群論

花木 章秀

2011 年度後期 (2011/02/08)

目次

1 群の定義と例 **7**
- 1.1 群の定義 . . . 7
- 1.2 部分群 . . . 8
- 1.3 剰余類分解 . . . 9
- 1.4 正規部分群 . . . 10
- 1.5 両側剰余類 . . . 11
- 1.6 剰余群 . . . 12
- 1.7 生成系と基本関係 . . . 12
  - 1.7.1 自由群 . . . 12
  - 1.7.2 生成系と基本関係 . . . 13
- 1.8 群の例 . . . 14
  - 1.8.1 行列群 . . . 14
  - 1.8.2 置換群 . . . 15
- 1.9 モノイドの単元群 . . . 17

2 準同型定理と同型定理 **19**
- 2.1 群準同型 . . . 19
- 2.2 準同型定理 . . . 22
- 2.3 同型定理 . . . 23
- 2.4 自己同型 . . . 24

3 群の作用 **27**
- 3.1 群の作用 . . . 27
- 3.2 安定化部分群と軌道 . . . 29
- 3.3 群の左剰余類への作用 . . . 30
- 3.4 共役による作用 . . . 31

4 シローの定理 **35**
- 4.1 シローの定理 . . . 35

5 群の直積 **39**
- 5.1 外部直積 . . . 39
- 5.2 内部直積 . . . 40

6 有限生成アーベル群 **43**
6.1 有限アーベル群 43
6.2 有限生成アーベル群 45
6.2.1 有限生成自由アーベル群 46
6.2.2 トーション部分群 47
6.2.3 有限生成アーベル群の基本定理 48

はじめに

普通の数、ベクトル、行列、多項式、など加法を考えることが出来るものはたくさんある。これらの計算に関する公式も色々と考えられるが、同じ加法に関する公式であっても、考える “もの” が違えば証明も違うはずで、それぞれに対して証明を行わなくてはならない。そこで加法の基本的な性質のみを抽出して、そこから得られる結果だけを考えたならば、それはどの対象に対しても正しいはずである。

このような考えで、抽象的な集合と演算を考え、その演算がある条件をみたすものを考えるというのが現代代数学の基本的な考えである。ここでは代数の主要な研究対象のうち、最も基本的なものの一つである「群」について学ぶ。群は一つの演算をもち、それがある種の性質をみたすものとして定義される。

このテキストでは、群の基本事項については簡単に解説し、

- 準同型定理と同型定理
- シローの定理
- 有限生成アーベル群の基本定理

を理解することを目的とする。

Chapter 1

群の定義と例

1.1 群の定義

集合 A に対して、写像 $f : A \times A \to A$ を A の**二項演算**という。像 $f(a, b)$ を ab や $a+b$ とな ど表す。

二項演算 $(a, b) \to ab$ が**結合法則**をみたすとは、任意の $a, b, c \in A$ に対して

$$(ab)c = a(bc)$$

が成り立つことである。結合法則をみたす二項演算が定義された集合を**半群**という。

半群 A の元 e が A の**単位元**であるとは、任意の $a \in A$ に対して

$$ae = ea = a$$

が成り立つことである。単位元は存在すれば一意的である。半群 A の単位元を 1_A、または単に 1 とも表す。(演算が加法的に $(a, b) \to a + b$ と書かれている場合には、単位元を 0_A、または 0 と表す。) 単位元をもつ半群を**モノイド**という。

モノイド A の元 a に対して

$$ab = ba = 1_A$$

となる元 b が存在するとき a を A の**正則元**、**単元**、または**単数**などという。このとき b を a の**逆元**という。正則元の逆元は一意的に定まる。これを a^{-1} と表す。(演算が加法的に $(a, b) \to a + b$ と書かれている場合には、逆元を $-a$ と表す。) モノイド A のすべての元が正則元であるとき A を**群**という。

二項演算 $(a, b) \to ab$ が**交換法則**をみたすとは、任意の $a, b \in A$ に対して

$$ab = ba$$

が成り立つことである。通常は、加法的な表記 $(a, b) \to a + b$ は交換法則が成り立つときにしか用いない。交換法則をみたす演算をもつ半群、モノイド、群を、それぞれ**可換半群**、**可換モノイド**、**可換群**という。特に可換群は**アーベル群**と呼ばれることが多い。

群の演算が加法を用いて表されるときには**加法群**ともよぶ。加法群はアーベル群であるものとする。

群 A の集合としての要素の数 (濃度) を A の**位数**といい $|A|$ と表す。特に A が有限集合であるとき A を**有限群**と呼び、そうでないとき**無限群**と呼ぶ。

問 1.1.1. 群 G の元 a, b, a_i に対して、次のことを示せ。

(1) $(a^{-1})^{-1} = a$ である。

(2) $(ab)^{-1} = b^{-1}a^{-1}$ である。より一般に $(a_1 \cdots a_\ell)^{-1} = {a_\ell}^{-1} \cdots {a_1}^{-1}$ である。

1.2 部分群

G を群とする。G の空でない部分集合 H が G の演算でまた群となるとき、H を G の**部分群**という。H が部分群であるための条件は、次のように言い換えることが出来る。

(1) $x, y \in H$ ならば $xy \in H$ である。$x \in H$ ならば $x^{-1} \in H$ である。

またこの二つの条件をまとめて

(2) $x, y \in H$ ならば $xy^{-1} \in H$ である。

あるいは

(3) $x, y \in H$ ならば $x^{-1}y \in H$ である。

と書くことも出来る。

例 1.2.1. G を群とすると G 自身は G の部分群である。また、単位元のみからなる集合 $\{1_G\}$ も G の部分群である。この二つを G の**自明な部分群**という。$\{1_G\}$ を単に 1 とも表す。

