4 部分群, 剰余類

• 4-1 : 部分群

群は, 単に集合というだけでなく演算という数学的な構造が入っている. そこで, 群の部分集合についても, 演算を込めて「部分構造」となっているものを考えることは自然である.

定義 4.1. 群 G の部分集合 H が G の **部分群** であるとは, G の積に関して H が群となっているときをいう. H が G の部分群であることを $H \leq G$ で表す.

つまり, 群 G に対して, $H \subset G$ が G の部分群とは, G の演算が H で閉じている, すなわち, 任意の $x, y \in H$ に対して $x * y \in H$ であって以下の 3 条件をみたすときをいう.

(G1) (結合法則) 任意の $x, y, z \in H$ に対して, $(x * y) * z = x * (y * z)$ を満たす.
(G2) (単位元の存在) ある $e_H \in H$ が存在して, 任意の $x \in H$ に対して $x * e_H = x = e_H * x$ が成り立つ.
(G3) (逆元の存在) 任意の $x \in G$ に対して, ある $y \in H$ が存在して $x * y = e_H = y * x$ が成り立つ.

例 4-1 (1) 集合として, $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ であるが, 通常の和に関して, この包含は部分群の対応にもなっている. 例えば, $\mathbb{Z}$ は $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ の部分群である.

(2) k を $\mathbb{R}$ または $\mathbb{C}$ とする. 行列の和に関して, $\mathsf{sl}_n(\mathsf{k}) := \{X \in \mathsf{Mat}_n(\mathsf{k}) \mid \mathsf{tr}(X) = 0\}$ は $\mathsf{Mat}_n(\mathsf{k})$ の部分群である. ここで, $X = (x_{ij})_{1 \leq i,j, \leq n}$ に対して, $\mathsf{tr}(X) = \sum_{k=1}^{n} x_{ii}$ であり, これは行列 X の **トレース** と呼ばれる. まず, 行列の和の演算が閉じていることを確認しておこう. 任意に $X, Y \in \mathsf{sl}_n(\mathsf{k})$ をとれば,

$$\mathsf{tr}(X + Y) = \mathsf{tr}(X) + \mathsf{tr}(Y) = 0 + 0 = 0$$

なので $X + Y \in \mathsf{sl}_n(\mathsf{k})$ である.

(G1) $\mathsf{Mat}_n(\mathsf{k})$ 上の演算 $+$ が結合法則を満たすので , その部分集合である $\mathsf{sl}_n(\mathsf{k})$ も結合法則を満たす.

(G2) 零行列 O をとれば, $\mathsf{tr}(O) = 0$ なので, $O \in \mathsf{sl}_n(\mathsf{k})$ である. このとき. 零行列 O は $\mathsf{Mat}_n(\mathsf{k})$ の和に関する単位元であったので, これは $\mathsf{sl}_n(\mathsf{k})$ の単位元にもなる.

(G3) 任意の $X \in \mathsf{sl}_n(\mathsf{k})$ をとると, $-X$ を考えれば,

$$\mathsf{tr}(-X) = -\mathsf{tr}(X) = 0$$

だから $-X \in \mathsf{sl}_n(\mathsf{k})$ である. これは X の逆元となる.

(3) 行列の積に関して, $\mathsf{SL}_n(\mathbb{C}) := \{X \in \mathsf{GL}_n(\mathbb{C}) \mid \det(X) = 1\}$ は $\mathsf{GL}_n(\mathbb{C})$ の部分群である. これを $\mathbb{C}$ 上の **特殊線形群** と呼ぶ. また, $\mathsf{U}_n(\mathbb{C}) := \{X \in \mathsf{GL}_n(\mathbb{C}) \mid X^* X = E_n\}$ とおくと, これも $\mathsf{GL}_n(\mathbb{C})$ の部分群である. ここで, X^* は X の随伴行列を表す. これを $\mathbb{C}$ 上の **ユニタリ群** と呼ぶ.

(4) 全ての群 G は, 単位元のみからなる部分群 $\{e\}$ と G 自身を部分群としてもつ. これらを **自明な部分群** と呼ぶ.

レポート 4-1 $\mathsf{SL}_n(\mathbb{C})$ と $\mathsf{U}_n(\mathbb{C})$ が $\mathsf{GL}_n(\mathbb{C})$ の部分群であることを示せ.

