ALGEBRA I*

Hiroshi SUZUKI†
Department of Mathematics
International Christian University

2004年度版

目 次

*教科書として、永尾汎著「代数学」朝倉書店 を指定。その関係で、証明なども、この教科書に負うところが多い。アーベル群の基本定理の証明は、鈴木通夫「群論上・下」岩波書店を参照。

†E-mail:hsuzuki@icu.ac.jp

1　群の定義と例

定義 1.1 演算 $\circ$ が定義されている集合を G とする。

- $G1$ G の任意の元 a, b, c に対して、$(a \circ b) \circ c = a \circ (b \circ c)$ が成り立つ。（結合律）
- $G2$ G のある元 e に対して、$e \circ a = a \circ e = a$ が G の任意の元 a について、成り立つ。（単位元の存在）
- $G3$ G の各元 a に対し $a \circ b = b \circ a = e$ となる G の元 b が存在する。（逆元の存在）
- $G4$ G の任意の元 a, b に対して、$a \circ b = b \circ a$ が、成り立つ。（交換律）

$G1$ が成立するとき、半群 (semigroup)、$G1$、$G2$ が成立するとき、モノイド (monoid) $G1$、$G2$、$G3$ が成立するとき、群 (group) という。さらに $G4$ が成立するものをそれぞれ、可換半群、可換モノイド、可換群という。可換群をアーベル群 (abelian group) ともいう。

注　ここで、集合 G に演算 $\circ$ が定義されているとは、

$$f : G \times G \to G \ ((a, b) \mapsto a \circ b)$$

が写像であることをいう。

例 1.1 $(\boldsymbol{Z}, +)$、$(\boldsymbol{Q}, +)$、$(\boldsymbol{R}, +)$、$(\boldsymbol{C}, +)$ は、可換群である。これに対して、$(\boldsymbol{Z}, \cdot)$、$(\boldsymbol{Q}, \cdot)$、$(\boldsymbol{R}, \cdot)$、$(\boldsymbol{C}, \cdot)$ は、モノイドである。後の 3 つは、0 以外の元は、逆元を持つ。そこで、# をつけたときは、0 以外の元を表すとする。このとき、$(\boldsymbol{Q}^{\#}, \cdot)$、$(\boldsymbol{R}^{\#}, \cdot)$、$(\boldsymbol{C}^{\#}, \cdot)$ も可換群になる。

例 1.2 $\mathrm{Mat}(n, \boldsymbol{R})$ で、n 次正方行列全体を表し、$\mathrm{GL}(n, \boldsymbol{R})$ で、n 次正則行列全体を表すものとする。このとき、$(\mathrm{Mat}(n, \boldsymbol{R}), +)$ は、群、$(\mathrm{Mat}(n, \boldsymbol{R}), \cdot)$ は、モノイドであるが、$(\mathrm{GL}(n, \boldsymbol{R}), \cdot)$ は、群となる。これは、可換群ではない。

基本的性質

1. $(G, \circ)$ を半群とする。 $a_1, a_2, \ldots, a_n \in G$ に対して、

$$a_1 \circ a_2 \circ \cdots \circ a_n = (\cdots ((a_1 \circ a_2) \circ a_3) \circ \cdots) \circ a_n$$

で、定義する。このとき、項の前後を入れ替えなければ、括弧の付け方によらず演算の結果は同じである。

例えば、4 個の場合は 5 通りの括弧の付け方があり、それらは、以下のようになる。

$$\begin{aligned} ((a_1 \circ a_2) \circ a_3) \circ a_4 &= (a_1 \circ a_2) \circ (a_3 \circ a_4) = a_1 \circ (a_2 \circ (a_3 \circ a_4)) \\ &= a_1 \circ ((a_2 \circ a_3) \circ a_4) = (a_1 \circ (a_2 \circ a_3)) \circ a_4. \end{aligned}$$

一般の時はどうであろうか。

2. $(G,\circ)$ がモノイドの時は、単位元は、ただ一つ。

   $e, e' \in G$ が $a \circ e = e \circ a = a$、$a \circ e' = e' \circ a = a$ を任意の元 $a \in G$ について満たすとする。
   $$e = e \circ e' = e'.$$

3. $(G,\circ)$ モノイドにおいて、$u \in G$ に対して、$u \circ v = v \circ u = 1$ なる $v \in G$ が存在するとき、u を正則元 v を u の逆元という。モノイドの正則元 u の逆元はただ一つ。
   v と w を u の逆元とする。
   $$v = v \circ e = v \circ (u \circ w) = (v \circ u) \circ w = e \circ w = w.$$

. 以後、$a \circ b$ を ab、e を 1、正則元 u の逆元を u^{-1} と、積表示する。また、x の n 個の積を、$x \cdot x \cdots x = x^n$、x^{-1} の n 個の積を、$x^{-1} \cdot x^{-1} \cdots x^{-1} = x^{-n}$ とかく。これにより、任意の整数 n に関して、x^n が定義された。

命題 1.1 群 G の任意の元 x に対して、$x^2 = 1$ が成り立てば G は、可換群（アーベル群）である。

証明　$a, b \in G$ とする。このとき、
$$ab = ab(ba)^2 = abbaba = ba.$$
従って、G は、交換律 $G4$ を満たす。 ■

注　上の証明で、暗黙の内に、一般結合律を用いている。

命題 1.2 モノイド G の正則元全体 $U(G)$ は、G の演算に関して、群になる。

証明　まず、演算が定義できること、すなわち、G の演算に関して、$U(G)$ が閉じていることを示す。$a, b \in U(G)$ とする。$abb^{-1}a^{-1} = 1$ より、ab は、正則元、従って、$ab \in U(G)$。また、$1 \cdot 1 = 1$ より、$1 \in U(G)$。$a^{-1}a = aa^{-1} = 1$ より、a^{-1} は、a を逆元に持つから、$a^{-1} \in U(G)$。これらにより、$U(G)$ は、G の演算に関して、群となる。 ■

例 1.3 $\boldsymbol{Z}$ を 乗法に関するモノイドとすると、$U(\boldsymbol{Z}) = \{\pm 1\}$ となり、これは、積に関して、群となる。同様に、$U(\boldsymbol{Q}) = \boldsymbol{Q}^{\#}$、$U(\boldsymbol{R}) = \boldsymbol{R}^{\#}$、$U(\boldsymbol{C}) = \boldsymbol{C}^{\#}$ なども、これから、群になる。$U(\mathrm{Mat}(n, \boldsymbol{R})) = \mathrm{GL}(n, \boldsymbol{R})$。この群を一般線形群という。

2　部分群

定義 2.1 群 G の部分集合 H が G の演算に関して群になるとき、H を G の部分群であるといい、$H \leq G$ と書く。

命題 2.1 G を群とする。このとき、次は、同値。

(1) $H \leq G$。

(2) (i) $\emptyset \neq H \subset G$、$(ii)$ $a, b \in H \to ab \in H$、(iii) $a \in H \to a^{-1} \in H$。

証明　(1) ⇒ (2) 明らか。

(2) ⇒ (1) (ii) より、演算に関して閉じている。(i) より、$a \in H$ とすると、(iii)、(ii) より、$a^{-1} \in H$、従って、$1 = aa^{-1} \in H$。結合律は、G で成立しているから、H でも成立。従って、H は、G の演算に関して、群となる。 ■

$A, B \subset G$ とする。このとき、

$$AB = \{ab \mid a \in A,\ b \in B\},\ A^{-1} = \{a^{-1} \mid a \in A\}$$

と書く。特に、$B = \{b\}$ の時、$AB = Ab$、$BA = bA$ ともかく。

この記法を用いると、

$$H \leq G \Leftrightarrow \emptyset \neq H \subset G,\ HH \subset H,\ H^{-1} \subset H.$$

常に、$G \leq G$、$\{1\} \leq G$ である。これらを自明な部分群と呼び、特に、$\{1\}$ を 1 とも書く。

$S \subset G$ のとき、

$$< S >= \{a_1^{n_1} \cdot a_2^{n_2} \cdots a_r^{n_r} \mid a_1, a_2, \ldots, a_r \in S,\ n_1, n_2, \ldots, n_r \in \boldsymbol{Z}\}$$

を S で生成される部分群という。これは、実際、G の部分群となる。

特に、一つの元 a で生成される部分群、

$$< a >= \{a^n \mid n \in \boldsymbol{Z}\}$$

を a で生成された巡回群といい、a を生成元という。

群 G の元の数を 位数 (order) といい、$|G|$ と書き $o(a) = |< a >|$ を 元 a の位数と呼ぶ。

命題 2.2 巡回群 $< a >$ について、$S = \{n \in \boldsymbol{N} \mid a^n = 1\}$ とする。

(1) $S = \emptyset$ の時、$\min S = n$ とする。このとき、$o(a) = |< a >| = n$ で、次が成立。

　(i) $a^m = 1 \Leftrightarrow n \mid m$、$(ii)$ $< a >= \{1, a, a^2, \ldots, a^{n-1}\}$。