H が G の部分群であることを $H \leq G$ と表すことにする。$H < G$ は $H \leq G$ かつ $H \neq G$ を意味するものとする。

A, B を群 G の部分集合とするとき

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

と定める。このとき $A(BC) = (AB)C$, $(AB)^{-1} = B^{-1}A^{-1}$ などが成り立つ。この記号を用いると部分群であるための条件は以下のように書き換えることが出来る。

(4) $HH \subset H$, $H^{-1} \subset H$

(5) $HH^{-1} \subset H$

(6) $H^{-1}H \subset H$

H が G の部分群であるならば

$$H = HH = H^{-1} = HH^{-1} = H^{-1}H$$

が成り立っている。

この表記で $A = \{a\}$ のとき $\{a\}B$ を aB と書く。Ab も同様である。すなわち

$$aB = \{ab \mid b \in B\}, \quad Ab = \{ab \mid a \in A\}$$

である。

問 1.2.2. H, K が群 G の部分群ならば、$H \cap K$ も G の部分群であることを示せ。より一般に $\{H_\lambda \mid \lambda \in \Lambda\}$ が G の部分群の族とするとき $\bigcap_{\lambda\in\Lambda} H_\lambda$ は G の部分群であることを示せ。

群 G に対して

$$Z(G) = \{g \in G \mid \text{任意の } x \in G \text{ に対して } xg = gx\}$$

とおいて、これを G の**中心** (center) という。G がアーベル群ならば $Z(G) = G$ である。

問 1.2.3. 群 G の中心 $Z(G)$ は G の部分群であることを示せ。

G を群とする。$S \subset G$ に対して S を含む部分群の全体を考え、その共通部分をとれば、それは G の S を含む最小の部分群となる。これを S で**生成される部分群**といい $\langle S\rangle$ と表す。$S = \{s_1, \cdots, s_\ell\}$ の場合には、これを $\langle s_1, \cdots, s_\ell\rangle$ とも表す。

問 1.2.4. 群 G の二つの部分群 H, K について、HK が G の部分群になることと $HK = KH$ が成り立つことは同値であることを示せ。

1.3 剰余類分解

G を群、H をその部分群とする。$a, b \in G$ に対して $a^{-1}b \in H$ であるときに $a \sim b$ として G 上の関係 $\sim$ を定める。このとき $\sim$ は同値関係となる。この同値関係による $a \in G$ を含む同値類は

$$aH = \{ah \mid h \in H\}$$

であることがすぐに分かる。これを G の H による a を含む**左剰余類** (left coset) という。左剰余類全体の集合を G/H と表す。異なる左剰余類の全体を $\{a_\lambda H \mid \lambda \in \Lambda\}$ とすると、この同値関係による類別は

$$G = \bigcup_{\lambda\in\Lambda} a_\lambda H$$

となる。これを G の H による**左剰余類分解**という。記号の乱用を許し、G/H をこの類別の完全代表系を表すものとして、左剰余類分解を

$$G = \bigcup_{a\in G/H} aH$$

のように表すこともある。G の H による異なる左剰余類の個数 (濃度) を $|G : H|$ と表し H の G における**指数** (index) という。すぐに分かるように、任意の $a \in G$ に対して $|aH| = |H|$ が成り立つ。したがって G が有限群ならば次の定理が成り立つ。

定理 1.3.1 (ラグランジェ)**.** G を有限群、H をその部分群とするとき

$$|G| = |G : H| \cdot |H|$$

が成り立つ。特に H の位数と指数は G の位数の約数である。

群 G の元 a に対して $a^n = 1$ となる自然数 n が存在するとき、そのような n のうち最小のものを a の**位数**といい $o(a)$ で表す。このとき

$$\langle a \rangle = \{1, a, a^2, \cdots, a^{o(a)-1}\}$$

は G の部分群で、したがって $o(a)$ は $|G|$ の約数である。$\langle a \rangle$ を a **の生成する巡回部分群**という。

関係 $\sim_r$ を $ab^{-1} \in H$ のときに $a \sim_r b$ で定めれば、これは上と同様に同値関係となる。この同値関係による同値類は

$$Ha = \{ha \mid h \in H\}$$

となる。これを G の H による a を含む**右剰余類**という。右剰余類全体の集合を $H \backslash G$ と表す。**右剰余類分解**も同様に定義される。

$\{a_\lambda \mid \lambda \in \Lambda\}$ を G の H による左剰余類分解の完全代表系とすると $\{{a_\lambda}^{-1} \mid \lambda \in \Lambda\}$ は右剰余類分解の完全代表系となる。したがって左剰余類の個数 (濃度) と右剰余類の個数 (濃度) は一致する。

1.4 正規部分群

任意の $a \in G$ に対して、それを含む左剰余類と右剰余類が一致するとき、すなわち

$$aH = Ha$$

が成り立つとき、H を G の**正規部分群** (normal subgroup) といい $H \trianglelefteq G$ と表す。$H \triangleleft G$ は $H \trianglelefteq G$ かつ $H \neq G$ を意味するものとする。H が正規部分群であるときには、その左剰余類と右剰余類は一致するので区別の必要がなく、単に**剰余類** (coset) といわれる。

任意の群 G について、1 と G は G の正規部分群である。

群 G がアーベル群ならば、そのすべての部分群は正規部分群である。

命題 1.4.1. 群 G の部分群 H に対して、以下の条件は同値である。

(1) $H \trianglelefteq G$ (すなわち、任意の $g \in G$ に対して $gH = Hg$)