• 4-2 : 生成された部分群

G を群, $S \subset G$ をとる. S 上の **語** とは, ある $x_1, \ldots, x_n \in S$ で

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}, \quad \varepsilon_k \in \{1, -1\} \quad (k = 1, 2, \ldots, n)$$

と表される G の元をいう. ただし, $n = 0$ のときの語は G の単位元 e を表すとする. S 上の語全体の集合を $\langle S \rangle$ で表す. $S = \{g_1, \ldots, g_n\}$ であるとき, $\langle S \rangle$ の代わりに $\langle g_1, \ldots, g_n \rangle$ とかく.

群 G の元 $a \in G$ と正の整数 n をとる．このとき，

$$a^0 = e, \quad a^n = \overbrace{aa\cdots a}^{n}, \quad a^{-n} = \overbrace{a^{-1}a^{-1}\cdots a^{-1}}^{n}$$

と定義する．（結合法則はこの定義に意味を持たせるためにある．）

命題 4.2. G を群, $S \subset G$ をとる．このとき, 次の 2 つが成り立つ．

(1) $\langle S\rangle$ は G の部分群である．
(2) $S \subset H \leq G$ であるとき, $\langle S\rangle \subset H$ である．

証明. (1) S 上の 2 つの語 $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n}$, $y_1^{\varepsilon_1'}y_2^{\varepsilon_2'}\cdots y_m^{\varepsilon_m'} \in \langle S\rangle$ をとれば,

$$(x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n})(y_1^{\varepsilon_1'}y_2^{\varepsilon_2'}\cdots y_m^{\varepsilon_m'}) = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n}y_1^{\varepsilon_1'}y_2^{\varepsilon_2'}\cdots y_m^{\varepsilon_m'} \in \langle S\rangle$$

となる．従って, G の積は $\langle S\rangle$ で閉じている．

(G1) G は群なので, G の積は結合法則をみたす．$\langle S\rangle$ の積は G の積と同じなので同様に結合法則を満たす．

(G2) $n = 0$ のときの語は単位元 e も S 上の語だから $\langle S\rangle$ は単位元をもつ．

(G3) 任意に $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n} \in \langle S\rangle$ をとれば, $x_n^{-\varepsilon_n}x_{n-1}^{-\varepsilon_{n-1}}\cdots x_1^{-\varepsilon_1} \in \langle S\rangle$ であり,

$$(x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n})(x_n^{-\varepsilon_n}x_{n-1}^{-\varepsilon_{n-1}}\cdots x_1^{-\varepsilon_1}) = e = (x_n^{-\varepsilon_n}x_{n-1}^{-\varepsilon_{n-1}}\cdots x_1^{-\varepsilon_1})(x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n})$$

である．従って, $x_n^{-\varepsilon_n}x_{n-1}^{-\varepsilon_{n-1}}\cdots x_1^{-\varepsilon_1}$ が $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n}$ の逆元である．

以上で $\langle S\rangle$ は G の部分群である．

(2) H を S を部分集合として含んでいるような G の部分群であるとする．任意に $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n} \in \langle S\rangle$ をとる．$n = 0$ とすれば, 対応する語は $e \in G$ である．$H \leq G$ なので, $e \in H$ である．次に $n \geq 1$ とする．$S \subset H$ なので, $x_1, \ldots, x_n \in H$ である．H は群なので $x_1^{\varepsilon_1}, \ldots, x_n^{\varepsilon_n} \in H$ である．H は積で閉じているので, $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n} \in H$ となる．以上で $\langle S\rangle \subset H$ である．□

定義 4.3. **命題 4.2** によって, $\langle S\rangle$ は群である．この $\langle S\rangle$ を **S によって生成された部分群** と呼ばれる．1 つの元で生成される群 $\langle g\rangle$ を **巡回群** と呼ぶ．

G 自身が巡回群なら, ある $x \in G$ で $G = \{x^n \mid n \in \mathbb{Z}\}$ である．このとき, $i, j \in \mathbb{Z}$ なら

$$x^i x^j = x^{i+j} = x^j x^i$$

だから, 巡回群の積は交換可能である．このように, 積が可換である, すなわち群 G が任意の $x, y \in G$ が $xy = yx$ を満たすとき G は **アーベル群** と呼ばれる．