(2) $S \neq \emptyset$ のとき、$< a >$ は、無限巡回群で、$\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots$ は、すべて異なる。

証明　(1) $m = nq + r$、$q, r \in \boldsymbol{Z}$、$0 \leq r < n$ とする。$a^n = 1$ より、

$$a^m = a^{nq+r} = (a^n)^q \cdot a^r = a^r$$

で、$r < n$ だから、

$$a^m = 1 \Leftrightarrow r = 0 \Leftrightarrow n \mid m.$$

従って、$< a > \subset \{1, a, a^2, \ldots, a^{n-1}\} \subset < a >$。さらに、

$$a^i = a^j \to a^{i-j} = 1 \to n \mid i - j,\ 0 \leq i, j \leq n - 1$$

より、$i = j$、従って、$1, a, \ldots, a^{n-1}$ は、すべて異なり、$o(a) = n$。

(2) $a^i = a^j$、$i > j$ とすると、$a^{i-j} = 1$、$i - j \in \boldsymbol{N}$ より、$S = \emptyset$ に矛盾。従って、a^i は、すべて異なり、$< a >$ は、無限巡回群。 ■

例 2.1 $(\boldsymbol{Z}, +)$ 無限巡回群。a^i は、この場合は、ia のこと。

$(\boldsymbol{Z}_n, +)$、$\boldsymbol{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ において、演算を

$$\bar{i} + \bar{j} = \overline{i + j \text{ の } n \text{ による剰余}}$$

とすると、$\boldsymbol{Z}_n$ は、位数 n の巡回群になる。

例 2.2 X を集合としたとき、X^X で X から X 自身への写像全体の集合を表すものとする。$\sigma \in X^X$ のとき、$a \in X$ の σ による像を、a^σ と書くことにする。$\sigma, \tau \in X^X$ に対して、$\sigma \cdot \tau : a \mapsto (a^\sigma)^\tau$ とすると、$\sigma \cdot \tau \in X^X$ となり、X^X は、モノイドになる。この正則元の全体 $S^X = U(X^X)$ は、X から、X への全単射全体となるが、これを、X 上の対称群という。$X = \{1, 2, \ldots, n\}$ のときは、S^X を S_n と書き、n 次対称群という。$\sigma \in S_n$ のとき、

$$\sigma = \begin{pmatrix} i \\ i^\sigma \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1^\sigma & 2^\sigma & \cdots & n^\sigma \end{pmatrix}$$

で表す。また、$(i_1, i_2, \ldots, i_r)$ で、$i_j^\sigma = i_{j+1}$、$(j = 1, \ldots, r-1)$、$i_r^\sigma = i_1$ それ以外の、i については、$i^\sigma = i$ である置換を表し、r 次の巡回置換という。２次の巡回置換を互換という。

3　剰余類

まず、同値関係、同値類、類別 について復習し、群に応用する。

定義 3.1 集合 A における関係 $\sim$ が、3つの条件

(i) $a \sim a$　(ii) $a \sim b \to b \sim a$　(iii) $a \sim b,\ b \sim c \to a \sim c$。

を満たすとき、$\sim$ を同値関係 (equiavelence relation) という。このとき、$C_a = \{b \in A \mid a \sim b\}$ （a と同値な元全体）を、a を含む同値類という。

補題 3.1 同値類について次が成立。

(1) $a \in C_a$

(2) $b \in C_a \Leftrightarrow C_a = C_b$

(3) $C_a \neq C_b \Leftrightarrow C_a \cap C_b = \emptyset$

証明　(1) 同値関係の (i) より明らか。

(2) (ii) によって、$b \in C_a \Leftrightarrow a \in C_b$。従って、$C_a \subset C_b$ を示せばよい。$c \in C_a$ とすると、$a \sim c, a \sim b$ より、$b \sim c$。これは、$c \in C_b$ を意味する。

(3) $c \in C_a \cap C_b$ とすると、(2) より、$C_a = C_c = C_b$ 従って、(3) が成立する。 ■

$\{C_\lambda \mid \lambda \in \Lambda\}$ を異なる同値類としたとき、

$$A = \cup_{\lambda \in \Lambda} C_\lambda \ \ \text{(disjoint union)}$$

を類別、$a_\lambda \in C_\lambda$ を代表元 $\{a_\lambda \mid \lambda \in \Lambda\}$ を完全代表系という。

数学においては、各所で、同値関係を定義し、それによって、類別するということをよく用いるが、群においては、様々な形で、同値関係が、自然に定義される。まずは、部分群が与えられたときのいくつかの同値関係の定義、それによる類別とその応用を述べる。

$H \leq G$ のとき、右合同 $\equiv_r$ を、次のように定義する。

$$a, b \in G \text{ について、} a \equiv_r b \, (\mathrm{mod} H) \Leftrightarrow ab^{-1} \in H.$$

このとき、$\equiv_r$ は、同値関係になる。a を含む同値類は $\{b \in G \mid a \equiv_r b \, (\mathrm{mod} H)\} = Ha$ となる。これを右剰余類という。したがって、$Ha = Hb \Leftrightarrow ab^{-1} \in H$ である。G における H の異なる右剰余類の集合 $\{Ha_i \mid i \in I\}$ を、$H \backslash G$ と書き、G の右剰余類への分解を、G の H による右分解という。

$$G = \sum_{i \in I} Ha_i = Ha_1 + Ha_2 + \cdots + Ha_n \quad \text{（有限の時）}$$

とも書く。$\{a_i \mid i \in I\}$ を $H \backslash G$ の完全代表系という。右剰余類の個数 $|H \backslash G|$ を H の G における指数 (index) と呼び、$|G : H|$ と書く。

左合同 $\equiv_l$ を、次のように定義する。

$$a, b \in G \text{ について、} a \equiv_l b\,(\mathrm{mod} H) \Leftrightarrow a^{-1}b \in H.$$

すると、右合同の時と同様に、$\equiv_l$ は、同値関係になる。a を含む同値類は $\{b \in G \mid a \equiv_l (\mathrm{mod} H)\} = Ha$ となる。これを左剰余類といい。左分解なども同様に定義される。

$$H\backslash G = \{Ha_i \mid i \in I\} \ni Ha \leftrightarrow a^{-1}H \in \{a_i^{-1}H \mid i \in I\} = G/H$$

なる対応により、右剰余類と、左剰余類は 1 対 1 に対応する。特に、

$$|H\backslash G| = |G/H| = |G : H|.$$

定理 3.2 (Lagrange 1736–1813) G を有限群 H を G の部分群とすると、

$$|G| = |G : H||H|.$$

特に、H の位数も、指数も共に G の位数の約数である。

証明　まず 任意の $a \in G$ に対して $|H| = |Ha|$ である。このことは、例えば、

$$r_a : H \to Ha\ (h \mapsto ha)$$

が全単射であることから分かる。従って、

$$G = \sum_{i=1}^{n} Ha_i$$

を H による G の右分解とすると、$n = |G : H|$、$Ha_i \cap Ha_j = \emptyset\ (i \neq j)$。これより、

$$|G| = \left|\sum_{i=1}^{n} Ha_i\right| = \sum_{i=1}^{n} |Ha_i| = \sum_{i=1}^{n} |H| = n|H| = |G : H||H|.$$

これより、定理の主張が得られる。 ■

系 3.3 G を有限群、$a \in G$ とする。このとき、$o(a)$ は、$|G|$ の約数である。特に、$a^{|G|} = 1$。

証明　$o(a) = |<a>|$ だったから、$o(a)$ も部分群の位数であり、$|G|$ を割り切る。 ■

系 3.4 位数 $|G|$ が素数の群 G は、巡回群である。

証明　$|G| \neq 1$ だから、$1 \neq a \in G$ を取る。$o(a) \neq 1$ で、かつ、$o(a)$ は、$|G|$ の約数である。仮定から、$o(a) = |G|$ となり、$|<a>| = |G|$ だから、$G = <a>$ を得る。 ■