(2) $h \in H$, $g \in G$ ならば $ghg^{-1} \in H$

(3) 任意の $g \in G$ に対して $gHg^{-1} \subset H$

(4) 任意の $g \in G$ に対して $gHg^{-1} = H$

証明. (1) $\Longrightarrow$ (2). $h \in H$, $g \in G$ とする。$gH = Hg$ である。$gh \in gH = Hg$ なので、ある $h' \in H$ があって $gh = h'g$ となる。よって $ghg^{-1} = h' \in H$ である。

(2) $\Longrightarrow$ (1). $g \in G$ として $gH = Hg$ と示す。$x \in gH$ とする。ある $h \in H$ があって $x = gh$ である。条件より $ghg^{-1} \in H$ であるから

$$x = gh = (ghg^{-1})g \in Hg$$

となる。よって $gH \subset Hg$ である。$y \in Hg$ とする。ある $h \in H$ があって $y = hg$ である。条件より $g^{-1}hg = g^{-1}h(g^{-1})^{-1} \in H$ であるから

$$y = hg = g(g^{-1}hg) \in gH$$

となる。よって $Hg \subset gH$ である。したがって $gH = Hg$ となる。

(2) と (3) は記号の違いだけである。

(4) $\Longrightarrow$ (3) は明らか。

(3) $\Longrightarrow$ (4) を示す。$g \in G$ とする。$gHg^{-1} \subset H$ である。また $g^{-1} \in G$ に (3) の条件を適用すれば $g^{-1}Hg \subset H$ である。両辺に、左から g、右から g^{-1} をかければ $H \subset gHg^{-1}$ である。よって (4) が成り立つ。 □

問 1.4.2. H, K が群 G の正規部分群ならば、$H \cap K$ も G の正規部分群であることを示せ。より一般に $\{H_\lambda \mid \lambda \in \Lambda\}$ が G の正規部分群の族とするとき $\bigcap_{\lambda\in\Lambda} H_\lambda$ は G の正規部分群であることを示せ。

問 1.4.3. H が G の部分群で N が G の正規部分群ならば HN は G の部分群であることを示せ。また H, K が群 G の正規部分群ならば、HK も G の正規部分群であることを示せ。

問 1.4.4. H が G の部分群で N が G の正規部分群ならば $H \cap N$ は H の正規部分群であることを示せ.

1.5 両側剰余類

G を群とし H, K をそれぞれ G の部分群とする。$a, b \in G$ に対して $a \approx b$ を $HaK = HbK$ となることで定める。ただし $HaK = \{hak \mid h \in H,\ k \in K\}$ である。このとき $\approx$ は同値関係となる。この同値関係による a を含む同値類は HaK となる。これを G の (H, K) による**両側剰余類** (double coset) という。両側剰余類の全体の集合を $H \setminus G/K$ と表す。左剰余類の場合と同様に**両側剰余類分解**を

$$G = \bigcup_{a\in H\setminus G/K} HaK$$

のようにも表す。$HaK = \bigcup_{h\in H} haK$ であるから、両側剰余類 HaK は K によるいくつかの左剰余類の和集合である。同様に HaK は H によるいくつかの右剰余類の和集合である。

命題 1.5.1. G を有限群、H, K をその部分群とする。また $a \in G$ とする。このとき HaK は $|H : H \cap aKa^{-1}|$ 個の K による左剰余類の和集合である。特に $|HaK| = |H : H \cap aKa^{-1}| \cdot |K|$ である。

証明. $f : H/(H \cap aKa^{-1}) \to \{haK \mid h \in H\}$ を $f(h(H \cap aKa^{-1})) = haK$ で定め、これが全単射になることを示す。

まず写像が矛盾なく定義されることを見る。$h(H \cap aKa^{-1}) = h'(H \cap aKa^{-1})$ とする。ある $k \in K$ があって $h' = h(aka^{-1})$ である。このとき $h'aK = h(aka^{-1})aK = haK$ である。よって f は矛盾なく定義される。

f が全射であることは定義から明らかである。f が単射であることを示す。$haK = h'aK, h, h' \in H$ とする。このとき $a^{-1}(h')^{-1}ha \in K, (h')^{-1}h \in H \cap aKa^{-1}$ である。よって $h(H \cap aKa^{-1}) = h'(H \cap aKa^{-1})$ となり f は単射である。 □

H が G の正規部分群ならば、両側剰余類 HaK について $HaK = aHK$ が成り立ち、よってこれは部分群 HK による左剰余類と一致する。

1.6 剰余群

G を群とし H をその部分群とする。このとき、一般には、左剰余類の集合 G/H に自然な方法で群の構造を考えることは出来ない。しかし H が正規部分群ならば以下のようにして G/H は群となる。

$H \trianglelefteq G$ とする。G/H に以下のように積を定義する。

$$(aH)(bH) = (ab)H$$

このとき、この積が矛盾なく定義され、結合法則をみたし、$H = 1H$ が単位元、$a^{-1}H$ が aH の逆元となり、G/H は群となる。これを G の H による**剰余群** (factor group) という。

$N \leq H \leq G$ とし $N \trianglelefteq G$ とする。このとき剰余群 G/N が定義されるが

$$H/N = \{hN \mid h \in H\}$$

とおくと、これは G/N の部分群となる。実際、$h, h' \in H$ に対して

$$(hN)(h'N)^{-1} = (hN)((h')^{-1}N) = (h(h')^{-1})N \in H/N$$

である。一方で、$N \trianglelefteq H$ と見ることも出来るので、この意味での剰余群 H/N も定義される。どちらの意味で H/N を考えても、演算は同じなので本質的な違いはない。

