f\left(f^{-1}(x)\,f^{-1}(y)\right)$$ である.

f が単射であるので $f^{-1}(xy) = f^{-1}(x)\,f^{-1}(y)$ が成り立つ. □

群同型 $G_1 \longrightarrow G_2$ が存在するときに, $G_1 \simeq G_2$ で表す.

例 5.4.3 n, m を自然数とし, $\gcd(n,m) = 1$ とする. 命題 2.6.3 より

$$f: \mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$
$$k + nm\mathbb{Z} \longmapsto (k + n\mathbb{Z},\ k + m\mathbb{Z})$$

は全単射である. f は群準同型であるので, 群同型である.

命題 5.4.4 $f: G_1 \longrightarrow G_2$ を群準同型とする. このとき

f が単射である $\iff$ $\mathrm{Ker}(f) = \{e_1\}$

(e_1 は G_1 の単位元)

証明

($\Rightarrow$) $x \in \mathrm{Ker}(f)$ とする. $f(x) = e_2 = f(e_1)$ である. f が単射であるので $x = e_1$ となる. よって $\mathrm{Ker}(f) = \{e_1\}$ である.

($\Leftarrow$) $f(x) = f(y)$ $(x, y \in G_1)$ とする. このとき,

$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = f(x)f(x)^{-1} = e_2$ より

$xy^{-1} \in \mathrm{Ker}(f)$ が言える. ゆえに $xy^{-1} = e_1$ であり, $x = y$ となる.

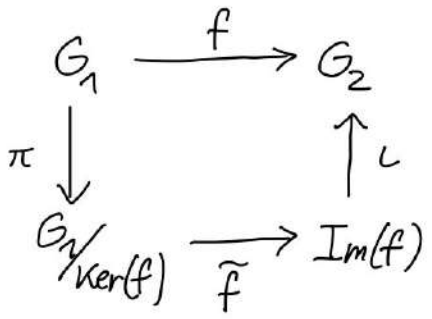
したがって f は単射である. □

定理 5.4.5 (準同型定理) $f : G_1 \longrightarrow G_2$ を群準同型とする.

(i) 以下の写像は well-defined であり, 群同型である.

$$\tilde{f} : G_1/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$$
$$g\,\mathrm{Ker}(f) \longmapsto f(g)$$

(ii) f が次のように分解できる: $f = \iota \circ \tilde{f} \circ \pi$ である.



ただし,

- $\iota : \mathrm{Im}(f) \longrightarrow G_2$ $(x \longmapsto x)$ は自然な包含写像である
- $\pi : G_1 \longrightarrow G_1/\mathrm{Ker}(f)$ は自然な射影である.

証明

(i) $\tilde{f}$ が well-defined であることを示す.

$gKer(f) = g'Ker(f)$ $(g, g' \in G_n)$ とする. よって $g^{-1}g' \in Ker(f)$ である.

ゆえに $f(g^{-1}g') = e_2$ である. $f(g^{-1}g') = f(g^{-1})f(g') = f(g)^{-1}f(g') = e_2$

より $f(g) = f(g')$ が分かる. よって $\tilde{f}$ は well-defined である.

$\tilde{f}$ は明かに全射であるので, $\tilde{f}$ が単射であることを示せば良い. $g \in G_n$ とする.

$$gKer(f) \in Ker(\tilde{f}) \iff \tilde{f}(gKer(f)) = f(g) = e_2$$
$$\iff g \in Ker(f).$$

よって, $\tilde{f}$ は単射である.

(ii) $g \in G_n$ に対して

$$\iota \circ \tilde{f} \circ \pi(g) = \iota(\tilde{f}(gKer(f))) = \iota(f(g)) = f(g)$$

よって $\iota \circ \tilde{f} \circ \pi = f$ である. □

例 5.4.6

- $det : GL_n(\mathbb{C}) \longrightarrow \mathbb{C}^\times$ は全射であり, $Ker(det) = SL_n(\mathbb{C})$ である.
  よって $SL_n(\mathbb{C}) \lhd GL_n(\mathbb{C})$ であり, 群同型 $GL_n(\mathbb{C})/SL_n(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}^\times$ が存在する.