例 3.1 $S_3 = \{1, (12), (13), (23), (123), (132)\}$ の 6 個の元の位数は、それぞれ、1, 2, 2, 2, 3, 3 である。$|S_3| = 6$ だから、S_3 の部分群の位数は、1, 2, 3, 6 のいずれかである。位数が、1 の場合は、単位元 1 だけからなり、6 の場合は、S_3 となることは明らかである。2 又は、3 のときは、共に素数だから、系 3.4 より、巡回群、すべて、それぞれ、位数が、2、3 の元で生成されることが分かる。従って、$< (123) >=< (132) >= \{1, (123), (132)\}$ であることに注意すると、位数が、2 の部分群は、$< (12) >, < (13) >, < (23) >$ の 3 種類、位数が、3 のものは、$< (123) >$ の一つだけであることが分かる。この様に、S_3 には、全部で、6 個の部分群がある。

H、K を群 G の部分群とする。$a, b \in G$ について、

$$a \equiv b \,(\mathrm{mod}(H, K)) \Leftrightarrow b = hak \;\text{ for some }\; h \in H, k \in K$$

とすると、これは同値関係になる。a を含む同値類は、明らかに、HaK となり、(H, K) の G における両側剰余類と呼ばれる。G における (H, K) の異なる両側剰余類の集合 $\{Ha_iK \mid i \in I\}$ を $H\backslash G/K$ と書き、

$$G = \sum_{i \in I} Ha_iK$$

を G の (H, K) による両側分解という。

命題 3.5 $H, K \leq G$、$a \in G$ とする。K の $K \cap a^{-1}Ha$ による右分解を

$$K = \sum_{j \in J} (K \cap a^{-1}Ha)k_j$$

とすれば、$\{Hak_j \mid j \in J\}$ は、HaK に含まれる H の異なる右剰余類全体と一致する。特に、G が有限群の時は、

$$|HaK| = |H||K : K \cap a^{-1}Ha|.$$

さらに、$G = \sum_{i \in I} Ha_iK$ （すなわち、$\{a_i \mid i \in I\}$ を両側剰余類の完全代表系）とすると、

$$|G : H| = \sum_{i \in I} |K : K \cap a^{-1}Ha_i.$$

証明　$k, k' \in K$ に対して、

$$\begin{aligned} Hak = Hak' \quad &\Leftrightarrow \quad akk'^{-1}a^{-1} \in H \\ &\Leftrightarrow \quad kk'^{-1} \in K \cap a^{-1}Ha \\ &\Leftrightarrow \quad (K \cap a^{-1}Ha)k = (K \cap a^{-1}Ha)k' \end{aligned}$$

これよりすべての主張をうる。 ■

系 3.6 $|HK| = |H||K : K \cap H| = |H||K|/|K \cap H|.$

証明　上の命題において、$a = 1$ と置く。 ■

4　巡回群

G が巡回群 (cyclic group) であるとは、G の元 a で、

$$G =< a >= \{a^n \mid n \in bZ\}$$

となるものが存在する事であった。この、a を巡回群 G の生成元と言う。

定理 4.1 $G =< a >$ を巡回群とする。このとき、以下が成り立つ。

(1) $1 \neq H \leq G$ とし、$h = \min\{i \in \boldsymbol{N} \mid a^i \in H\}$ とすると、$H =< a^h >$。特に巡回群の部分群は、巡回群。

(2) $|G| = n = ml$ とすると、$< a^l >$ は G の位数 m のただ一つの部分群である。

証明　(1) $1 \neq a^i \in H$ とする。$a^{-i} = (a^i)^{-1} \in H$ だから、$\{i \in \boldsymbol{N} \mid a^i \in H\} \neq \emptyset$。そこで、$h = \min\{i \in \boldsymbol{N} \mid a^i \in H\}$ とする。$a^h \in H$ だから

$$< a^h >= \{(a^h)^i \mid i \in \boldsymbol{Z}\} \subset H.$$

一方、$a^i \in H$、$i = hq + r,\ q, r \in \boldsymbol{Z},\ 0 \leq r < h$ とすると、

$$a^r = a^{i-hq} = (a^i)(a^h)^{-q} \in HH \subset H.$$

h の取り方から $r = 0$。従って、$a^i = a^{hq} \in< a^h >$。

(2) $G =< a >= \{1, a, a^2, \ldots, a^{n-1}\}$、そして、命題 2.2 によって、この n 個の元はすべて異なる。$n = ml$ とする。このとき、m が、$(a^l)^m = 1$ となる、最小の自然数だから、命題 2.2 によって

$$< a^l >= \{1, a^l, a^{2l}, \ldots, a^{(m-1)l}\},\ (a^{ml} = 1)$$

は、G の位数 m の部分群である。一方、$H \leq G$、$|H| = m$ とし、h を (1) の様に取ると、$H =< a^h >$。$a^n = 1 \in H$ だから、n は、h の倍数である。従って、(1) より、$|H| = n/h = m$。これより、$h = l$ を得る。 ■

命題 4.2 $(\boldsymbol{Z}, +)$ は、1 で生成される巡回群である。$a_1, a_2, \ldots, a_r \in \boldsymbol{Z}$ の最大公約数を d とすると、

$$< a_1, a_2, \ldots, a_r >=< d > .$$

従って、$a_1x_1 + a_2x_2 + \cdots + a_rx_r = d$ となる、整数 $x_1, x_2, \ldots, x_r$ となる整数、$x_1, x_2, \ldots, x_r$ が存在する。

証明　$H =< a_1, a_2, \ldots, a_r >= \{a_1x_1 + a_2x_2 + \cdots + a_rx_r \mid x_1, x_2, \ldots, x_r \in \boldsymbol{Z}\}$ である。$\boldsymbol{Z}$ は、巡回群だから、命題 4.1 より、その部分群も巡回群。そこで、$H =< c >= \{cx \mid x \in \boldsymbol{Z}\}$ とすると、$a_i \in H$ より、c は、a_i の約数、従って、c は、d の約数である。また、$c = a_1x_1 + a_2x_2 + \cdots + a_rx_r$ であることより、d は、c の約数である。従って、$c = \pm d$。従って、$< c >=< d >$。 ■

二つの整数 m, n の最大公約数を (m, n) で表す。

命題 4.3 $G =< a >$ を位数 n の有限巡回群とする。このとき、

$$< a^r >=< a^{(n,r)} >, \ o(a^r) = n/(n,r).$$

証明　$d = (n,r)$ とする。$d \mid r$ より、$< a^r >\subset< a^d >$。また、命題 4.2 より、$d = nx + ry$ となる、$x, y \in \boldsymbol{Z}$ が存在する。従って、

$$a^d = (a^n)^x (a^r)^y = (a^r)^y \in< a^r > .$$

すなわち、$< a^d >\subset< a^r >$ を得る。また、定理 4.1 より、$o(a^d) = n/d$。 ■

例 4.1 $(\boldsymbol{Z}_n, +)$ を考える。$\boldsymbol{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ で、

$$\bar{a} + \bar{b} = \overline{a + b \text{ を } n \text{ で割った余り}}$$

であった。上で学んだことより、例えば、$\boldsymbol{Z}_6$ の部分群は、以下の 4 つであることが分かる。

$$< \bar{0} >= \{0\}, \ < \bar{1} >=< \bar{5} >= \boldsymbol{Z}_6, \ < \bar{2} >=< \bar{4} >= \{\bar{0}, \bar{2}, \bar{4}\}, \ < \bar{3} >= \{\bar{0}, \bar{3}\}.$$

例 4.2 $(\boldsymbol{Z}_n, \cdot)$ は、モノイドであった。演算は、

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b \text{ を } n \text{ で割った余り}}.$$

この、正則元全体 $\boldsymbol{Z}_n^* = U(\boldsymbol{Z}_n, \cdot)$ は、群となるが、これを既約剰余類群と呼ぶ。また、その位数 $|\boldsymbol{Z}_n^*|$ を $\phi(n)$ と書く。ϕ は、オイラー関数 (Euler function) と呼ばれる。

$$\begin{aligned} \bar{a} \in \boldsymbol{Z}_n^* \quad &\Leftrightarrow \quad \bar{a}\bar{b} = \bar{1} \text{ for some } \bar{b} \in \boldsymbol{Z}_n^* \\ &\Leftrightarrow \quad ab + qn = 1 \text{ for some } b, q \in \boldsymbol{Z} \\ &\Leftrightarrow \quad (a, n) = 1 \end{aligned}$$