1.7 生成系と基本関係

1.7.1 自由群

X を集合とする。$x \in X$ に対して、形式的に x^{-1} というものを考え $X^{-1} = \{x^{-1} \mid x \in X\}$ とおく。$(x^{-1})^{-1} = x$ と考えることにする。$X \cup X^{-1}$ の要素を有限個並べたものを**語** (word) という。二つの語は xx^{-1} を語の途中に加えたり、除いたりすることで移り合うときに同じものと考えることにする。また $X \cup X^{-1}$ の要素を 0 個並べることも形式的に許すこととし、これを 1 と表す。このとき語の全体の集合は、語をつなぐことを演算として 1 を単位元とする群となる。これを X で生成される**自由群** (free group) といい $F(X)$ と表すことにする。

例 1.7.1 (無限巡回群)**.** $X = \{a\}$ のとき、$F(X) = \{a^i \mid i \in \mathbb{Z}\}$ である。これを**無限巡回群**という。無限巡回群はアーベル群で、加法群としては $\mathbb{Z}$ と本質的に同じものである。

1.7.2 生成系と基本関係

X を集合とし $F(X)$ を自由群とする。$R \subset F(X)$ とし、R を含む $F(X)$ の最小の正規部分群を N とする。実際 R を含む正規部分群全体の集合は $F(X)$ を含むので空ではなく、そのすべての共通部分をとれば、それが N となるので、そのような N は存在する。このとき剰余群 $F(X)/N$ が考えられる。この群を

$$\langle X \mid R \rangle$$

と書き、X をその**生成系**、R を**基本関係式**という。これは、自由群 $F(X)$ の元で R に含まれるものを 1 と思うことに相当する。このため $\langle X \mid R \rangle$ という表記で、R の要素 r に対して $r = 1$ のような表記をする場合が多い。以下に簡単な例を示す。

例 1.7.2 (有限巡回群)**.** $\langle a \mid a^n = 1 \rangle$ を位数 n の (有限) **巡回群**という。(無限巡回群と有限巡回群をあわせて、単に**巡回群** (cyclic group) という。) 位数 n の巡回群を C_n という記号で表す。

$$C_n = \{1, a, a^2, \cdots, a^{n-1}\}$$

である。加法群としては $\mathbb{Z}$ の n を法とする剰余類のなす群 $\mathbb{Z}/n\mathbb{Z}$ と本質的に同じものである。

例 1.7.3 (二面体群)**.** $\langle x, y \mid x^n = y^2 = 1,\ yx = x^{n-1}y \rangle$ を位数 $2n$ の**二面体群** (dihedral group) という。位数 $2n$ の二面体群を D_{2n} という記号で表す。

$$D_{2n} = \{1, x, x^2, \cdots, x^{n-1}, y, xy, x^2y, \cdots, x^{n-1}y\}$$

である。

生成系と基本関係式が与えられても、それがどのような群になるかを決めることは一般には難しい。

巡回群に関する基本的な性質はよく用いられるので、簡単にまとめておく。

命題 1.7.4. $G = \langle a \mid a^n = 1 \rangle$ とする。

(1) $a^m = 1$ となる必要十分条件は $n \mid m$ である。

(2) $o(a^m) = n/\gcd(m, n)$ である。特に $\gcd(m, n) = 1$ とすると $o(a^m) = o(a)$ であり、$\langle a^m \rangle = \langle a \rangle$ である。

証明. (1) は簡単なので省略する。演習問題として各自で確認しておくとよいであろう。

(2) $d = \gcd(m, n)$ とし $m = dm'$, $n = dn'$ と書く。このとき $(a^m)^{n'} = a^{m'n} = 1$ であるから $o(a^m) \mid n'$ である。特に $|\langle a^m \rangle| = o(a^m) \leq n'$ である。

最大公約数に関する定理より、ある整数 x, y が存在して $xm + yn = d$ となる。したがって

$$a^d = a^{xm+yn} = (a^m)^x (a^n)^y = (a^m)^x \in \langle a^m \rangle$$

である。よって $\langle a^d \rangle \subset \langle a^m \rangle$ である。ここで $o(a^d) = n'$ はすぐに分かるので

$$n' = |\langle a^d \rangle| \leq |\langle a^m \rangle| = o(a^m)$$

となる。したがって $o(a^m) = |\langle a^m \rangle| = n' = n/d$ である。 □

問 1.7.5. G を位数 n の有限巡回群とするとき、$d \mid n$ に対して $\sharp\{x \in G \mid x^d = 1\} = d$ であることを示せ。

問 1.7.6. $N \trianglelefteq G$ とし $g \in G$ とする。このとき剰余群 G/N における gN の位数 $o(gN)$ は $o(g)$ の約数であることを示せ。

1.8 群の例

1.8.1 行列群

ここでは行列の集合として表されるいくつかの群を定義する。体 K 上 n 次正方行列全体の集合を $M_n(K)$ と表す。$M_n(K)$ は乗法に関して単位行列を単位元とするモノイドであるが群ではない。(加法も考えれば $M_n(K)$ は環であり、K **上** n **次全行列環**と呼ばれる。)

例 1.8.1 (一般線型群 $GL_n(K)$)**.** K を体とする。K を成分とする n 次正方行列が逆行列をもつとき、それを**正則行列**という。ある行列が正則であるための必要十分条件は、その行列式の値が 0 でないことである。K を成分とする n 次正則行列の全体は行列の積によって群をなす。これを K **上** n **次一般線型群** (general linear group) といい $GL_n(K)$ と表す。

