代数学 I 第 6 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

これまでの講義では様々な群と部分群の例を見てきた．今回からは少し抽象的に群に関する一般論を解説してゆく．抽象度は上がるが，常にこれまで勉強してきたような様々な具体例を頭に浮かべながらついてきてもらいたい．今回は，群が与えられた時にその部分群を構成する一般的な方法について解説を行う．以下では，群の単位元をしばしば断り無く e と書く．さらに，群の元 g, h に対し，それらの二項演算の結果 gh を与えることを，g と h を「掛ける」という言い方をすることにする．

5.1 自明な部分群

まず，ウォーミングアップとして自明な例を書いておこう．数学において自明な例は面白いものでは無いが，きちんと意識しておくことはいつも大事である．

定義 5.1

G を群とする．このとき，

- 単位元のみからなる G の部分集合 $\{e\}$
- G 自身

はどちらも G の部分群である．これらを G の**自明な部分群**という．

5.2 部分集合の生成する部分群

群 G の部分集合が与えられるとそこから G の部分群を生成することができる．

定義 5.2

S を群 G の任意の部分集合とする．このとき，

$$\langle S\rangle \coloneqq \{g_1^{m_1}\cdots g_k^{m_k} \mid g_i \in S, m_i \in \mathbb{Z}\ (i=1,\dots,k), k \in \mathbb{N}\} (\subset G)$$

とする．言葉で書くと，$\langle S\rangle$ は「S の元とその逆元たちを何度も掛けてできる元全体のなす集合」である．このとき，$\langle S\rangle$ は定義から二項演算と逆元を取る操作で閉じており，G の部分群となる．これを，S **で生成される部分群**という．
$G = \langle S\rangle$ となるとき，S **は** G **を生成する**と言い，S を G の**生成系**と言う．また，このとき S の元は**生成元**と呼ばれる．

例えば，S が $S = \{a, b, c\}$ という 3 つの元からなる集合であった場合，$\langle S\rangle$ は

$$e(=a^0),\ a,\ ab^2,\ ac^2b^{-3}a,\ b^4c^{-2}a^{-1}b^2c^4b^2c^{-6}a,\ c^{-2}, \cdots$$

などを全て集めてきてできる集合である．これは二項演算と逆元を取る操作で閉じているということも明らかであろう．例えば，ab^2 と $ac^2b^{-3}a$ を掛けてできる元は $ab^2ac^2b^{-3}a$ なのでやはり $\langle S\rangle$ の元であり，$b^4c^{-2}a^{-1}b^2c^4b^2c^{-6}a$ の逆元 $a^{-1}c^6b^{-2}c^{-4}b^{-2}ac^2b^{-4}$ も $\langle S\rangle$ の元である．

* *e-mail* : hoya@shibaura-it.ac.jp

命題 5.3

群 G の部分集合 S に対し，$\langle S\rangle$ は S を含む最小の部分群である．

証明. H を S を含む G の部分群としたとき，$\langle S\rangle \subset H$ となることを言えば良い．第 1,2 回講義資料命題 1.5 より，H は二項演算と逆元を取る操作で閉じていることから，H は S の元とその逆元たちを何度も掛けてできる元を全て含んでいる．つまり $\langle S\rangle \subset H$ である． □

例 1. n を 2 以上の整数としたとき，以下が成立する．

(1) 第 4 回講義資料定理 3.7 より，n 次対称群 $\mathfrak{S}_n$ は隣接互換のなす集合 $\{(1\ 2), (2\ 3), \ldots, (n-1\ n)\}$ によって生成される．つまり，
$$\langle\{(1\ 2), (2\ 3), \ldots, (n-1\ n)\}\rangle = \mathfrak{S}_n$$
である．

(2) 定義より n 次二面体群 D_n は $\{\sigma, \tau\}$ によって生成される．つまり，
$$\langle\{\sigma, \tau\}\rangle = D_n$$
である．ここで，σ, τ は第 5 回講義資料のものとする (以下同様).

例 2. D_4 において $\{\sigma^2, \tau\}$ が生成する部分群は
$$\langle\{\sigma^2, \tau\}\rangle = \{e, \sigma^2, \tau, \sigma^2\tau\}$$
である．実際，$H = \{e, \sigma^2, \tau, \sigma^2\tau\}$ とすると，H の全ての元は σ^2, τ らに二項演算を施すことで得られるので $H \subset \langle\{\sigma^2, \tau\}\rangle$ である．$\{\sigma^2, \tau\} \subset H$ でもあるから，あとは H が D_4 の部分群であることが示されれば，命題 5.3 で述べた最小性により，$H = \langle\{\sigma^2, \tau\}\rangle$ であることがわかる．いま，H の元らの間の二項演算の結果は以下の表のようになる．

	e	σ^2	τ	$\sigma^2\tau$
e	e	σ^2	τ	$\sigma^2\tau$
σ^2	σ^2	e	$\sigma^2\tau$	τ
τ	τ	$\sigma^2\tau$	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	τ	σ^2	e