このことから、$\boldsymbol{Z}_6^* = \{\bar{1}, \bar{5}\}$ は、位数 $\phi(6) = 2$ の巡回群であること、 $\boldsymbol{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ は、位数 $\phi(5) = 4$ の巡回群であることが分かる。p を素数とすると、$\phi(p) = p - 1$ であるが、$\boldsymbol{Z}_p^*$ は、巡回群であることが分かる。しかし、一般的には、$\boldsymbol{Z}_n^*$ は、巡回群であることも、そうでないこともある。また、系 3.3 より以下が成り立つことも分かる。$(a, 6) = 1 \to a^2 \equiv 1 \pmod{6}$、また、$(a, 5) = 1 \to a^4 \equiv 1 \pmod{5}$。より一般には、$(a, n) = 1 \to a^{\phi(n)} \equiv 1 \pmod{n}$。$n$ が素数の時は、フェルマーの小定理と呼ばれ、一般の場合は、オイラーの定理と呼ばれる。

5　正規部分群と剰余群

定義 5.1 G の部分群 N が、G のすべての元 $a \in G$ について $a^{-1}Na = N$ が成り立つとき、N を G の正規部分群であると言い、$N \lhd G$ と書く。この条件は、$Na = aN$ とも書くことが出来る。

アーベル群の部分群は、すべて正規部分群である。条件は、G の元 a と、N の元とが交換可能と言っているのではない。aN と、Na が、集合として同じだと言うことである。

補題 5.1 G の部分群 N について次は同値。

$$N \lhd G \Leftrightarrow (aN)(bN) = abN \ \ \textit{for all}\ a, b \in G.$$

証明　($\Rightarrow$)　$aNbN = abNN = abN$。$H \leq G \Rightarrow HH = H$ であることに注意。

($\Leftarrow$)　$a^{-1} \to a$、$a \to b$、また、$a \to a$、$a^{-1} \to b$ として、適用することによって、

$$\begin{aligned} a^{-1}Na &\subset a^{-1}NaN = a^{-1}aN = N \\ &= a^{-1}aNa^{-1}a \subset a^{-1}aNa^{-1}Na = a^{-1}Na \end{aligned}$$

■

$N \lhd G$ とする。$aN, bN \in G/N$ とするとき、補題 5.1 により、

$$aNbN = abN \in G/N.$$

従って、これにより G/N に演算が定義できる。この演算により G/N は群になる。これを G の N による剰余群 (factor group) と呼ぶ。ここで、

$$1_{G/N} = N = 1N,\ (aN)^{-1} = a^{-1}N.$$

例 5.1 $\boldsymbol{Z}$ はアーベル群であるから、$n\boldsymbol{Z} \lhd \boldsymbol{Z}$。ここで、

$$a \equiv_r b \pmod{n\boldsymbol{Z}} \Leftrightarrow a \equiv b \pmod{n}.$$

$\boldsymbol{Z}/n\boldsymbol{Z} = \{n\boldsymbol{Z}, 1 + n\boldsymbol{Z}, \ldots, n-1+n\boldsymbol{Z}\}$ で、演算は、

$$(a + n\boldsymbol{Z}) + (b + b\boldsymbol{Z}) = (a+b) + n\boldsymbol{Z} = \overline{a+b} + n\boldsymbol{Z}$$

従って、$\boldsymbol{Z}/n\boldsymbol{Z}$ は、本質的に $\boldsymbol{Z}_n$ と同じである。(このことを同型という。)

補題 5.2 群 G の指数 2 の部分群は、正規部分群である。

証明　$a \in H$ とすると、$Ha = H = aH$。一方、$a \notin H$ とすると、$aH \neq H \neq Ha$ だから、$|G:H| = 2$ だから、G の H による右分解も左分解も

$$G = H + Ha = H + aH$$

となる。従って、$aH = G - H = Ha$。これは、上で示したこととあわせると、G のすべての元 a について、$aH = Ha$ が成り立つ。すなわち $H \lhd G$。■

例 **5.2** $|S_n : A_n| = 2$（Exercise 3.5 参照) だから、$A_n \lhd S_n$。さらに、$S_n/A_n = \{A_n, (12)A_n\}$ は、位数 2 の巡回群である。これは、本質的に、$\boldsymbol{Z}_2$、$(\{\pm 1\}, \cdot)$ と同じ（同型）である。

定義 **5.2** G を群、$S \subset G$ とする。このとき、

1. $N_G(S) = \{x \in G \mid x^{-1}Sx = S\}$ を S の正規化群 (normalizer) という。
2. $C_G(S) = \{x \in G \mid x^{-1}sx = s, \text{ for all } s \in S\}$ を S の中心化群 (centralizer) という。
3. $Z(G) = C_G(G)$ を G の中心という。
4. $S = \{a\}$ のときは、$N_G(S) = C_G(S)$ であり、これを、$C_G(a)$ とも書く。

簡単に定義から分かるように、$H \leq G$ とすると、

$$H \lhd G \Leftrightarrow N_G(H) = G.$$

例 **5.3** $G = S_3$、$H =< (123) >= \{1, (123), (132)\} = A_3$、$C_G(H) = H$、$N_G(H) = G$。$(12)^{-1}(123)(12) = (132)$ であることに注意。

$S \subset G$、$x \in G$ のとき、$x^{-1}Sx = \{x^{-1}sx \mid s \in S\}$ を、S^x とも書き、S の x による共役 (conjugate) と言う。$S, T \subset G$ について、$T = S^x$ となる $x \in G$ が存在するとき、T と S は、共役であると言い、$T \sim_G S$ と書く。$\sim_G$ は、$\mathcal{P}(G) = 2^G$ 上の同値関係。また、G の元は、$a \sim_G b$ (すなわち $\{a\} \sim_G \{b\}$) である時、a と b は、共役であるという。その同値類を共役類という。すなわち

$$a \sim_G b \Leftrightarrow b = g^{-1}ag \ \text{ for some } g \in G.$$

$N \lhd G$ とすると、$a \in N$ に対し $g^{-1}ag \in g^{-1}Ng = N$。よって、$N$ は、G の共役類の和集合である。このことを用いると、正規部分群を決定することが楽になることが多い。

例 **5.4** S_3 の共役類は、$\{1\}$, $\{(12), (13), (23)\}$, $\{(123), (132)\}$ で、部分群の位数は、群の位数の約数だから、S_3 の正規部分群は、1, A_3, S_3 のみである。

より一般に

$$\tau = \begin{pmatrix} i \\ i^\tau \end{pmatrix}, \ \sigma = \begin{pmatrix} i \\ i^\sigma \end{pmatrix} \ \text{とすると、} \tau^{-1} = \begin{pmatrix} i^\tau \\ i \end{pmatrix}$$

これより、以下を得る。

$$\tau^{-1}\sigma\tau = \begin{pmatrix} i^\tau \\ i \end{pmatrix}\begin{pmatrix} i \\ i^\sigma \end{pmatrix}\begin{pmatrix} i \\ i^\tau \end{pmatrix} = \begin{pmatrix} i^\tau \\ i^{\sigma\tau} \end{pmatrix}.$$

例えば、

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}, \sigma = (123)(45) \to \tau^{-1}\sigma\tau = (512)(43).$$

従って、巡回置換への分解の型は、保たれ、逆に、型が同じものは、共役であることも分かる。(Exersise 5.8 参照)

6　同型と準同型

群 G から 群 G' への全単射 $f : G \to G'$ があって、

$$f(ab) = f(a)f(b) \text{ (for all } a, b \in G)$$

を満たすとき、G と G' は同型であると言い、$G \simeq G'$ と表す。このとき、f を G から G' への同型写像という。

同型とは ある 1 対 1 対応のもとで、乗積表が同じと言うことである。

例 6.1 $\omega = (-1 + \sqrt{-3})/2$ とする。ω は、1 の原始 3 乗根である。

$\boldsymbol{Z}_3$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\simeq$

$\boldsymbol{Z}/3\boldsymbol{Z}$

$+$	$3\boldsymbol{Z}$	$1+3\boldsymbol{Z}$	$2+3\boldsymbol{Z}$
$3\boldsymbol{Z}$	$3\boldsymbol{Z}$	$1+3\boldsymbol{Z}$	$2+3\boldsymbol{Z}$
$1+3\boldsymbol{Z}$	$1+3\boldsymbol{Z}$	$2+3\boldsymbol{Z}$	$3\boldsymbol{Z}$
$2+3\boldsymbol{Z}$	$2+3\boldsymbol{Z}$	$3\boldsymbol{Z}$	$1+3\boldsymbol{Z}$

$\simeq$

$(\{1, \omega, \omega^2\}, \cdot)$

$+$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

例 6.2 $G =< a >= \{a^n \mid n \in \boldsymbol{Z}\}$ を無限巡回群とする。$\boldsymbol{Z}$ で有理整数の加法群を表す。

$$f : \boldsymbol{Z} \to < a >= \{a^n \mid n \in \boldsymbol{Z}\} \ (n \mapsto a^n)$$

