1.4 剰余類の積

整数全体 $\mathbb{Z}$ は和に関して群になるが，積に関しては群にならない。整数の範囲で考えると，積に関しては，1 以外の整数は逆元を持たないからである。しかし，合同類で考えると，積という演算に関しても，群になる場合がある。

定義 1.22 n を自然数とし，$\mathbb{Z}_n$ を剰余群とする。$\mathbb{Z}_n$ 上の積を次のように定義する。

$$[a] \cdot [b] = [ab]$$

剰余群 $\mathbb{Z}_n$ 上の演算は加法 $+$ であったから，このように定義した積は，集合 $\mathbb{Z}_n$ 上の全く新しい演算となるべきものだが，まず最初に，そもそも，これが演算として正しく定義されていることを証明する必要がある。

命題 1.23 この積は $\mathbb{Z}_n$ 上の２項演算になる。

証明: $\mathbb{Z}_n$ 上の演算として定義可能であることを示す。

具体的には，$\mathbb{Z}_n$ の元として $[a] = [a']$, $[b] = [b']$ である時，$\mathbb{Z}_n$ の元として $[ab] = [a'b']$ であることを示せば良い。

$[a] = [a']$, $[b] = [b']$ であるから，$a - a' \in n\mathbb{Z}$, $b - b' \in n\mathbb{Z}$ である。すなわち，ある $k, k' \in \mathbb{Z}$ があって，$a = a' + kn$, $b = b' + k'n$ となっている。

$$ab = (a' + kn)(b' + k'n) = a'b' + ak'n + b'kn + kk'n^2 = a'b' + n(ak' + b'k + kk'n)$$

であるから，$ab - a'b' \in n\mathbb{Z}$ となり，$[ab] = [a'b']$ であることが示された。 ∎

a と a' が $\mathbb{Z}_n$ の同じ同値類に入っていることを

$$a \equiv a' \mod n \quad \text{または} \quad a \equiv a' \pmod n$$

と書いた。上の命題をこの記号を使って書き直すと，

命題 1.24 $a \equiv a' \pmod n$ であり $b \equiv b' \pmod n$ ならば $ab \equiv a'b' \pmod n$ である。

となる。例えば，$a \equiv 1 \pmod n$ ならば，任意の整数 b に対して $ab \equiv b \pmod n$ となる。

積が定義できたので，積の性質について確認しておく。

命題 1.25 $[a], [b], [c] \in \mathbb{Z}_n$ とする。

(1) $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$　　(結合法則)

(2) $[1] \cdot [a] = [a] \cdot [1] = [a]$　　(単位元の存在)

(3) $[a] \cdot [b] = [b] \cdot [a]$　　(交換法則)

(4) $[0]\cdot[a]=[0]$

命題 1.25 を合同の記号を使って書き直すと次のようになる。$a,b,c\in\mathbb{Z}$ とする。

(1) $(a\cdot b)\cdot c\equiv a\cdot(b\cdot c)\pmod n$

(2) $a\cdot 1\equiv 1\cdot a\equiv a\pmod n$

(3) $a\cdot b\equiv b\cdot a\pmod n$

(4) $0\cdot a\equiv 0\pmod n$

もし，全ての元に積に関する逆元があれば，積に関しても群になるのだが，それは成り立たない。

[0] は，他の元との積をとると常に [0] となり，[1] となることはない。すなわち，逆元を持たない。

それでは [0] 以外の元は逆元を持つだろうか？ すなわち，[0] を $\mathbb{Z}_n$ から除いてしまえば群になるだろうか？

これについても，一般には成立しない。[0] を除いてしまえば，積が定義されない場合があるからである。例えば，$n=4$ の場合，

$$\mathbb{Z}_4-\{\,[0]\,\}=\{\,[1],[2],[3]\,\}$$

を考えると，

$$[2]\cdot[2]\equiv[0]\pmod 4$$

であるから，0 がなければ，積が定義されない。しかし，$\mathbb{Z}_n-\{[0]\}$ が積に関して群になる場合もある。

$\mathbb{Z}_7^*=\mathbb{Z}_7-\{\,[0]\,\}=\{\,[1],[2],[3],[4],[5],[6]\,\}$ とする。$[2]^2=[2]\cdot[2]=[4]$，$[2]^3=[4]\cdot[2]=[8]=[1]$ なので $[2]\cdot[4]=[1]$ となり [2] の逆元は [4] である。即ち $[2]^{-1}=[4]$ である。また $[4]^{-1}=[2]$ でもある。

$[3]^2=[9]=[2]$，$[3]^3=[2]\cdot[3]=[6]$，$[3]^4=[6]\cdot[3]=[18]=[4]$，$[3]^5=[4]\cdot[3]=[12]=[5]$，$[3]^6=[5]\cdot[3]=[15]=[1]$ より $[3]\cdot[5]=[1]$ となり $[3]^{-1}=[5]$，$[5]^{-1}=[3]$ となる。