ただし，g 行 g' 列に gg' を書くというルールで表を書いている (このような表を群の**乗積表**と言う)．D_4 においては，$\tau\sigma^2 = \sigma^{-2}\tau = \sigma^2\tau$ であるということに注意しよう．この表より，H は二項演算と逆元を取る操作で閉じていることがわかる．よって，H が D_4 の部分群であることが示され，$H = \langle\{\sigma^2, \tau\}\rangle$ であることがわかった．

5.3 群の元の位数，巡回群

群 G の 1 元からなる部分集合 $\{g\}$ で生成される部分群は，定義より
$$\langle\{g\}\rangle = \{g^m \mid m \in \mathbb{Z}\}$$
となる．これを単に $\langle g\rangle$ と書く．$g^m g^{m'} = g^{m+m'} = g^{m'} g^m$ なので $\langle g\rangle$ は可換群である．

例 3. $n \geq 3$ とし，$D_n = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$ を n 次二面体群とする．このとき，
$$\langle\sigma\rangle = \{\sigma^m \mid m \in \mathbb{Z}\} = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$$
である．なお，
$$\langle\sigma^{-1}\rangle = \{\sigma^{-m} \mid m \in \mathbb{Z}\} = \{\sigma^m \mid m \in \mathbb{Z}\} = \langle\sigma\rangle.$$
となる．一般に群 G とその元 $g \in G$ に対して，同様の計算により $\langle g\rangle = \langle g^{-1}\rangle$ である．

定義 5.4

群 G の各元 $g \in G$ に対し，G の部分群 $\langle g \rangle$ の位数を g **の位数 (order)** といい，$\operatorname{ord} g$ と書く．

ここで，「位数」という用語が群論において 2 通り現れたことに注意しよう．

- G の位数 (=G の元の個数) と，
- G の元 g の位数 (上で定義したもの)

である．例 3 で述べたように，一般に $\langle g \rangle = \langle g^{-1} \rangle$ なので，$\operatorname{ord} g = \operatorname{ord} g^{-1}$ である．

例 4. 例 3 における計算より，D_n において，

$$\operatorname{ord} \sigma = \#\langle \sigma \rangle = n$$

である．

例 5. $n \in \mathbb{Z}_{>0}$ とし，整数の剰余類群 $\mathbb{Z}/n\mathbb{Z}$ を考える．$a \in \mathbb{Z}_{>0}$ に対して，

$$\langle [a]_n \rangle = \{ [ma]_n \mid m \in \mathbb{Z} \}$$

である ($\mathbb{Z}/n\mathbb{Z}$ における二項演算は $+$ であったことに注意)．このとき，第 3 回復習レポート課題解答問題 2 補足解説に書いた定理により，$\{ [ma]_n \mid m \in \mathbb{Z} \}$ の位数は $n/\gcd(a,n)$ である．よって，

$$\operatorname{ord} [a]_n = n/\gcd(a,n).$$

例えば，

$$\operatorname{ord} [2]_7 = 7, \quad \operatorname{ord} [4]_6 = 3, \quad \operatorname{ord} [8]_{12} = 3$$

である．

群の元 g の位数 $\operatorname{ord} g$ の計算は以下の命題を頭に置いておくと行いやすい．

命題 5.5

群 G の元 g に対し，$\operatorname{ord} g$ は $g^m = e$ となる最小の正の整数 m である．ただし，$g^m = e$ となる正の整数が存在しないとき，$\operatorname{ord} g = \infty$ である．

証明. $\operatorname{ord} g = \#\langle g \rangle < \infty$ のとき，ある $m_1, m_2 \in \mathbb{Z}, m_1 < m_2$ が存在して，

$$g^{m_1} = g^{m_2}$$

となる．このとき，両辺に g^{-m_1} を掛けると，

$$e = g^{m_2 - m_1}$$

なので，$g^m = e$ となる正の整数 m は少なくとも 1 つは存在することがわかる．このうち最小のものを ℓ とすると，

$$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \} = \{ e, g, \ldots, g^{\ell - 1} \}$$

である．いま示すべきことは，$\ell = \operatorname{ord} g$ なので，あとは $e, g, \ldots, g^{\ell-1}$ が全て異なる元であることを示せばよい．もし，$g^{k_1} = g^{k_2}$ $(0 \leq k_1 < k_2 \leq \ell - 1)$ となったとすると，両辺に g^{-k_1} を掛けることで，$e = g^{k_2 - k_1}$ となるが，$0 < k_2 - k_1 \leq \ell - 1$ なので，これは ℓ の最小性に矛盾する．よって，$0 \leq k_1 < k_2 \leq \ell - 1$ のとき $g^{k_1} = g^{k_2}$ とはならない．よって，$\ell = \operatorname{ord} g$ であることが示された．

また，上の議論により，$\operatorname{ord} g < \infty$ のとき，$g^m = e$ となる正の整数は存在するので，$g^m = e$ となる正の整数が存在しないのであれば，$\operatorname{ord} g = \infty$ である． □