特に K が q 個の元をもつ有限体 $\mathbb{F}_q$ であるとき $\mathbb{F}_q$ は同型を除いて一意的に定まるので、$GL_n(K)$ を $GL_n(q)$ とも書く。

問 1.8.2. $GL_2(2)$ の元をすべて書け。ただし $\mathbb{F}_2 = \{0, 1\}$ と表すことにする。

問 1.8.3. $GL_n(q)$ の位数を求めよ。

例 1.8.4 (特殊線型群 $SL_n(K)$)**.** K 上 n 次正則行列のうち、その行列式の値が 1 であるものの全体は、積と逆元で閉じていて、したがって $GL_n(K)$ の部分群となる。これを K **上** n **次特殊線型群** (special linear group) といい $SL_n(K)$ と表す。

一般線型群と同じように $SL_n(\mathbb{F}_q)$ を $SL_n(q)$ とも表す。

問 1.8.5. $SL_2(3)$ の元をすべて書け。ただし $\mathbb{F}_2 = \{0, 1, 2\}$ と表すことにする。

例 1.8.6 (直交群 $O(n)$)**.** $T \in M_n(\mathbb{R})$ が**直交行列** (orthogonal matrix) であるとは、${}^tTT = T{}^tT = E$ (E は単位行列)、すなわち ${}^tT = T^{-1}$ をみたすことである。n 次直交行列全体の集合は積と逆行列で閉じていて $GL_n(\mathbb{R})$ の部分群となる。これを n **次直交群** (orthogonal group) といい $O(n)$ で表す。

問 1.8.7. $O(n)$ が $GL_n(\mathbb{R})$ の部分群であることを確認せよ.

例 1.8.8 (ユニタリー群 $U(n)$)**.** $U \in M_n(\mathbb{C})$ が**ユニタリー行列** (unitary matrix) であるとは、$U^*U = UU^* = E$、すなわち $U^* = U^{-1}$ をみたすことである。ただし $U^* = {}^t\overline{U}$ である。n 次ユニタリー行列全体の集合は積と逆行列で閉じていて $GL_n(\mathbb{C})$ の部分群となる。これを n **次ユニタリー群** (unitary group) といい $U(n)$ で表す。

問 1.8.9. $U(n)$ が $GL_n(\mathbb{C})$ の部分群であることを確認せよ.

1.8.2 置換群

X を集合とする。X から X への全単射全体の集合は写像の結合を演算として、恒等写像を単位元、逆写像を逆元とする群となる。これを X 上の**対称群**といい $\mathrm{Sym}(X)$ と表す。$\mathrm{Sym}(X)$ の元、すなわち X から X への全単射を X 上の**置換**という。置換 σ は

$$\sigma = \begin{pmatrix} x \\ \sigma(x) \end{pmatrix}$$

のように表される。対称群の単位元は恒等写像であり、これを**恒等置換**ともいう。

特に $|X| = n < \infty$ のとき、$X = \{1, 2, \cdots, n\}$ と考えても本質的には変わらない。この場合、$\mathrm{Sym}(X)$ を S_n と表し、n **次対称群**という。S_n の元を n **次の置換**という。n 次の置換を具体的に書くには、1 行目に $1, 2, \cdots, n$ を書き、その下に元の移る先を書く。例えば

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

のようになる。置換の積は写像の結合なので、

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

のようになる。逆元は、置換の 1 行目と 2 行目を入れ替えて得られる。

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

この際、単に入れ替えただけだと 1 行目の並びが崩れるので、列毎に入れ替えて見やすくする。

置換 σ が、すべて異なる $a_1, a_2, \cdots, a_\ell$ を

$$a_1 \overset{\sigma}{\longmapsto} a_2 \overset{\sigma}{\longmapsto} a_3 \overset{\sigma}{\longmapsto} \cdots \overset{\sigma}{\longmapsto} a_\ell \overset{\sigma}{\longmapsto} a_1$$

のように順に移し、それ以外の元を動かさないとき、これを**巡回置換**、または**サイクル**といい $(a_1\ a_2\ \cdots\ a_{\ell-1}\ a_\ell)$ と表す。(見やすくするために $(a_1, a_2, \cdots, a_{\ell-1}, a_\ell)$ と表すこともある。) このときの ℓ を巡回置換の**長さ**という。すぐに分かるように長さ ℓ の巡回置換の位数は ℓ である。特に長さ 2 の巡回置換を**互換**という。長さ 1 の巡回置換は恒等置換であり、省略されたり ( ) と表されたりする。例えば

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3), \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1\ 2)$$

である。

以下の定理は証明を省略するが、問を見れば雰囲気は分かるであろう。

定理 1.8.10. 任意の n 次の置換は、共通の数字を含まないいくつかの巡回置換の積に分解することが出来る。

問 1.8.11. 置換 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 5 & 8 & 1 & 2 & 7 & 9 & 4 \end{pmatrix}$ を共通の数字を含まないいくつかの巡回置換の積に分解せよ。

定理 1.8.12. 任意の n 次の置換はいくつかの互換の積として表すことが出来る。

問 1.8.13. 巡回置換 $(1\ 2\ \cdots\ \ell) = (1\ \ell)(1\ \ell-1)\cdots(1\ 3)(1\ 2)$ を示せ。