- $sgn : G_n \longrightarrow \{\pm 1\}$ については $Im(sgn) = \{\pm 1\}$, $Ker(f) = A_n$ である
  よって $A_n \lhd G_n$ であり, 群同型 $G_n/A_n \xrightarrow{\sim} \{\pm 1\}$ が存在する. ← 偶置換の集合

§5.5 巡回群

G を群とし, $g \in G$ とする. 次の写像を考える:

$$f : \mathbb{Z} \longrightarrow G, \quad k \longmapsto g^k$$

明かに f は準同型である. また, $Im(f) = \{g^k \mid k \in \mathbb{Z}\} = \langle g \rangle$ である.

命題 5.5.1

(i) g の位数が有限ならば $\mathrm{Ker}(f) = n\mathbb{Z}$ $(n = \mathrm{ord}(g))$ である．このとき $\langle g \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ である．

(ii) g の位数が無限ならば $\mathrm{Ker}(f) = \{0\}$ である．このとき $\langle g \rangle \simeq \mathbb{Z}$ である．

証明：(i) $\mathrm{Ker}(f)$ は $\mathbb{Z}$ の部分群だから，$\mathrm{Ker}(f) = m\mathbb{Z}$ となる $m \geq 0$ が存在．
また，準同型定理より $\mathbb{Z}/m\mathbb{Z} \simeq \langle g \rangle$ である．ゆえに $m = n$ となる．

(ii) g の位数は無限だから $\mathrm{Ker}(f) = \{k \in \mathbb{Z} \mid g^k = e\} = \{0\}$．

よって f は単射である．したがって $\langle g \rangle \simeq \mathbb{Z}$ である． □

系 5.5.2 g の位数が有限とし，$\mathrm{ord}(g) = n$ とおく．このとき，$m \in \mathbb{Z}$ に対して $g^m = e \iff n \mid m$ である．

証明：$g^m = e \iff m \in \mathrm{Ker}(f) \iff m \in n\mathbb{Z} \iff n \mid m$． □

命題 5.5.3 p を素数とし，G を位数 p の群とする．このとき，G は巡回群である．

証明：$g \in G$，$g \neq e$ とする．ラグランジュの定理より $\mathrm{ord}(g) \mid p$．
よって $\mathrm{ord}(g) = p$ となり，$\langle g \rangle = G$ となる．

定理 5.5.4 p を素数とする．このとき，$(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群である．

証明を説明する前に以下の補題をのべる．

補題 5.5.5 G を有限なアーベル群とし，$n = |G|$ とおく．n の任意の約数 $d \geq 1$ に対して $|\{x \in G \mid x^d = e\}| \leq d$ を仮定する．このとき，G は巡回群である．

証明：$X_d = \{x \in G \mid \mathrm{ord}(x) = d\}$ と定義する．$X_d \neq \emptyset$ とすると，位数 d の元 $z \in G$ が存在する．全ての $k \in \mathbb{Z}$ に対して，$(z^k)^d = z^{kd} = (z^d)^k = e$ である．よって，$\langle z \rangle$ は集合 $\{x \in G \mid x^d = e\}$ に含まれる．仮定より，$\langle z \rangle = \{x \in G \mid x^d = e\}$ となる．ゆえに $X_d \subset \langle z \rangle$ である．また，X_d は $\langle z \rangle$ の生成元全体の集合と一致する．$\langle z \rangle \simeq \mathbb{Z}/d\mathbb{Z}$ より $|X_d| = \varphi(d)$ となる．

したがって，n の約数 d に対して $|X_d| = 0$ または $|X_d| = \varphi(d)$ である．

$G = \bigsqcup_{d \mid n} X_d$ より $n = \sum_{d \mid n} |X_d|$ である．

期末レポート問6 (6) より $n = \sum_{d \mid n} \varphi(d)$ が成り立つ．

よって，全ての $d \mid n$ に対して $|X_d| = \varphi(d)$ である．とくに $X_n \neq \emptyset$ となる．

$g \in X_n$ とすると $|\langle g \rangle| = n$ より $\langle g \rangle = G$ となる． □

定理 5.5.4 の証明：

$(\mathbb{Z}/p\mathbb{Z}, +, \times)$ は可換体である．よって，任意の $m \geq 1$ に対して多項式 $X^m - 1$ は $\mathbb{Z}/p\mathbb{Z}$ において高々 m 根をもつ．よって，$|\{x \in (\mathbb{Z}/p\mathbb{Z})^\times \mid x^d = 1\}| \leq d$ が成り立つ．補題 5.5.5 より，$(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群である．