# 06 剰余類

ゼロから始める群論 2020

**剰余類の定義**

$G$ を群，$H$ をその部分群，$a \in G$ とする．
$Ha := \{ha | h \in H\}$
を $a$ の $H$ による**右剰余類**という*.

**定理 07**

$G$ を群，$H$ をその部分群とする．
(1) 任意の $a, b \in G$ に対して，
$Ha \cap Hb \neq \varnothing \Rightarrow Ha = Hb$
(2) 任意の $a, b \in G$ に対して，
$|Ha| = |Hb|$
が成り立つ．

(証明) (1) $x \in Ha \cap Hb$ とする．ある $h_1, h_2 \in H$ が存在して，
$x = h_1 a = h_2 b$
となる．中辺と右辺の左から $(h_1)^{-1}$ および $(h_2)^{-1}$ をかけることで
$a = (h_1)^{-1} h_2 b \cdots ①$
$b = (h_2)^{-1} h_1 a \cdots ②$
となる．以下，$Ha = Hb$ を示す．$Ha$ の任意の元 $ha$ $(h \in H)$ をとる．このとき①から
$ha = h(h_1)^{-1} h_2 b \in Hb$ となるから，$Ha \subset Hb$ を得る．同様に②から $Ha \supset Hb$ が示せるので，$Ha = Hb$ となる．
(2) 任意の $a \in G$ で $|H| = |Ha|$ であることを示す．簡単のため，$|H|$ が有限として示す．$H = \{h_1, h_2, \cdots, h_n\}$ とする (もちろん各 $h_i$ はすべて異なる)．$a \in G$ に対して $Ha = \{h_1 a, h_2 a, \cdots, h_n a\}$ となるが，$h_i a = h_j a$ とすれば両辺の右から $a^{-1}$ をかけて $h_i = h_j$ となるので，集合 $Ha$ の元 $h_1 a, h_2 a, \cdots, h_n a$ はすべて異なる．すなわち $|H| = |Ha|$ を得る ($|H|$ が有限であると仮定して説明したが，一般には，写像 $H \to Ha, (x \mapsto xa)$ が全単射であることを示せばよい)．任意の $a \in G$ で言えたのだから，任意の $a, b \in H$ で $|Ha| = |H| = |Hb|$. □

**系**

$G$ を有限群，$H$ をその部分群とする．
(1) $|H|$ は $|G|$ の約数である (ラグランジュの定理)．
(2) $G$ の元 $a$ の位数は $|G|$ の約数である．
(3) $G$ の元 $a$ について $a^{|G|} = e$ である．

(証明)(1) 定理 07 により，$G$ は互いに共通部分がなく，元の個数が等しい右剰余類の和集合
$G = Ha_1 \cup Ha_2 \cup \cdots Ha_m \ (a_1 = e)$
の形に表されるから系が従う．

(2) $a$ の位数は $a^n = e$ となる最小の自然数であるが，これは $a$ から生成される部分群の位数 $|<a>|$ のことでもあった．よってラグランジュの定理により $a$ の位数は $|G|$ の約数である．

(3) $a$ の位数 $|<a>|$ を $n$ とかくことにする．(2) により，ある整数 $q$ が存在して，$|G| = nq$ となっている．よって
$a^{|G|} = a^{nq} = (a^n)^q = e^q = e$. □

(例)(1) $G$ を位数 $p$($p$ は素数) の群とすると，単位元以外の任意の元 $x \in G (x \neq e)$ で $G = <x>$ となる．
実際，$H = <x>$ とすればラグランジュの定理から $|H|$ は $|G| = p$ の約数である．仮定により $|H| \neq 1$ であるから $|H| = p$．$H \subset G$ で元の個数が等しいことから $H = G$ とならざるを得ない． □

(例)(2) $p$ を素数とする．以下の集合は演習 06-2 で示すように，群となる．
$(\mathbb{Z}/p\mathbb{Z})^\times := \{\overline{1}, \overline{2}, \cdots \overline{p-1}\}$
ただし，$\overline{i}$ と $\overline{j}$ の演算は
$\overline{i} \times \overline{j} = \overline{(i \times j \text{ を } p \text{ でわったときのあまり})}$
として定義する．この群について系 (3) の事実を適用すると，任意の $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ に対して，
$(\overline{x})^{p-1} = \overline{1}$
となる．合同式*の記法で表現すると以下の通

*他の剰余類も同様に定義される．$aH := \{ah | h \in H\}$ (左剰余類)，$aHb := \{ahb | h \in H\}$.

*$a \equiv b \pmod p$ は $a - b$ が $p$ で割り切れることを意味する．これは「$a$ を $p$ で割った余りと $b$ を $p$ で割った

りになる．

$p$ で割り切れない任意の整数 $x$ について
$$x^{p-1} \equiv 1 \pmod{p}$$
である．
これは**フェルマーの小定理**とよばれる． □

〜演習問題〜
06-1 $G$ を有限群，$H, H'$ をその部分群とする．$|H|, |H'|$ が互いに素†ならば $H \cap H' = \{e\}$ であることを示せ．

06-2 任意の $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ に対して，2つの集合
$$\{\overline{1} \times \overline{a},\ \overline{2} \times \overline{a},\ \overline{3} \times \overline{a},\ \cdots, (\overline{p-1}) \times \overline{a}\},$$
$$\{\overline{1},\ \overline{2},\ \overline{3},\ \cdots, \overline{p-1}\}$$
が集合として等しいことを示し，このことから $\overline{a}$ の逆元が $(\mathbb{Z}/p\mathbb{Z})^\times$ に存在することを導け．

((例)(2) の補足) もっと一般に
$(\mathbb{Z}/n\mathbb{Z})^\times := \{\overline{m} | 1 \leqq m < n, m \text{ と } n \text{ は互いに素 }\}$
も群である．ここで $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$(**オイラー関数**，これは $n$ と互いに素な自然数の個数を表す) とかくことにすれば，系 (3) より，任意の $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対して，
$$\overline{x}^{\varphi(n)} = \overline{1}$$
となる．合同式の記法で表現すると以下の通りになる．

$n$ と互いに素な任意の整数 $x$ について
$$x^{\varphi(n)} \equiv 1 \pmod{n}$$
である．
これは**オイラーの定理**とよばれる．$n = p$ とした場合がフェルマーの小定理に相当する． □

---

あまりが等しい」とも言い換えられる．
†「整数 $a, b$ が互いに素」とは「$a$ と $b$ の最大公約数が 1」のことを意味する
(06-1)$H \cap H'$ は $H$ の部分群，かつ $H'$ の部分群となるからラグランジュの定理により，$|H \cap H'|$ は $|H|$ と $|H'|$ の公約数．よって仮定により $|H \cap H'| = 1$ となり $H \cap H' = e$ を得る． (06-2) $\overline{1} \times \overline{a},\ \overline{2} \times \overline{a},\ \overline{3} \times \overline{a},\ \cdots, (\overline{p-1}) \times \overline{a}$ はすべて異なる元であることを示す．実際，$\overline{i} \times \overline{a} = \overline{j} \times \overline{a}$ とすれば $ia - ja = (i-j)a$ は $p$ で割り切れる．$a$ は $p$ で割り切れないから，$i-j$ が $p$ で割り切れる．$-p < i-j < p$ であるから $i - j = 0$，すなわち $\overline{i} = \overline{j}$．集合として等しいことから，ある $\overline{a'} \in (\mathbb{Z}/p\mathbb{Z})^\times$ が存在して $\overline{a'} \times \overline{a} = \overline{1}$ を得る．