例 6. 巡回置換 $(i_1\ i_2 \cdots i_k) \in \mathfrak{S}_n$ に対し，第 4 回講義資料命題 3.4 (2) より，

$$(i_1\ i_2 \cdots i_k)^\ell \neq e \quad (1 \leq \ell \leq k-1), \qquad (i_1\ i_2 \cdots i_k)^k = e$$

なので，$(i_1\ i_2 \cdots i_k)^\ell = e$ となる最小の整数 ℓ は k である．よって，

$$\operatorname{ord}(i_1\ i_2 \cdots i_k) = k. \tag{$*$}$$

一般に $\sigma_1, \ldots, \sigma_s$ をどの 2 つも互いに素な巡回置換とする．このとき，第 4 回講義資料命題 3.6 の互いに素な巡回置換の可換性より，各 $\ell \in \mathbb{Z}$ に対し，

$$(\sigma_1 \cdots \sigma_s)^\ell = \sigma_1^\ell \cdots \sigma_s^\ell$$

が成立する．このことから，$\#S(\sigma_1), \ldots, \#S(\sigma_s)$ の最小公倍数を L とすると，$(*)$ より，

$$\operatorname{ord}(\sigma_1 \cdots \sigma_s) = L$$

である．例えば，第 4 回講義資料定理 3.7 の直後で扱った $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 8 & 7 & 6 & 9 & 1 & 5 & 10 & 3 \end{pmatrix} \in \mathfrak{S}_{10}$ を考えると，

$$\sigma = (1\ 4\ 7)(3\ 8\ 5\ 6\ 9\ 10)$$

であり，$\#S((1\ 4\ 7)) = 3, \#S((3\ 8\ 5\ 6\ 9\ 10)) = 6$ なので，

$$\operatorname{ord}\sigma = 6$$

である．実際，$\sigma^6 = (1\ 4\ 7)^6(3\ 8\ 5\ 6\ 9\ 10)^6 = e \cdot e = e$ である．

定義 5.6

群 G においてある $g \in G$ が存在して $G = \langle g \rangle$ となるとき，G を**巡回群 (cyclic group)** といい，g を G の**生成元**という．

5.3 節冒頭の計算より，巡回群は可換群である．また，生成元の取り方は 1 つとは限らない ($\langle g \rangle = \langle g^{-1} \rangle$ なので，g が生成元であれば少なくとも g^{-1} は生成元である)．以下の命題は定義からすぐにわかる．

命題 5.7

群 G の元 g に対し，以下の同値関係が成立する．

(1) $\operatorname{ord} g = 1 \Leftrightarrow g = e$.

(2) G が有限群のとき，

$$\operatorname{ord} g = \#G \Leftrightarrow G \text{ は巡回群で，} g \text{ はその生成元}$$

例 7. 以下が巡回群，巡回群でないものの例である．

- $n, a \in \mathbb{Z}_{>0}$ を互いに素な整数とする．このとき例 5 での計算より，$\operatorname{ord}[a]_n = n$．特に，$\operatorname{ord}[1]_n = n$．よって，$\mathbb{Z}/n\mathbb{Z} = \langle [a]_n \rangle$ であるので，$\mathbb{Z}/n\mathbb{Z}$ は巡回群であり，$[a]_n$ は $\mathbb{Z}/n\mathbb{Z}$ の生成元である．
- $\mathbb{Z} = \langle 1 \rangle$ であるので，加法群 $\mathbb{Z}$ は巡回群であり，1 は $\mathbb{Z}$ の生成元である．ここで，加法群 $\mathbb{Z}$ においては，二項演算が $+$ であることに注意．$\operatorname{ord} 1 = \infty$ である．
- $n \in \mathbb{Z}_{>0}$ に対し，乗法群 $\mathbb{C}^\times$ の部分群 $\mu_n := \{e^{\frac{2m\pi}{n}i} \mid m \in \mathbb{Z}\}$ を考える． このとき，$\mu_n = \langle e^{\frac{2\pi}{n}i} \rangle$ であるので，μ_n は巡回群であり，$e^{\frac{2\pi}{n}i}$ は μ_n の生成元である．$\operatorname{ord} e^{\frac{2\pi}{n}i} = n$ である．
- $n \geq 3$ のとき，二面体群 D_n は非可換群なので，D_n は特に巡回群ではない．例 4 より，D_n において，$\operatorname{ord}\sigma = n$ である．また，任意の $k = 0, 1, \ldots, n-1$ に対し，

  $$(\sigma^k\tau)(\sigma^k\tau) = \sigma^k(\tau\sigma^k)\tau = \sigma^k(\sigma^{-k}\tau)\tau = \tau^2 = e$$

  となるので，$\operatorname{ord}\sigma^k\tau = 2$ である．“正 n 角形の板の対称変換” という考え方からすると，各 $\sigma^k\tau$ は適当な対称軸に関する折り返しに対応する (正 n 角形の対称軸は n 本あるので，このような元が計 n 個ある)．