とすると、これは、同型写像である。実際、全単射は 命題 2.2 より明らか。また、

$$f(i + j) = a^{i+j} = a^i a^j = f(i)f(j)$$

を満たす。$\boldsymbol{Z}$ の演算を $+$ で、G の演算を積で書いていることに注意。

例 6.3 $G =< a >= \{1, a, a^2, \ldots, a^{n-1}\}$ を位数 n の巡回群とする。

$$f : \boldsymbol{Z}/n\boldsymbol{Z} \to < a >= \{1, a, a^2, \ldots, a^{n-1}\} \ (i + n\boldsymbol{Z} \mapsto a^i)$$

とする。まず、f は写像となることを確認する。

$$i + n\boldsymbol{Z} = j + n\boldsymbol{Z} \Leftrightarrow i - j \in n\boldsymbol{Z} \Leftrightarrow n \mid i - j \Leftrightarrow a^i = a^j.$$

これは、$i + n\boldsymbol{Z}$ を他の表し方 $j + n\boldsymbol{Z}$ と表しても剰余類として同じならば、$a^i = a^j$ である事を言っている。従って、$\boldsymbol{Z}/n\boldsymbol{Z}$ の元に対して、$< a >$ の元が一つ定まる。すなわち f は、写像である。このことを f を (写像として) well-defined であるという。また、この写像が全単射であることは、明らか。

$$f((i + n\boldsymbol{Z}) + (j + n\boldsymbol{Z})) = f(i + j + n\boldsymbol{Z}) = a^{i+j} = a^i a^j = f(i + n\boldsymbol{Z})f(j + n\boldsymbol{Z})$$

従って、f は同型写像で、G（任意の位数 n の巡回群）は、$\boldsymbol{Z}/n\boldsymbol{Z}$ と同型である。（上で、$f(i+j+n\boldsymbol{Z}) = a^{i+j}$ と出来たのは、一般に $i+n\boldsymbol{Z}$ の対応先を a^i とし、これが well-defined であることを示してあるからである。もし、$i + n\boldsymbol{Z}$ の i を例えば、$0, 1, \ldots, n-1$ に限定すれば、写像の定義は問題ないが、$f(i + j + n\boldsymbol{Z}) = a^{i+j}$ は、明らかではない。以下に現れる準同型定理の証明と比べよ。）

例 6.4 $\boldsymbol{R}$ で、実数全体からなる加法群を表し、$\boldsymbol{R}^+$ で、正の実数からなる乗法群を表すものとする。これらは、以下の対応によって同型である。

$$f : \boldsymbol{R} \to \boldsymbol{R}^+ \ (a \mapsto e^a).$$

実際 $f(a+b) = e^{a+b} = e^a e^b = f(a)f(b)$ を満たす。f が全単射であることを示すのは、直接にも出来るが、$g : \boldsymbol{R}^+ \to \boldsymbol{R} \ (a \mapsto \log a)$ が、$fg = id_{\boldsymbol{R}^+}$、$gf = id_{\boldsymbol{R}}$ を満たすことからも言える。

一般に、写像 $f : X \to Y$、$g : Y \to X$ が与えられたとき、$gf = id_X$ ならば、f が単射、g が全射を満たす。

定義 6.1 G、G' を群とする。写像 $f : G \to G'$ が

$$f(ab) = f(a)f(b) \ (\text{for all } a, b \in G)$$

を満たすとき、f を 準同型（写像）(homomorphism) と言う。全単射準同型を、同型写像と言う。

命題 6.1 $f : G \to G'$ を 準同型とする。このとき、次が成立する。

(1) $f(1_G) = 1_{G'}$。

(2) G の任意の元 a について、$f(a^{-1}) = f(a)^{-1}$。

(3) $\mathrm{Im} f = \{f(a) \mid \in G\} \leq G'$、即ち、$f$ の像は G' の部分群である。

(4) $\mathrm{Ker} f = f^{-1}(1_{G'}) = \{a \in G \mid f(a) = 1_{G'}\} \lhd G$、即ち、$f$ の核は G の正規部分群である。

証明　(1) $f(1) = f(1 \cdot 1) = f(1)f(1)$ である。この両辺に $f(1)^{-1}$ をかけると、$1 = f(1)$ を得る。

(2) $1 = f(1) = f(aa^{-1}) = f(a)f(a^{-1})$ である。この両辺に $f(a)^{-1}$ を左からかけると、$f(a)^{-1} = f(a^{-1})$ を得る。

(3) $f(a)f(b) = f(ab) \in \mathrm{Im} f$、$f(a)^{-1} = f(a^{-1}) \in \mathrm{Im} f$ であるから、$\mathrm{Im} \leq G'$ である。

(4) $a, b \in \mathrm{Ker} f$ とすると、$f(a) = f(b) = 1$。$f(ab) = f(a)f(b) = 1$、$f(a^{-1}) = f(a)^{-1} = 1$ であるから、$ab \in \mathrm{Ker} f$、$a^{-1} \in \mathrm{Ker} f$。従って $\mathrm{Ker} f \leq G$。さらに、$x \in G$ とすると、

$$f(x^{-1}ax) = f(x^{-1})f(a)f(x) = f(x^{-1})f(x) = f(1) = 1$$

より、$x^{-1}ax \in \mathrm{Ker} f$ を得る。従って $\mathrm{Ker} f \lhd G$ である。 ■

例 6.5 N を群 G の正規部分群とする。

$$f : G \to G/N \ (a \mapsto aN)$$

を自然な準同型 (cannonical homomorphism) という。実際、

$$f(ab) = abN = aNbN = f(a)f(b)$$

より、f は準同型写像となる。

7　同型定理

定理 7.1　(準同型定理)　G、G' を群とし、$f: G \to G'$ を準同型とする。このとき、

$$G/\mathrm{Ker}f \simeq \mathrm{Im}f.$$

証明　$K = \mathrm{Ker}f$ とすると、命題 6.1 によって $K \lhd G$。$a, b \in G$ に対して、

$$f(a) = f(b) \Leftrightarrow f(a)f(b)^{-1} = f(ab^{-1}) = 1 \Leftrightarrow ab^{-1} \in K \Leftrightarrow Ka = Kb$$

ここで、$\bar{f}(Ka) = f(a)$ とすると以下のことが分かる。

- $\bar{f}$ は、well-defined（剰余類 Ka の代表元 a の取り方によらず一定)。
- $\bar{f}$ は、単射（$\bar{f}(Ka) = \bar{f}(Kb) \to Ka = Kb$)。
- $\bar{f}$ は、準同型。なぜなら、

$$\bar{f}(KaKb) = \bar{f}(Kab) = f(ab) = f(a)f(b) = \bar{f}(Ka)\bar{f}(Kb).$$

- $\mathrm{Im}\bar{f} = \mathrm{Im}f$。

従って、$\bar{f}: G/K \to \mathrm{Im}f$ は、同型写像。これより $G/K \simeq \mathrm{Im}f$。 ■

定理 7.2　(同型定理)

(1) $H \leq G,\ N \lhd G \Rightarrow NH/N \simeq H/H \cap N.$

(2) $f: G \to G'$ を全射準同型 $H' \lhd G'$、$H = f^{-1}(H')$ とすると、$H \lhd G$ かつ、$G/H \simeq G'/H'$。

証明　(1) $f: H \to G/N$ $(h \mapsto Nh)$ とすると、f は準同型でかつ

$$\mathrm{Im}f = f(H) = NH/N,\ \mathrm{Ker}f = H \cap N$$

従って、定理 7.1 によって $H/H \cap N \simeq NH/N$。

(2) $g: G \xrightarrow{f} G' \to G'/H,\ a \to f(a) \to H'f(a)$ は全射準同型である。

$$\mathrm{Ker}g = \{a \in G \mid H'f(a) = H'\} = \{a \in G \mid f(a) \in H'\} = f^{-1}(H')$$

従って、定理 7.1 によって $G/H \simeq G'/H'$ である。 ■

系 7.3 $H,\ N \lhd G$、$N \subset H$ ならば $G/H \simeq (G/N)\big/(H/N)$。

証明　$f: G \to G/N$ を自然な準同型とする。$f^{-1}(H/N) = H$ であるから、定理 7.2 (2) により主張が得られる。 ■

以下に、準同型定理、同型定理の応用例をあげる。

例 7.1 $G=<a>$ を巡回群とする。$f:\boldsymbol{Z}\to G=<a>=\{a^n\mid n\in\boldsymbol{Z}\}$ $(i\mapsto a^i)$ は、全射準同型である。実際

$$f(i+j)=a^{i+j}=a^ia^j=f(i)f(j).$$

従って、定理 7.1 によって $\boldsymbol{Z}/\mathrm{Ker}f\simeq<a>$。$\mathrm{Ker}f$ は、巡回群 $\boldsymbol{Z}$ の部分群だから 定理 4.1 によって、$\mathrm{Ker}f$ も巡回部分群で $\mathrm{Ker}f\simeq n\boldsymbol{Z}$ と書ける。$n=0$ の時、G は、無限巡回群であり、$<a>\simeq\boldsymbol{Z}/\{0\}\simeq\boldsymbol{Z}$。また、$n\neq 0$ の時は、G は、位数 n の巡回群であり、そのような群は、$\boldsymbol{Z}/n\boldsymbol{Z}$ と同型である。