置換 σ を共通の数字を含まないいくつかの巡回置換の積に分解するとき、その分解は積の順序を除いて一意的であり、その巡回置換の長さの (重複度を含む) 集合が決まる。これを σ の**型**といい

$$[\ell_1, \ell_2, \cdots, \ell_r], \quad \ell_1 \geq \ell_2 \geq \cdots, \ell_r \geq 1$$

のように表す。$\ell_i = 1$ なる ℓ_i を省略することもある。例えば

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix} = (1\ 2\ 3)(4\ 5)(6)$$

の型は $[3, 2, 1]$ (または $[3, 2]$) と表される。

定理 1.8.14. 置換 σ の型が $[\ell_1, \ell_2, \cdots, \ell_r]$ であるとき σ の位数 $o(\sigma)$ は $\ell_1, \ell_2, \cdots, \ell_r$ の最小公倍数である。

定理 1.8.15. (1) 置換 σ, τ について、σ と $\tau\sigma\tau^{-1}$ は同じ型をもつ。

(2) 置換 σ と σ' が同じ型をもつならば、ある置換 τ が存在して $\sigma' = \tau\sigma\tau^{-1}$ となる。

与えられた n 次の置換 σ を互換の積として表すとき、その表し方や積に現れる互換の個数は一意的に決まるものではないが、その個数が偶数であるか、奇数であるかは決まる。(ここでは証明は省略するが、線形代数で学んだはずである。) 個数が偶数である置換を**偶置換**、奇数である置換を**奇置換**とよぶ。置換 σ の**符号**とは、偶置換のとき 1、奇置換のとき -1 と定めたもので、$\mathrm{sgn}(\sigma)$ と表される。すぐに分かるように置換の符号はその型だけで決まる。偶置換全体の集合は S_n の部分群をなす。この部分群を n 次**交代群**とよび A_n と表す。$n \geq 5$ のとき、n 次交代群 A_n の正規部分群は 1 と A_n 自身しかないことが知られている。このように自明でない正規部分群をもたない群を**単純群**[1] (simple group) という。

問 1.8.16. 置換 $(1\ 2\ 3\ 4\ 5)$, $(1\ 2\ 3\ 4)(5\ 6)$ の符号をそれぞれ求めよ。

問 1.8.17. A_4 の元をすべて書け。

[1]単純群は有限群論で極めて重要な役割をもっている。有限単純群は 1980 年代にその分類が完成し、これは 20 世紀の数学のもっとも重要な結果の一つとされている。しかし、その証明は長く難解であり、そのすべてを理解している人はいないようである。

1.9 モノイドの単元群

M をモノイドとし、$U(M)$ を M の正則元全体の集合とする。このとき $U(M)$ は M の演算で閉じていて、群となる。これをモノイド M の**単元群**という。

例 1.9.1. 体 K 上の n 次正方行列の全体 $M_n(K)$ は積に関してモノイドとなり、その正則元は正則行列である。このモノイドの単元群が一般線型群 $GL_n(K)$ である。

例 1.9.2. 集合 X から X への写像全体の集合は写像の合成を演算として、恒等写像を単位元とするモノイドになる。正則元は全単射であり、このモノイドの単元群が対称群 $\mathrm{Sym}(X)$ である。

例 1.9.3. 単位元をもつ環 R は乗法に関してモノイドであるから、その単元群 $U(R)$ が定義される。これを単に、単位元をもつ環 R の単元群という。

例 1.9.4. 体 (または斜体) K の単元群は $U(K) = K - \{1_K\}$ である。これを体 K の乗法群ともいう。

例 1.9.5. 有理整数環 $\mathbb{Z}$ の単元群は $U(\mathbb{Z}) = \{1, -1\}$ である。

演習問題

問 1.9.6. 位数が素数である群は巡回群であることを示せ。

問 1.9.7. 群 G の部分群が 1 と G しかないならば G は素数位数巡回群であることを示せ。

問 1.9.8. 群 G の任意の元 g に対して $g^2 = 1$ であるとする。このとき G はアーベル群であることを示せ。

問 1.9.9. G を群、$Z(G)$ をその中心とする。$G/Z(G)$ が巡回群であれば G はアーベル群であることを示せ。(この場合、結果として $G = Z(G)$ となる。)

問 1.9.10. K を体とする。$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ に対して $M' = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$ とおくと $M' \in GL_3(K)$ である。これを同一視することによって $GL_2(K)$ を $GL_3(K)$ の部分集合と考える。このとき $GL_2(K)$ は $GL_3(K)$ の部分群であることを示せ。(同様にして $m \leq n$ に対して $GL_m(K)$ は $GL_n(K)$ の部分群となる。)

問 1.9.11. 集合 X 上の対称群 $\mathrm{Sym}(X)$ について考える。$Y \subset X$ とするとき、$\mathrm{Sym}(Y)$ の元は $X - Y$ の元を動かさないものと見て $\mathrm{Sym}(X)$ の元と見ることが出来る。このとき $\mathrm{Sym}(Y) \subset \mathrm{Sym}(X)$ であるが、$\mathrm{Sym}(Y)$ は $\mathrm{Sym}(X)$ の部分群になることを示せ。(特に $m \leq n$ のとき S_m は S_n の部分群であると考えることが出来る。)

問 1.9.12. 位数 8 の二面体群 $G = D_8 = \langle x, y \mid x^4 = y^2 = 1,\ yx = x^3y \rangle$ の部分群 $H = \langle y \rangle$ を考える。G の H による左剰余類分解と右剰余類分解を求めよ。また (H, H) による両側剰余類分解を求めよ。

