剰余類
Coset

剰余類は整数を類別するときに使われるが，さらに一般化してみよう．

定理 1 H を群 G の部分群とする．$a, b \in G$ について，$ab^{-1} \in H$ であることを

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

と定義すと，この関係 $\equiv$ は同値関係である．

［証明］$aa^{-1} = e \in H$ より

$$a \equiv a \pmod{H}$$

$a \equiv b \pmod{H}$ のとき $ab^{-1} \in H$．H はそれ自身で群構造をもっているので，

$$(ab^{-1})^{-1} \in H$$

$$\therefore ba^{-1} \in H$$

$$\therefore b \equiv a \pmod{H}$$

$a \equiv b, b \equiv c \pmod{H}$ のとき，

$$ab^{-1} \in H, bc^{-1} \in H$$

H は演算に対して閉じているので

$$ab^{-1}bc^{-1} \in H$$

$$\therefore ac^{-1} \in H$$

$$a \equiv c \pmod{H}$$

反射律，対称律，推移律が成り立っているので $\equiv$ は同値関係である．［証明おわり］

$\equiv$ の代わりに $\sim$ を用いている書物もある．この関係を右合同と呼び，後述の左合同と区別するが，記号でかくと同じである．

定理 2 H を群 G の部分群であるとき

$$a \equiv b \pmod{H} \iff a \in Hb \quad ^{*1}$$

［証明］$a \equiv b \pmod{H} \iff ab^{-1} \in H \iff ab^{-1}b \in Hb \iff a \in Hb$ ［証明おわり］

定理 3 H を群 G の部分群とするとき $a, b \in G$ ならば $Ha \cap Hb = \phi$ または $Ha = Hb$ が成り立つ．

［証明］まず $Ha \cap Hb \neq \phi \Longrightarrow Ha \subset Hb$ を証明する．
$g \in Ha \cap Hb$ とすると，$g \in Ha$ かつ $g \in Hb$．よって，

$$g \equiv a \equiv b \pmod{H}$$

---

*1 $H = \{h_1, h_2, h_3, \cdots, h_n\}$ のとき $Ha \overset{\text{def.}}{=} \{h_1 a, h_2 a, h_3 a, \cdots, h_n a\}$

$$\therefore a \in Hb$$

$$\therefore a = hb \ (\exists h \in H) \tag{1}$$

$\forall x \in Ha$ について

$$x = h'a \ (\exists h' \in H)$$

が言えるので，(1) を用いて，

$$x = h'hb$$

$h'h \in H$ だから

$$x \in Hb$$

つまり Ha の全ての元が Hb に含まれる．よって $Ha \subset Hb$ が証明された．

同様にこれまでの証明の a と b を入れ替えることにより，

$$Ha \cap Hb \neq \phi \Longrightarrow Hb \subset Ha$$

も証明でき，双方をあわせると，

$$Ha \cap Hb \neq \phi \Longrightarrow Hb = Ha$$

が言える．よって，$a, b \in G$ ならば $Ha \cap Hb = \phi$ または $Ha = Hb$ が成り立つ． ［証明おわり］

以上のことから次のことが言える．

定理 4 群 G を

$$a \equiv b \ (\mathrm{mod} H) \Longrightarrow ab^{-1} \in H$$

という関係で類別すると，

$$\{H, Ha, Hb, \cdots\}$$

という類に類別される．

この類別を G の H による**右剰余類 (right coset)** といい，H/G で表す．

定理 5 群 G を

$$a \equiv b \ (\mathrm{mod} H) \Longrightarrow a^{-1}b \in H$$

という関係で類別すると，

$$\{H, Ha, Hb, \cdots\}$$

という類に類別される．

この類別を G の H による**左剰余類 (left coset)** といい，G/H で表す．アーベル群の場合は右剰余類と左剰余類は同じものである．また整数の類別で用いられる剰余類という言葉をそのまま流用しているが，一般には割ったときの余りという意味ではない．またここまで，演算記号は省略したが，整数の剰余類の場合は演算は $+$ である．

このような剰余類（左剰余類，右剰余類）の元の個数を，群 G の部分群 H に対する**指数**といい，$[G : S] = m$ と表す．

これまでのことから有限群に関して次の定理がいえる．

定理 6 （Lagrange の定理） 位数 n の有限群 G において，G の任意の部分群 H の位数 m は G の位数の約数である．

有限群の位数を $|\ |$ という記号で表すと，$|S|$ は $|G|$ の約数であるということである．

またこのことから次の系が導かれる．

系 G が有限群であるとき，$|G| = n$ とすると，$\forall x \in G$ に対して

$$x^n = e$$

例 1 $G = \{1, -1, i, -i\}, H = \{1, -1\}$ のとき G の H による右剰余類は $\{H, Hi\}$ の 2 つである．左剰余類は $\{H, iH\}$ の 2 つで，演算は可換であるため，両剰余類は等しい．

例 2 対称群 $S_3 = \{\iota, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ を部分群 $H = \{\iota, (1\ 2)\}$ で類別すると，右剰余類は

$$\{H, H(1\ 3), H(2\ 3)\} = \{H, \{(1\ 3), (1\ 3\ 2)\}, \{(2\ 3), (1\ 2\ 3)\}\}$$

の 3 つである．左剰余類は

$$\{H, (1\ 3)H, (2\ 3)H\} = \{H, \{(1\ 3), (1\ 2\ 3)\}, \{(2\ 3), (1\ 3\ 2)\}\}$$

である．

参考文献

[1] 石村園子『すぐわかる代数』（東京図書，2003 年）
[2] 長岡亮平『線形代数学』（放送大学教育振興会，2004 年）
[3] 「物理のかぎしっぽ」<http://hooktail.sub.jp/>