第 3 回 赤雪江ゼミ

climax

2025 年 6 月 24 日

目次

1　部分群と生成元

この節では、群の部分集合が生成する部分群と、巡回群の概念について見ていく。

1.1　生成された部分群

まず、群の任意の部分集合から部分群を構成する方法を定義する。

■教科書 p.35　G を群、$S \subset G$ を部分集合とする。$x_1, \ldots, x_n \in S$ に対し、$x_1^{\pm 1} \cdots x_n^{\pm 1}$ という形の G の元を、S の元による**語 (word)** という。 ただし、$n = 0$ の場合は、語は単位元 1_G を表すものとする。

命題 1.1 (教科書 p.35 命題 2.3.13)**.** S の元による語全体の集合を $\langle S \rangle$ とするとき、次の *(1), (2)* が成り立つ。

1. $\langle S \rangle$ は G の部分群である。

2. H が G の部分群で S を含めば、$\langle S \rangle \subset H$ である（つまり $\langle S \rangle$ は S を含む最小の部分群である)。

証明. (1) $n = 0$ の場合、語は 1_G と定義されるため、$1_G \in \langle S \rangle$ である。 $w_1, w_2 \in \langle S \rangle$ をとる。これらは S の元による語であるから、$w_1 = x_1^{\pm 1} \cdots x_n^{\pm 1}$, $w_2 = y_1^{\pm 1} \cdots y_m^{\pm 1}$ $(x_i, y_j \in S)$ と書ける。 このとき、積 $w_1 w_2 = x_1^{\pm 1} \cdots x_n^{\pm 1} y_1^{\pm 1} \cdots y_m^{\pm 1}$ も S の元による語であるから、$\langle S \rangle$ の元である。 また、w_1 の逆元は $(x_1^{\pm 1} \cdots x_n^{\pm 1})^{-1} = x_n^{\mp 1} \cdots x_1^{\mp 1}$ であり、これも S の元による語となるため $\langle S \rangle$ に含まれる。 したがって、$\langle S \rangle$ は G の部分群である。

(2) H を S を含む G の任意の部分群とする。 H は部分群なので $1_G \in H$ である。 $S \subset H$ であるから、任意の $x_i \in S$ に対して $x_i \in H$ である。 H は逆元と積について閉じているので、$x_i^{\pm 1} \in H$ であり、任意の語 $x_1^{\pm 1} \cdots x_n^{\pm 1}$ は H の元でなければならない。 したがって、$\langle S \rangle \subset H$ が示された。

定義 1.2 (教科書 p.36)**.** 命題 2.3.13 の $\langle S \rangle$ を S **によって生成された部分群** という。 S を **生成系**、その元を **生成元** という。 特に $S = \{g_1, \ldots, g_n\}$ のとき、$\langle S \rangle$ を $\langle g_1, \ldots, g_n \rangle$ とも書く。

命題 1.3 (教科書 p.36 命題 2.3.14)**.** G を群、$S_1 \subset S_2 \subset G$ を部分集合とする。このとき、$\langle S_1 \rangle \subset \langle S_2 \rangle$ である。

証明. [ノートによる補足] $\langle S_1 \rangle$ の任意の元 g をとる。g は S_1 の元による語なので、$g = x_1^{\pm 1} \cdots x_n^{\pm 1}$ $(x_i \in S_1)$ と書ける。仮定より $S_1 \subset S_2$ であるから、各 x_i は S_2 の元でもある。 したがって、g は S_2 の元による語と見なすことができる。 よって、$g \in \langle S_2 \rangle$ である。以上より $\langle S_1 \rangle \subset \langle S_2 \rangle$ が示された。

例 1.4 (教科書 p.36 例 2.3.15 生成された部分群 1)**.** G を群、$x \in G$, $S = \{x\}$ とする。 $x^{\pm 1} \cdots x^{\pm 1}$ という形の語は、指数の和を k とすると x^k と書ける。 k は任意の整数になりうるので、$\langle S \rangle = \{x^n \mid n \in \mathbb{Z}\}$ となる。例えば、$G = \mathbb{Z}$ (ノートより補足：演算は加法)、$S = \{n\}$ とすると、$\langle S \rangle = n\mathbb{Z}$ である。

1.2　巡回群

定義 1.5 (教科書 p.36 定義 2.3.16)**.** 一つの元で生成される群を **巡回群** という。 群の部分群で巡回群であるものを巡回部分群という。言い換えると、群 G が巡回群であるとは、ある元 $x \in G$ が存在して、G のすべての元 g が $g = x^n$ $(n \in \mathbb{Z})$ という形に書けることである。

例 1.6 (教科書 p.36 例 2.3.17, 2.3.18 巡回群)**.**

- 加法群 $\mathbb{Z}$ は、$\mathbb{Z} = \langle 1 \rangle$ と書けるので、位数が無限大の巡回群である。 例 2.3.15 の $n\mathbb{Z}$ は n を生成元とする $\mathbb{Z}$ の巡回部分群である。
- 環 $\mathbb{Z}/n\mathbb{Z}$ は加法についてアーベル群である。 $\bar{1}$ を i 回足せば $\bar{i}$ となるので、$\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ であり、これ