問 1.9.13. $Q_8 = \{\pm 1, \pm i, \pm, j, \pm k\}$ とし、積を

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

で定める。ただし 1 は単位元で、-1 の積は通常の積のように定める。このとき Q_8 は群となる。これを**四元数群**という。Q_8 のすべての元について、その位数を求めよ。

また位数 8 の二面体群 D_8 のすべての元についてもその位数を求め、Q_8 と D_8 が本質的に異なる群であることを確認せよ。

問 1.9.14. $V = \langle x, y \mid xy = yx,\ x^2 = y^2 = 1 \rangle$ とおく。V のすべての元を求め、その演算表を書け。(V を**クラインの四元群**という。)

問 1.9.15. 複素数体上の一般線形群 $GL_n(\mathbb{C})$ の中心を求めよ。

Chapter 2

準同型定理と同型定理

2.1 群準同型

G, H を群とする。写像 $f : G \to H$ が**群準同型** (group homomorphism)、または単に**準同型**であるとは、任意の $a, b \in G$ に対して

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

が成り立つこととする。加法群を考えるときには、その演算が加法であることに注意して

$$f(a + b) = f(a) + f(b)$$

が成り立つことが準同型であることの条件となる。

問 2.1.1. G を乗法群、H を加法群とするとき、$f : G \to H$ が群準同型となる条件を書け。

例 2.1.2. K を体とし、一般線型群 $GL_n(K)$ を考える。$\det : GL_n(K) \to K^\times$ を行列式をとる写像とする。このとき $\det(AB) = \det(A)\det(B)$ が成り立つので、これは群準同型である。

例 2.1.3. n 次の置換 σ に対して、その符号 $\mathrm{sgn}(\sigma)$ を対応させる写像は、対称群 S_n から乗法群 $\{1, -1\}$ への群準同型である。

例 2.1.4. K を体とし V, W は K-ベクトル空間とする。線型写像 $f : V \to W$ は $f(v + v') = f(v) + f(v')$ をみたすので、加法群の準同型である。

例 2.1.5. $\mathbb{R}$ を加法群と見る。また $\mathbb{R}^\times = \mathbb{R} - \{0\}$ とおいて、これを乗法群と見る。指数関数 $\exp : \mathbb{R} \to \mathbb{R}^\times$ は $\exp(x + y) = \exp(x)\exp(y)$ をみたし、加法群から乗法群への群準同型である。

例 2.1.6. G を群とし H をその部分群とする。このとき自然な埋め込み $\iota : H \to G$, $\iota(h) = h$ は群準同型である。

問 2.1.7. $f : G \to H$, $g : H \to K$ をそれぞれ群準同型とすると、合成写像 $g \circ f : G \to K$ も群準同型であることを示せ。

命題 2.1.8. $f : G \to H$ を群準同型とするとき、次が成り立つ。

(1) $f(1_G) = 1_H$

(2) $a \in G$ に対して $f(a^{-1}) = f(a)^{-1}$

証明. (1) $f(1_G) = f(1_G 1_G) = f(1_G)f(1_G)$ である。両辺に右から $f(1_G)^{-1}$ をかければ $1_H = f(1_G)$ となる。

(2) $1_H = f(1_G) = f(aa^{-1}) = f(a)f(a^{-1})$ である。両辺に左から $f(a)^{-1}$ をかければ $f(a)^{-1} = f(a^{-1})$ となる。 □

$f : G \to H$ を群準同型とする。

$$\mathrm{Ker}f = \{a \in G \mid f(a) = 1_H\}$$

とおいて、これを f の**核** (kernel) という。また

$$\mathrm{Im}f = \{f(a) \mid a \in G\}$$

とおいて、これを f の**像** (image) という。

問 2.1.9. $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ を $f(a + 4\mathbb{Z}) = 2a + 4Z$ で定める。このとき f は加法群の群準同型であることを示せ。また f の核と像を求めよ。

命題 2.1.10. $f : G \to H$ を群準同型とするとき、次が成り立つ。

(1) $\mathrm{Ker}f \trianglelefteq G$

(2) $\mathrm{Im}f \leq H$

証明. (1) まず $f(1_G) = 1_H$ より $1_G \in \mathrm{Ker}f$ なので $\mathrm{Ker}f \neq \emptyset$ である。$x, y \in \mathrm{Ker}f$ とする。$f(xy^{-1}) = f(x)f(y)^{-1} = 1_H$ となるので $xy^{-1} \in \mathrm{Ker}f$ となり、$\mathrm{Ker}f \leq G$ である。$x \in \mathrm{Ker}f$, $g \in G$ とする。$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g)^{-1} = 1_H$ となるので $gxg^{-1} \in \mathrm{Ker}f$ となり、$\mathrm{Ker}f \trianglelefteq G$ である。

(2) まず $1_H = f(1_G) \in \mathrm{Im}f$ より $\mathrm{Im}f \neq \emptyset$ である。$a, b \in \mathrm{Im}f$ とする。ある $x, y \in G$ があって $a = f(x)$, $b = f(y)$ である。このとき

$$ab^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in \mathrm{Im}f$$

となるから $\mathrm{Im}f \leq H$ である。 □

例 2.1.11. 対称群 S_n とその符号 sgn について、sgn は準同型であり、その核は交代群 A_n である。$(\mathrm{Ker}(\mathrm{sgn}) = A_n)$

群準同型 $f : G \to H$ が、写像として単射のとき f を**単準同型** (monomorphism)、写像として全射のとき f を**全準同型** (epimorphism) という。また f が全単射のとき**同型** (isomorphism)、または**同型写像**という。f が同型であることを $f : G \xrightarrow{\sim} H$ とも表す。二つの群 G と H の間に同型が存在するとき、G と H は**同型である**といい $G \cong H$ と表す。同型な群は群としては “同じもの” と考えることができ、しばしば同一視される。