例 4-2　$\mathbb{Z}$ は和に関して群であるが, これは 1 で生成される．すなわち $\mathbb{Z} = \langle 1\rangle$ である．これは次のようにして確かめられる．まず, $1 \in \mathbb{Z}$ なので, $\langle 1\rangle \subset \mathbb{Z}$ は明らかである．（明らかであるのはなぜかを説明できるようにしておくこと．）逆に, 任意に $m \in \mathbb{Z}$ をとる．$m = 0$ ならば, これは単位元であるから $0 \in \langle 1\rangle$ である．$m \neq 0$ であれば,

$$m = \begin{cases} \overbrace{1 + 1 + \cdots + 1}^{m} & (m > 0 \text{ のとき}), \\ \overbrace{(-1) + (-1) + \cdots + (-1)}^{m} & (m < 0 \text{ のとき}) \end{cases}$$

である．いずれにしても $m \in \langle 1\rangle$ であるから $\mathbb{Z} \subset \langle 1\rangle$ がわかった．以上で $\mathbb{Z} = \langle 1\rangle$ である．

また, $m \in \mathbb{Z}$ に対して, $m\mathbb{Z} := \langle m\rangle$ とおく．$\mathbb{Z}$ の部分群 $m\mathbb{Z}$ は整数 m によって生成されているから, その元は m の倍数となる．つまり,

$$m\mathbb{Z} = \{\ldots, -2m, -m, 0, m, 2m, 3m, \ldots\}$$

- **4-3： 剰余類**

命題 4.4. 群 G の部分群 H をとる.

(1) $x, y \in G$ に対して, G 上の関係 $\sim$ を, $x \sim y$ を $x^{-1}y \in H$ で定義する. これは, G 上の同値関係を定める.
(2) $x, y \in G$ に対して, G 上の関係 $\sim$ を, $x \sim y$ を $yx^{-1} \in H$ で定義する. これは, G 上の同値関係を定める.

証明. (1) のみ示す. (2) も同様.

(反射律) 任意に $x \in G$ をとると, $x^{-1}x = e \in H$ だから $x \sim x$ である.

(対称律) 任意に $x, y \in G$ で $x \sim y$ であるものをとると, $x^{-1}y \in H$ である. このとき, H は群なので $(x^{-1}y)^{-1} = y^{-1}x \in H$ である. 従って $y \sim x$ である.

(推移律) 任意に $x, y, z \in G$ で $x \sim y$, $y \sim z$ であるものをとると, $x^{-1}y, y^{-1}z \in H$ である. このとき, H は群なので $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$ である. 従って $x \sim z$ である. □

定義 4.5. H を群 G の部分群であるとする.

(1) $x, y \in G$ に対して, G 上の同値関係 $\sim$ を $x^{-1}y \in H$ と定める. このとき, $x \in G$ の同値類を xH と表し, x の H による **左剰余類** と呼ぶ. このとき, 商集合を G/H とかく.
(2) $x, y \in G$ に対して, G 上の同値関係 $\sim$ を $yx^{-1} \in H$ と定める. このとき, $x \in G$ の同値類を Hx と表し, x の H による **右剰余類** と呼ぶ. このとき, 商集合を $H\backslash G$ とかく.

命題 4.6. H を G の部分群であるとする. このとき, 次の 2 つが成り立つ.

(1) $|G/H| = |H\backslash G|$ である.
(2) 任意の $g \in G$ に対して, $|gH| = |Hg| = |H|$ である.

証明. (1) 2 つの集合の個数（本来は濃度と呼ばれる）が等しいことを示すには, その集合の間に全単射な写像が存在すれば良い. 写像 $f : G/H \to H\backslash G$ を $f(gH) = Hg^{-1}$ と定義する. これは well-defined である. 実際, $gH = g'H$ であるときに $Hg^{-1} = Hg'^{-1}$ となればよいのでこれを示す. 仮定より, $g'^{-1}g \in H$ であるが, $g'^{-1}g = g'^{-1}(g^{-1})^{-1} \in H$ であり, これは $Hg^{-1} = Hg'^{-1}$ を意味する. 従って写像 f は well-defined であることがわかった. このように定めた写像 f が全単射であることを示そう.

（単射性） $f(gH) = f(g'H)$ であると仮定すると, $Hg^{-1} = Hg'^{-1}$ だから $g'^{-1}(g^{-1})^{-1} = g'^{-1}g \in H$ である. H による左剰余類の定義より $gH = g'H$ となるから f は単射である.

（全射性） 任意に $Hg \in H\backslash G$ をとれば $Hg = H(g^{-1})^{-1}$ なので $f(g^{-1}H) = H(g^{-1})^{-1} = Hg$ となるため, f は全射である.