例 7.2 $f:\boldsymbol{R}\to\boldsymbol{C}$ $(a\mapsto e^{2\pi ai})$ とすると、$\mathrm{Im}f=\{z\in\boldsymbol{C}\mid |z|=1\}$、$\mathrm{Ker}f=\{a\in\boldsymbol{R}\mid e^{2\pi ai}=1\}=\boldsymbol{Z}$。従って準同型定理により $\boldsymbol{R}/\boldsymbol{Z}\simeq S^1$。

例 7.3 $\mathrm{GL}(n,\boldsymbol{R})$ で n 次正則行列全体からなる n 次一般線形群を表すものとする。このとき、

$$f:G=\left\{\left(\begin{array}{cc}A&O\\B&C\end{array}\right)\middle|\,A\in\mathrm{GL}(r,\boldsymbol{R}),\ C\in\mathrm{GL}(s,\boldsymbol{R})\right\}\to\mathrm{GL}(r,\boldsymbol{R})\ \left(\left(\begin{array}{cc}A&O\\B&C\end{array}\right)\mapsto A\right).$$

とすると、これは、全射でかつ、

$$\mathrm{Ker}f=\left\{\left(\begin{array}{cc}I&O\\B&C\end{array}\right)\middle|\,C\in\mathrm{GL}(s,\boldsymbol{R})\right\}\lhd G.$$

ここで、I は、r 次の単位行列を表すものとする。定理 7.1 によって $G/\mathrm{Ker}f\simeq\mathrm{GL}(r,\boldsymbol{R})$ である。

$G\rhd N$、$G\geq H\geq N$ とする。$f:G\to G/N$ $(a\mapsto aN)$ を自然な準同型とする。このとき、

$$f(H)=\{hN\mid h\in N\}=HN/N\leq G/N$$

逆に、$\bar{H}\leq G/N$ とすると、

$$H=f^{-1}(\bar{H})=\{h\in G\mid hN\in\bar{H}\}$$

とすると、$N\lhd H\lhd G$ かつ、$f(H)=H/N=\bar{H}$ である。従って、

$$\mathcal{S}(G,N)=\{H\lhd G\mid N\subset H\}\ \text{:}G\ \text{の部分群で}\ N\ \text{を含むもの全体}$$

$$\mathcal{S}(G/N,1)=\{\bar{H}\mid\bar{H}\leq G/N\}\ \text{:}G/N\ \text{の部分群全体}$$

このとき、$\mathcal{S}(G,N)$ の元、H に対し、$f(H)=H/N$ は、$\mathcal{S}(G/N,1)$ の元であり、$\mathcal{S}(G/N,1)$ の元 $\bar{H}$ に対して、$f^{-1}(\bar{H})$ は、$\mathcal{S}(G,N)$ の元になっている。この対応は、1 対 1 対応である。

例 7.4 $\boldsymbol{Z}\to\boldsymbol{Z}/12\boldsymbol{Z}$ を自然な準同型。このとき、

$$\begin{array}{rcl}\mathcal{S}(\boldsymbol{Z},12\boldsymbol{Z})&=&\{n\boldsymbol{Z}\mid 12\boldsymbol{Z}\subset n\boldsymbol{Z},\ n\mid 12\}\\&=&\{12\boldsymbol{Z},6\boldsymbol{Z},4\boldsymbol{Z},3\boldsymbol{Z},2\boldsymbol{Z},\boldsymbol{Z}\}\\\mathcal{S}(\boldsymbol{Z}/12\boldsymbol{Z},0)&=&\{m\boldsymbol{Z}/12\boldsymbol{Z}\mid n\mid 12\}\\&=&\{0,6\boldsymbol{Z}/12\boldsymbol{Z},4\boldsymbol{Z}/12\boldsymbol{Z},3\boldsymbol{Z}/12\boldsymbol{Z},2\boldsymbol{Z}/12\boldsymbol{Z},\boldsymbol{Z}/12\boldsymbol{Z}\}\end{array}$$

8　群の作用

定義 8.1 G を群、X を集合とする。

$$f : X \times G \to X,\ ((\alpha, a) \in X \times G \mapsto f(\alpha, a) = \alpha^a)$$

が、次の２条件

$$\alpha^1 = \alpha,\ \alpha^{ab} = (\alpha^a)^b$$

を満たすとき、群 G は、集合 X に作用しているといい、X は、G-集合であるという。

X を G-集合、$\alpha, \beta \in X$ のとき、

$$\alpha \sim_G \beta \Leftrightarrow \alpha^a = \beta \ \text{ for some } a \in G$$

とすると、$\sim_G$ は、同値関係になる。この同値類を G-軌道 (G-orbit) という。このとき、α を含む G-軌道 $\{\alpha^a \mid a \in G\}$ を、α^G ともかく。また、$|\alpha^G|$ を　軌道の長さという。

G-軌道がただ一つであるとき、すなわち $X = \alpha^G$ であるとき、可移（可遷とも言う。transitive）という。

$G_\alpha = \{a \in G \mid \alpha^a = \alpha\}$ とすると、$G_\alpha \leq G$ である。$\beta = \alpha^a$ ならば、$x \in G_\alpha$ としたとき、$G_\beta = a^{-1}G_\alpha a$ である。実際、

$$\beta^{a^{-1}xa} = \alpha^{aa^{-1}xa} = \alpha^{xa} = \alpha^a = \beta$$

だから、$G_\beta \subset a^{-1}G_\alpha a$、また、$\alpha = \beta^{a^{-1}}$ だから、$G_\alpha \subset aG_\beta a^{-1}$ である。これは、$a^{-1}G_\alpha a \subset G_\beta$ を意味する。

G_α を α の G における安定部分群と呼ぶ。

定理 8.1 $|\alpha^G| = |G : G_\alpha|$

証明　$a, b \in G$ に対して、

$$\alpha^a = \alpha^b \Leftrightarrow \alpha^{ab^{-1}} = \alpha \Leftrightarrow ab^{-1} \in G_\alpha \Leftrightarrow G_\alpha a = G_\alpha b$$

従って、$\phi : G_\alpha\backslash G \to \alpha^G\ (G_\alpha a \mapsto \alpha^a)$ は、全単射である。 ■

X を G-集合とする。$a \in G$ に対して、$\sigma(a) : X \to X\ (\alpha \mapsto \alpha^a)$ とすると、$\sigma(a)$ は、X 上の全単射である。さらに、

$$\sigma : G \to S^X\ (a \mapsto \sigma(a))$$

は、準同型になる。この σ の核（Kerσ）を Ker(X, G) と書き G の X 上の作用の核という。(確認せよ。)

逆に $\sigma : G \to S^X$ を準同型とすると、$X \times G \to X\ ((\alpha, a) \mapsto \alpha^{\sigma(a)})$ により、X は、G-集合となる。この準同型を G の置換表現という。

注　群 G から、一般線形群 GL$(n, \boldsymbol{C})$ への準同型を線形表現という。G を有限群とすると、必ず線形表現があることが知られているが、以下に見るように、置換表現はいつでも存在し、さらに、核が 1 となる（これを忠実な表現という）置換表現がある。

例 **8.1** $H \leq S^X$ とすると、$\sigma : H \to S^X$ を埋め込みとすると、明らかに置換表現となるから、作用が定義できる。実際、$X \times H \to X,\ ((\alpha, h) \mapsto \alpha^h)$ により、X は、H 集合になる。特に、S_n の部分群は、$\{1, 2, \ldots, n\}$ に自然に作用する。($H \leq S^X$ を X 上の置換群、$H \leq S_n$ を n 次置換群という。)

例 **8.2** $H \leq G$ とする。

$$f : H\backslash G \times G \to H\backslash G,\ ((Hx, a) \mapsto Hxa)$$

により、G は、$H\backslash G$ に作用する。実際、

$$(Hx)^1 = Hx1 = Hx,\ (Hx)^{ab} = Hxab = (Hxa)^b = (Hxa)^b = ((Hx)^a)^b$$

この作用は明らかに可移である。

$$\begin{aligned} \mathrm{Ker}(H\backslash G, G) &= \{a \in G \mid Hxa = Hx \ \text{ for all } x \in G\} \\ &= \bigcap_{x \in G} x^{-x} Hx \lhd G \end{aligned}$$