$[6]^2=[36]=[1]$ なので $[6]^{-1}=[6]$ である。よって $\mathbb{Z}_7^*$ に関しては乗法の逆元がすべて存在するので，乗法に関しても群になる。一般に次が成立する。

定理 1.26 p を素数とし，$\mathbb{Z}_p^*=\mathbb{Z}_p-\{[0]\}$ とすると，これは積に関して群になる。

証明　$\mathbb{Z}_p^*$ が積に関して逆元を持つことを言えば良い。

$[q]\in\mathbb{Z}_p^*$ を任意の元とすると，p は素数なので，p と q は互いに素である。定理 1.9 より，ある整数 k_1,k_2 があって，$k_1p+k_2q=1$ となる。

k_2 を p で割ると，ある整数 m と，$0\leqq r\leqq p-1$ となる整数 r があって，$k_2=mp+r$ となっている。ここで $r=0$ ならば，$k_2=mp$ なので，$k_1p+mpq=(k_1+mq)p=1$ となり，1 より大きい整数 p に他の整数をかけて 1 となることはあり得ないので矛盾である。従って，$1\leqq r\leqq p-1$ である。

$(mp+r)q=(-k_1)p+1$ であるから，$rq=(-mq-k_1)p+1$ であり，これは $rq\equiv 1\pmod p$ であることを示している。$r\in\mathbb{Z}_p^*$ とみなすと，これは r が q の逆元であることを示している。∎

$|\mathbb{Z}_p^*|=p-1$ であるから，$\mathbb{Z}_p^*$ の任意の元 a に対し，$\mathbb{Z}_p^*$ 上の積に関して，$a^{p-1}=1$ が成り立つ。

これが，初等整数論において有名な次の定理である。

定理 1.27 [フェルマーの小定理] 素数 p と $(p,a)=1$ となる自然数 a に対して次が成り立つ。

$$a^{p-1} \equiv 1 \pmod{p}$$

証明　p を素数とし，a を $(p,a)=1$ となる自然数とする。このとき $[a] \in \mathbb{Z}_p^*$ である。

定理 1.26 より，$\mathbb{Z}_p^*$ は積に関して群であり，$|\mathbb{Z}_p^*| = p-1$ である。$[a]$ の位数を k とすると $[a]^k = [1]$ であり，定理 1.21 より，k は $p-1$ の約数なのである整数 m を用いて $p-1=km$ と書ける。

$$[a^{p-1}] = [a]^{p-1} = [a]^{km} = \left([a]^k\right)^m = [1]^m = [1]$$

が成立する。これは，

$$a^{p-1} \equiv 1 \pmod{p}$$

を意味する。∎

注意： **(1)** 素数 p に対して，$a \in \mathbb{Z}$ が $(p,a)=1$ すなわち，p と a が互いに素であるということは，a が p の倍数になっていない，ということである。

(2) $a^{p-1} \equiv 1 \pmod{p}$ の両辺に a をかけて，

$$a^p \equiv a \pmod{p}$$

という形で使われることもある。

例： **(1)** $p=5$, $a=4$ とすると $(5,4)=1$ である。

$$4^{5-1} = 4^4 = 256 \equiv 1 \pmod{5}$$

(2) $p=11$, $a=12$ とすると $(11,12)=1$ である。

$$12^{11-1} = 12^{10} = 61917364224 = 5628851293 * 11 + 1 \equiv 1 \pmod{11}$$

(3) 例題：$2^{1,000,000} \pmod{7}$ を求めよ。

解：$(2,7)=1$ であり 7 は素数だから，フェルマーの小定理から $2^6 \equiv 1 \pmod{7}$ である。$1,000,000 = 166666 * 6 + 4$ であるから，

$$\begin{aligned} 2^{1,000,000} &= 2^{166666*6+4} = 2^{166666*6} 2^4 = \left(2^6\right)^{166666} 2^4 \\ &\equiv 2^4 \pmod{7} \equiv 2 \pmod{7} \end{aligned}$$

(4) 例題：$1234^{1,000,000,000} \pmod{997}$ を求めよ。

解：$(1234,997)=1$ であり 997 は素数だから，フェルマーの小定理から $1234^{996} \equiv 1 \pmod{997}$ である。

$1,000,000,000 = 1004016 * 996 + 64$ であるから，

$$\begin{aligned} 1234^{1,000,000,000} &= 1234^{1004016*996+64} = 1234^{1004016*996} 1234^{64} \\ &= \left(1234^{996}\right)^{1004016} 1234^{64} \\ &\equiv 1234^{64} \pmod{997} \end{aligned}$$

となり，$1234^{64} \pmod{997}$ を求める問題に帰着された。あとは，$1234 = 237 \pmod{997}$ なので，

$$1234^{64} \equiv 237^{64} \pmod{997}$$

となる。

$$237^2 = 56169 \equiv 337 \pmod{997}$$

なので，

$$237^{64} = 56169^{32} \equiv 337^{32} \pmod{997}$$

というプロセスにより，$\log_2 64$ の回数で指数を 0 にできる。