以上で f は全単射であることが示されたので $|G/H| = |H\backslash G|$ となる.

(2) 写像 $f : H \to gH$ を $f(h) = gh$ で定義する. これが全単射であることを示せば, $|H| = |gH|$ であることがわかる.

（単射性） まず $f(h) = f(h')$, すなわち $gh = gh'$ であるとする. G は群であるから, g の逆元 $g^{-1} \in G$ が存在する. $gh = gh'$ の左から g^{-1} をかけると $h = h'$ を得る. よって f は単射である.

（全射性） 任意に $gh \in gH$ をとれば, $h \in H$ をとれば $f(h) = gh$.　よって f は全射である.

以上で f は全単射であることが示されたので $|H| = |gH|$ となる. 同様に $|H| = |Hg|$ である. □

定義 4.7. G を群として, $H \leq G$ であるとする. このとき, G/H の元の個数を $(G : H)$ で表し, H の G における **指数** という.

定理 4.8 (Lagrange の定理)**.** H を G の部分群であるとする. このとき, $|G| = (G : H)|H|$ が成り立つ.

証明. 群 G の H による左剰余類について, $G/H = \{g_1H, g_2H, \ldots, g_mH\}$ であるとする. このとき,

$$G = g_1H \cup g_2H \cup g_3H \cup \cdots \cup g_mH, \quad g_iH \cap g_jH = \varnothing \quad (i \neq j)$$

である. このとき, **命題 4.6** より

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

である. これが示すべき等式であるから証明が完了した. □

レポート 4-2　$G = S_3$ で $H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle$ とおく. このとき, 巡回群 H の位数を求めよ. また, $(G : H)$ を求めよ.

- **4-4 : 正規部分群**

群 G とその部分群 H に対して, 左剰余類 G/H や右剰余類 $H\backslash G$ は商集合であった. 例えば, $G = \mathbb{Z}$ の部分群 $m\mathbb{Z}$ $(m > 1)$ をとり, その左剰余類 $\mathbb{Z}/m\mathbb{Z}$ を考えることができるが, これは**命題 3.1** によって再び群となっていた. しかし, 左剰余類や右剰余類は群になるとは限らない.

では, いつ左剰余類や右剰余類は群になるのかを考えよう.

定義 4.9. 群 G の部分群 H が以下の条件を満たすとき, H を G の **正規部分群** と呼ぶ.

(NS) 任意の $g \in G$ と任意の $h \in H$ に対して, $ghg^{-1} \in H$ を満たす.

H が G の正規部分群であるとき, $H \triangleleft G$ とかく.

命題 4.10. $H \triangleleft G$ に対して, G/H は次の積で群となる. 任意の $gH, g'H \in G/H$ に対して,

$$(gH)(g'H) := gg'H.$$

証明. 積が well-defined であることを示そう.

$g_1H = g_1'H$, $g_2H = g_2'H$ であると仮定する. 同値関係の定義より, $g_1^{-1}g_1' \in H$, $g_2^{-1}g_2' \in H$ である. このとき, 示すことは $g_1g_2H = g_1'g_2'H$ であること, すなわち $(g_1g_2)^{-1}g_1'g_2' \in H$ である. ここで,

$$(g_1g_2)^{-1}g_1'g_2' = g_2^{-1}g_1^{-1}g_1'g_2g_2^{-1}g_2'$$

である. 仮定より, $g_1^{-1}g_1'$, $g_2^{-1}g_2 \in H$ であり, H は G の正規部分群であるから, $g_2^{-1}g_1^{-1}g_1'g_2$ は H に属する. H は群なので $(g_2^{-1}g_1^{-1}g_1'g_2)(g_2^{-1}g_2') \in H$. よって積は well-defined である.

(G1) 任意の $xH, yH, zH \in G/H$ に対して,

$$\{(xH)(yH)\}zH = (xyH)(zH) = (xy)zH = x(yz)H = (xH)(yzH) = xH\{(yH)(zH)\}.$$

(G2) 単位元は eH である.

(G3) 任意の $xH \in G/H$ に対して, これの逆元は $x^{-1}H$ である. □

定義 4.11. $H \triangleleft G$ であるとき, 群 G/H を G の H による **剰余群** と呼ぶ.

レポート 4-3　3 次対称群 S_3 の部分群 $H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle$ が S_3 の正規部分群であることを示せ.