特に、$H = 1$ のとき、右正則表現という。$\mathrm{Ker}(G, G) = 1$。$\sigma : G \to S^G$ は、単射である。従って、G は、S^G の部分群と同型である。

例 **8.3** $X = G$ とし、

$$G \times G \to G\ ((x, a) \mapsto a^{-1}xa = x^a)$$

とすると、この作用により、G は、G-集合になる。この場合は、

$$G_x = \{a \in G \mid x^a = x = \{a \in G \mid a^{-1}xa = x\} = C_G(x)$$

となる、x^G は、x の共役類となり、定理 8.1 から、

$$|x^G| = |G : C_G(x)|$$

である。特に、共役類の元の数は、$|G|$ の約数である。

$$\mathrm{Ker}(G, G) = \{a \in G \mid x^a = x,\ x \in G \text{ for all } x \in G\} = Z(G) \lhd G$$

また、

$$|x^G| = 1 \Leftrightarrow |G : C_G(a)| = 1 \Leftrightarrow x \in Z(G).$$

9 アーベル群の基本定理

以下で述べる有限生成アーベル群の基本定理は、数学の様々なところで用いられる基本的な定理である。巡回群は、群の中で構造が一番わかりやすいものであるが、巡回群の直積がアーベル群であることは簡単に分かる。基本定理は、生成元の数が有限個のアーベル群は、巡回群の直積であることを主張している。また、この定理によって、有限生成アーベル群の同型類を完全に記述することが出来る。有限生成でないアーベル群については、未解決な問題も多い。

定理 9.1 有限生成のアーベル群 G は、巡回群の直積である。さらに、

$$G = E_1 \times E_2 \times \cdots \times E_m \times I_1 \times I_2 \times \cdots \times I_r,$$

$E_i \simeq \boldsymbol{Z}_{e_i}$、$e_i > 1$、$i = 1, 2, \ldots, m$、$e_i \mid e_{i+1}$、$i = 1, 2, \ldots, m-1$、$I_j \simeq \boldsymbol{Z}$、$j = 1, 2, \ldots, r-1$ となる。この様な直積分解において、$(e_1, e_2, \ldots, e_m; r)$ は、 G により一意的に定まる。(これを不変系という。)

補題 9.2 有限生成のアーベル群 $G =< x_1, x_2, \ldots, x_n >$ の元、$y_1 = x^{a_1}x^{a_2}\cdots x^{a_n}$、$a_i \in \boldsymbol{Z}$、$(i = 1, 2, \ldots, n)$、$(a_1, a_2, \ldots, a_n) = 1$ とすると、$G =< y_1, y_2, \ldots, y_n >$ となる $y_2, \ldots, y_n$ が存在する。

証明　$m = |a_1| + |a_2| + \cdots + |a_n|$ による帰納法で示す。

$m = 1$ とする。これは、ある i について $a_i = \pm 1$ を意味するから $y_1 = x_i^{\pm 1}$ これより、この場合は明らか。

$m > 1$ とする。$(a_1, a_2, \ldots, a_n) = 1$ より $|a_i| \geq |a_j| > 0$ となる a_i, a_j が存在する。このとき、$|a_i - \epsilon a_j| < |a_i|$ となるように、$\epsilon = \pm 1$ を取ることが出来る。すると、

$$y_1 = x_1^{a_1} \cdots x_i^{a_i - \epsilon a_j} \cdots (x_j x_i^{\epsilon})^{a_j} \cdots x_n^{a_n}$$

だから、ここで、$b_k = a_k$ $(k \neq i)$、$b_i = a_i - \epsilon a_j$、$z_l = x_l$、$(l \neq j)$、$z_j = x_j x_i^{\epsilon}$ とおけば、

$$(b_1, b_2, \ldots, b_n) = (a_1, \ldots, a_{i-1}, a_i - \epsilon a_j, a_{i+1}, \ldots, a_n) = (a_1, \ldots, a_n) = 1$$

が成り立ち、かつ、

$$G =< x_1, \ldots, x_n >=< x_1, \ldots, x_{j-1}, x_j x_i^{\epsilon}, x_{j+1}, \ldots, x_n >=< z_1, z_2, \ldots, z_n > .$$

ここで、$y_1 = z_1^{b_1} \cdots z_n^{b_n}$、しかし、$|b_1| + \cdots + |b_n| < m$ だから、帰納法によって $y_2, \ldots, y_n$ で、$G =< y_1, \ldots, y_n >$ となるものが存在する。 ■

Proof of Theorem 9.1　G の元 $x_1, \ldots, x_n$ を次の条件を満たすように取る。

1. $G =< x_1, \ldots, x_n >$ で n は、最小。

2. $G =< x_1, \ldots, x_{i-1}, y_i, \ldots, y_n >$ ならば、x_i の位数は、高々 y_i の位数に等しい。

(x_1 を 1 を満たす、すべて可能な組の中で最小位数に取り、x_{i-1} まで取ったとき、x_i を $x_1, \ldots, x_{i-1}$ を固定したとき、すべて可能な y_i の中で最小位数に取ればよい。)

$< x_i >= E_i$、$|E_i| = e_i$ と置く。(∞ も含める。) このとき、$G = E_1 \times \cdots \times E_n$ かつ、$e_i \mid e_{i+1}$ を示す。

$$\phi : E_1 \times \cdots \times E_n \to G,\ ((x_1^{a_1}, \ldots, x_n^{a_n}) \mapsto x x_1^{a_1} \cdots x_n^{a_n})$$

は、準同型で、かつ条件 1 より、全射である。

$x_i^{a_i} \cdots x_j^{a_j} = 1$ とし、添字は順に大きくなるように取る。ここに現れるものについて、$0 < |a_k| \le e_k$ としてよい。$d = (a_i, \ldots, a_j)$ とし、$a_k = db_k$ と書く。すると、$(b_i, \ldots, b_j) = 1$ である。従って、補題 9.2 により、$y_i = x_i^{b_i} \cdots x_j^{b_j},\ y_{i+1}, \ldots, y_n$ があって、$< x_i, \ldots, x_n >=< y_i, \ldots, y_n >$。$y_i$ の定義により、

$$y_i^d = x_i^{db_i} \cdots x_j^{db_j} = x_i^{a_i} \cdots x_j^{a_j} = 1.$$

従って、y_i の位数は、高々 d。一方、x_i の取り方から、

$$e_i \le o(y_i) \le d \le |a_i| \le e_i.$$

従って、$e_i = d = |a_i|$。すなわち $x_i^{a_i} = 1$。従って、ϕ は、同型である事がわかる。さらに、$x_i^{e_i} x_{i+1}^{e_{i+1}} = 1$ だから、$d = (e_i, e_{i+1})$ とすると、上で示したことより、$e_i = d$ である。従って、$e_i \mid e_{i+1}$。$e_1, \ldots, e_m$ が、有限で e_{m+1} からさきが、無限なら、

$$G = E_1 \times \cdots \times E_m \times I_1 \times \cdots \times I_r$$

$E_i \simeq \boldsymbol{Z}_{e_i}$、$I_j \simeq \boldsymbol{Z}$、$e_i \mid e_{i+1}$、$1 < e_i$ が得られる。

(一意性)

$$\begin{aligned} G &= E_1 \times \cdots \times E_m \times I_1 \times \cdots \times I_r \\ &= E'_1 \times \cdots \times E'_{m'} \times I'_1 \times \cdots \times I'_{r'} \end{aligned}$$

$E_i =< x_i >$、$I_j =< z_j >$、$I'_j =< w_j >$、$E'_i =< y_i >$、$e_i = |E_i|$、$e'_i = |E'_i|$ とする。$T(G)$ を G の位数が有限なもの全体とする。すると、

$$T(G) = E_1 \times \cdots \times E_m = E'_1 \times \cdots \times E'_m$$

p を e_1 の一つの素因子とし、p は、e'_{i+1} 以降を割り切るとする。すると、

$$T(G)_p = \{x \in T(G) \mid x^p = 1\} =< x_1^{e_1/p}, \ldots, x_m^{e_m/p} >=< y_{i+1}^{e'_{i+1}/p}, \ldots, y_{m'}^{e'_{m'}/p} >$$

だから、位数を考えると、$|T(G)_p| = p^m = p^{m'-i}$ となり、$m \le m'$ を得る。同様にして、$m' \le m$ を得るから、$m = m'$、$p \mid e'_1$ を得る。ここで、

$$T(G)^p = \{x^p \mid x \in T(G)\} =< x_1^p, \ldots, x_m^p >=< y_1^p, \ldots, y_m^p >$$