は位数 n の巡回群である。

命題 1.7 (教科書 p.37 命題 2.3.19)**.** 巡回群はアーベル群である。

証明. G を x で生成される巡回群とすると $G=\{x^n \mid n\in\mathbb{Z}\}$ である。 G の任意の 2 元 g_1, g_2 は、ある整数 i, j を用いて $g_1=x^i, g_2=x^j$ と表せる。このとき、$g_1g_2=x^ix^j=x^{i+j}=x^{j+i}=x^jx^i=g_2g_1$ が成り立つため、G はアーベル群である。 (巡回群の場合は同じ元を並べているだけとみなせる。)

例 1.8 (教科書 p.37 例 2.3.20 生成された部分群 2)**.** $G=\mathfrak{S}_3$, $\sigma=(123)$, $\tau=(12)$ とする。

1. $\sigma^2=(132)$, $\sigma^3=1$ なので、$\langle\sigma\rangle=\{1,(123),(132)\}$ は巡回部分群である。
2. $\tau^2=1$ なので、$\langle\tau\rangle=\{1,(12)\}$ も巡回部分群である。
3. $S=\{\sigma,\tau\}$ とする。 $\langle S\rangle$ は σ, τ を含むため、これらの積から作られる元も含む。教科書では結論のみだが、計算をすると以下のようになる。

$$\sigma\tau\sigma^{-1}=(123)(12)(132)=(23)$$
$$\sigma^2\tau\sigma^{-2}=(123)(23)(132)=(13)$$

教科書にもあるように $(23)=\sigma\tau\sigma^{-1}$、$(13)=\sigma^2\tau\sigma^{-2}$ が成り立つ。 3 つの互換（巡回置換も含む）が生成されれば、$\mathfrak{S}_3$ のすべての元が生成可能である。したがって、$G=\langle\sigma,\tau\rangle$ であり、$\{\sigma,\tau\}$ は $\mathfrak{S}_3$ の生成系である。

2 群の直積

定義 2.1 (教科書 p.37 定義)**.** $\{G_i\}_{i\in I}$ を群の族とし（$I\neq\emptyset$)、集合としての直積を $G=\prod_{i\in I}G_i$ とする。このとき、G 上の積を**成分ごとに定義**する。すなわち、$(g_i)_{i\in I}, (h_i)_{i\in I}\in G$ に対し、その積を

$$(g_i)_{i\in I}(h_i)_{i\in I}\overset{\text{def}}{=}(g_ih_i)_{i\in I}$$

と定める。

■群となることの確認（教科書 p.37-38）　この演算によって G が群となることを確認する。

- **結合法則**: $g=(g_i), h=(h_i), k=(k_i)$ を G の元とすると、各成分 G_i で結合法則が成り立つため、

$$g(hk)=(g_i)_{i\in I}((h_i)_{i\in I}(k_i)_{i\in I})=(g_i(h_ik_i))_{i\in I}=((g_ih_i)k_i)_{i\in I}=(gh)k$$

  となり、G 全体で結合法則が成立する。
- **単位元**: 各 G_i の単位元を 1_{G_i} とするとき、$1_G=(1_{G_i})_{i\in I}$ とおくと、これは G の単位元となる。 実際、

$$(g_i)_{i\in I}1_G=(g_i1_{G_i})_{i\in I}=(g_i)_{i\in I}$$

  であり、同様に $1_G(g_i)_{i\in I}=(g_i)_{i\in I}$ も成り立つ。
- **逆元**: $g=(g_i)_{i\in I}\in G$ の逆元は、$g^{-1}=(g_i^{-1})_{i\in I}$ で与えられる。 なぜなら、

$$gg^{-1}=(g_i)_{i\in I}(g_i^{-1})_{i\in I}=(g_ig_i^{-1})_{i\in I}=(1_{G_i})_{i\in I}=1_G$$

  となるからである。

以上より、$G=\prod_{i\in I}G_i$ はこの演算で群となる。$I=\emptyset$ なら $\prod_{i\in I}G_i=\{1\}$ とみなす。
これを群の**直積**といい、各 G_i を**直積因子**という。

■**補足**

- すべての G_i がアーベル群なら、直積 G もアーベル群である。
- **自然な単射**: 各 $l \in I$ に対し、写像 $i_l : G_l \to \prod_{j \in I} G_j$ を

$$i_l(x) = g_j \quad \text{ただし} \quad g_j = \begin{cases} x & j = l \\ 1_{G_j} & j \neq l \end{cases}$$

  と定義すると、i_l は単射準同型となる。
- **有限個の場合**: $I = \{1, \ldots, t\}$ の場合、直積を $G_1 \times \cdots \times G_t$ とも書く 。このとき、自然な単射 i_l はより明示的に

$$i_l : g_l \mapsto (1_{G_1}, \ldots, 1_{G_{l-1}}, g_l, 1_{G_{l+1}}, \ldots, 1_{G_t})$$

  と表すことができる 。。