だから、それぞれの、直積因子の位数は、$e_1/p, \ldots, e_m/p$ および、$e'_1/p, \ldots, e'_m/p$ となり、数学的帰納法により、これらは、等しくなる。従って、$e_i = e'_i$ を得る。

ここでさらに、$e = e_m$ として、

$$G^e = \{x^e \mid x \in G\} =< z_1^e, \ldots, z_r^e >=< w_1^e, \ldots, w_{r'}^e >$$

$$G^{2e} = \{x^{2e} \mid x \in G\} =< z_1^{2e}, \ldots, z_r^{2e} >=< w_1^{2e}, \ldots, w_{r'}^{2e} >$$

だから、G^e/G^{2e} の位数を考えると、$2^r = 2^{r'}$ を得るから、$r = r'$ となる。 ■

例 9.1 G を 位数 12 のアーベル群とする。$12 = e_1 e_2 \cdots e_r$、$e_1 \mid e_2$, $e_2 \mid e_3 \ldots e_{r-1} \mid e_r$ だから、$e^r \mid 12$。これらは、$(12), (2, 6)$ のいずれかしかないことが分かる。すなわち、G は、$\boldsymbol{Z}_{12}$（位数 12 の巡回群）又は、$\boldsymbol{Z}_2 \times \boldsymbol{Z}_6$ のいずれかに同型であることが分かる。

10　シローの定理

この節では、G は、有限群を表すものとする。

定義 10.1 p を素数とするとき、G が p–群であるとは、$|G|$ が p–べき ($|G| = p^r$) であることである。$|G| = p^n g'$, $(p, g') = 1$ としたとき（p^n を $|G|$ を割り切る最大べき）P が G のシロー p-部分群 (Sylow-p-group) であるとは、$P \leq G$ かつ、$|P| = p^n$。

ここでまず問題となるのは、以下の事である。

1. 任意の有限群と任意の素数 p について、シロー p–部分群は存在するか。
2. シロー p–部分群について何が言えるか。複数個の シロー p–部分群があったとき、それらは、同型だろうか、共役だろうか、いくつあるだろうか。

二つの補題を準備する。

補題 10.1 p を素数とし、G は、その位数 $|G|$ が p で割り切れるアーベル群とする。このとき、G に位数 p の元が存在する。

証明　定理 9.1 より明らか。 ■

補題 10.2 $G \neq 1$ とし、G の任意の真部分群に対して、$p \mid |G : H|$ が成り立つとする。このとき、$p \mid |Z(G)|$ である。特に、$Z(G) \neq 1$。

証明　Exercise 8.2 参照。 ■

定理 10.3 ある素数 p に対して、$p^r \mid |G|$ ならば G に位数 p^r の部分群が存在する。特に、G のシロー p–部分群が存在する。

証明　G の位数に関する帰納法で証明する。明らかに、$G \neq 1$ としてよい。

Case 1.　G の真部分群 H で、$(|G : H|, p) = 1$ となるものが存在するとき。

このときは、$p^r \mid |G| = |G : H||H|$ だから、$p^r \mid |H|$ である。従って、帰納法の仮定より、H の部分群 P で、位数が p^r のものが存在する。$P \leq G$ だから、定理の主張が成り立つ。

Case 2.　G の任意の真部分群に対して $p \mid |G : H|$ が成立するとき。

このときは、補題 10.2 により $p \mid |Z(G)|$ である。$Z(G)$ は、アーベル群だから、補題 10.1 より、$Z(G)$ に位数 p の元 x があることが分かる。$A =< x >$ とする。$|A| = |< x >| = o(x) = p$。$A \leq Z(G)$ だから、$A \triangleleft G$。剰余群 G/A を考えると、

$$p^r \mid |G| = |G : A||A| = p|G/A|$$

だから、$p^{r-1} \mid |G/A|$ となる。従って、帰納法の仮定により、G/A は、位数が、p^{r-1} の部分群 P_1 を持つ。$\pi : G \to G/A$ を自然な準同型とし、$P = \pi^{-1}(P_1)$ とすると、$A \leq P$ だから、$P/A \simeq P_1$、従って、$|P| = p^r$ を得る。 ■

$\mathrm{Syl}_p(G)$ によって、G のシロー p–部分群全体を表すものとする。

定理 10.4 G を有限群、p を素数とする。

(1) H を G の p–部分群とすると、G の p–シロー部分群 P で H を含むものが存在する。

(2) P, Q を G のシロー p–部分群とすると、$Q = g^{-1}Pg$ となる G の元 g が存在する。

(3) $|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$、すなわち、シロー p–部分群の個数は、$kp+1$、$(k \in \boldsymbol{Z})$ と書ける。

証明　(1) $P \in \mathrm{Syl}_p(G)$、H を G の p–部分群とする。(P, H) による G の両側分解を

$$G = Pa_1H + Pa_2H + \cdots + Pa_rH$$

とすると、命題 3.5 によって、

$$|G : P| = \sum_{i=1}^{r} |H : H \cap a_i^{-1}Pa_i|$$

が成り立つ。P は、G のシロー p–部分群だから、左辺は p と素である。従って、右辺のある項は、p と互いに素であることが分かる。$(|H : H \cap a_i^{-1}Pa_i|, p) = 1$ とする。H は、p 群だから、

$$|H| = |H : H \cap a_i^{-1}Pa_i||H \cap a_i^{-1}Pa_i|$$

を考えると、$|H : H \cap a_i^{-1}Pa_i| = 1$ すなわち $H = H \cap a_i^{-1}Pa_i$ である。従って、$H \subset a_i^{-1}Pa_i$ である。$a_i^{-1}Pa_i$ は、P と同じ位数の G の部分群だから $a_i^{-1}Pa_i$ は、G の シロー p–部分群、従って、H を含む G のシロー p–部分群が存在する。

(2) $Q = H$ と置くと、(1) の証明より G の元 $g = a_i$ によって、$Q \subset g^{-1}Pg$ となる。$|Q| = |P| = |g^{-1}Pg|$ だから、$Q = g^{-1}Pg$ が成り立つ。

(3) $\mathrm{Syl}_p(G) \times G \to \mathrm{Syl}_p(G)$, $((P, a) \mapsto a^{-1}Pa)$ とすると ($a^{-1}Pa \in \mathrm{Syl}_p(G)$ に注意)、$\mathrm{Syl}_p(G)$ は、G-集合となり、(2) により、この作用は可移である。この作用に関する $P \in \mathrm{Syl}_p(G)$ の安定部分群を、N とすると、

$$N = \{a \in G \mid P^a = P\} = \{a \in G \mid a^{-1}Pa = P\} = N_G(P)$$

である。定理 8.1 により、

$$|\mathrm{Syl}_p(G) = P^G = |G : N| = |G : N_G(P)|$$

となる。ここで、G の (N, P) による両側分解を

$$G = Nb_1P + Nb_2P + \cdots + Nb_rP$$

ただし、$b_1 = 1$ とする。命題 3.5 によって

$$|G : N| = \sum_{i=1}^{r} |P : P \cap b_i^{-1}Nb_i|$$

となる。$P \subset N_G(P) = N$ だから、$|G:N| \mid |G:P|$ で、$|G:N|$ は、p と互いに素である。従って、右辺にも p と互いに素な項があることになるが、

$$\begin{aligned} |P : P \cap b_i^{-1} N b_i| = 1 \;\; &\Leftrightarrow \;\; P = P \cap b_i^{-1} N b_i \;\Leftrightarrow\; P \subset b_i^{-1} N b_i \\ &\Leftrightarrow \;\; b_i P b_i^{-1} \subset N \;\; \text{すなわち} \; b_i P b_i^{-1} \in \mathrm{Syl}_p(N) \\ &\Leftrightarrow \;\; b_i P b_i^{-1} = n^{-1} P n = P \;\; \text{となる} \; n \in N \;\; \text{が存在する。} \\ &\Leftrightarrow \;\; b_i \in N = N_G(P) \\ &\Leftrightarrow \;\; N b_i P = N 1 P (= N) \\ &\Leftrightarrow \;\; b_i = b_1 \end{aligned}$$

すなわち、この様な b_i は、ただ一つであり、他の $|P : P \cap b_i^{-1} N b_i|$ は、すべて p で割り切れる。$|P : P \cap b_1^{-1} N b_1| = |P : P \cap N| = |P : P| = 1$ だから、

$$|\mathrm{Syl}_p(G)| = |G : N_G(P)| = kp + 1$$

と書ける。 ■