任意の群 G に対して、G から G への恒等写像は同型であり、したがって $G \cong G$ である。また $f : G \to H$ が同型ならば、f が全単射であることから逆写像 $f^{-1} : H \to G$ が定義され、これもまた同型となる。したがって $G \cong H$ ならば $H \cong G$ である。$f : G \to H$ と $g : H \to K$ が共に同型であるならば、その合成写像 $g \circ f : G \to K$ も同型になる。よって $G \cong H$ かつ $H \cong K$ ならば $G \cong K$ も成り立つ。

例えば $G = \{a, b\}$, $H = \{x, y\}$ で、その演算表がそれぞれ

	a	b
a	a	b
b	b	a

	x	y
x	x	y
y	y	x

であったとしよう。このとき G と H はそれぞれ群となるが、この二つは用いている記号が違うだけで、本質的に同じものであることは理解できると思う。このとき $f : G \to H$ を

$$f(a) = x, \quad f(b) = y$$

で定めれば、f が同型である。このように二つの群が同型であるとは、適当な対応によってまったく同じ演算をもつ群であるということである。

命題 2.1.12. 群準同型 $f : G \to H$ について、f が単射であることと $\mathrm{Ker} f = 1$ であることは同値である。

証明. f が単射であるとする。$1_G \in \mathrm{Ker} f$ である。$x \in \mathrm{Ker} f$ とすると $f(x) = 1_H = f(1_G)$ で f が単射であることから $x = 1_G$ となる。よって $\mathrm{Ker} f = 1$ である。

$\mathrm{Ker} f = 1$ とする。$f(x) = f(y)$ とすると、$1 = f(x)f(y)^{-1} = f(xy^{-1})$ となり $xy^{-1} \in \mathrm{Ker} f = \{1_G\}$ である。よって $x = y$ となり f は単射である。 □

例 2.1.13. $N \trianglelefteq G$ とする。$f : G \to G/N$ を $f(g) = gN$ で定めると、これは全準同型となる。これを**自然な全準同型**という。このとき $\mathrm{Ker} f = N$ である。

命題 2.1.14. $f : G \to H$ を群準同型とする。

(1) $A \leq G$ とすると $f(A) \leq H$ である。

(2) $B \leq H$ とすると $f^{-1}(B) \leq G$ である。

(3) $B \trianglelefteq H$ とすると $f^{-1}(B) \trianglelefteq G$ である。

(4) f が全準同型であって $A \trianglelefteq G$ とすると $f(A) \trianglelefteq H$ である。

証明. (1) $x, y \in A$ とする。$f(x)f(y)^{-1} = f(xy^{-1}) \in f(A)$ なので $f(A) \leq H$ である。

(2) $s, t \in f^{-1}(B)$ とする。このとき $f(s), f(t) \in B$ なので、$f(st^{-1}) = f(s)f(t)^{-1} \in B$ となり、$st^{-1} \in f^{-1}(B)$ である。

(3) $f^{-1}(B) \leq G$ であることは (2) で示されている。$g \in G$, $s \in f^{-1}(B)$ とする。$f(s) \in B \trianglelefteq H$ である。このとき

$$f(gsg^{-1}) = f(g)f(s)f(g)^{-1} \in f(g)Bf(g)^{-1} \subset B$$

である。よって $gsg^{-1} \in f^{-1}(B)$ である。

(4) $f(A) \leq B$ は (1) で示されている。$x \in f(A)$, $h \in H$ とする。ある $a \in A$ があって $x = f(a)$ である。また、f は全射なので、ある $g \in G$ があって $h = f(g)$ となる。このとき

$$hxh^{-1} = f(g)f(a)f(g)^{-1} = f(gag^{-1}) \in f(gAg^{-1}) \subset f(A)$$

となる。 □

問 2.1.15. $f : G \to H$ を群準同型とし $A \trianglelefteq G$ としても、$f(A) \trianglelefteq H$ とは限らない。このような例を具体的に構成せよ。

2.2 準同型定理

ここでは群論でもっとも重要な定理の一つである準同型定理について解説する。

命題 2.2.1. $f : G \to H$ を群準同型とする。N は $\mathrm{Ker}f$ に含まれる G の正規部分群であるとする。このとき $\overline{f} : G/N \to H$ を $\overline{f}(gN) = f(g)$ で定めることができ、これは群準同型である。

証明. まず $\overline{f}$ が矛盾なく定義されることを示す。$aN = bN$ とする。ある $n \in N$ があって $b = an$ と書ける。このとき、$n \in N \subset \mathrm{Ker}f$ なので

$$f(b) = f(an) = f(a)f(n) = f(a)1_H = f(a)$$

である。よって $\overline{f}$ は矛盾なく定義される。

$\overline{f}$ が準同型であることは

$$\overline{f}((aN)(bN)) = \overline{f}((ab)N) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN)$$

から分かる。 □

定理 2.2.2 (準同型定理)**.** $f : G \to H$ を群準同型とし、$\overline{f} : G/\mathrm{Ker}f \to \mathrm{Im}f$ を $\overline{f}(g(\mathrm{Ker}f)) = f(g)$ で定めれば、これは同型である。したがって

$$G/\mathrm{Ker}f \cong \mathrm{Im}f$$

が成り立つ。特に f が全準同型ならば $G/\mathrm{Ker}f \cong H$ である。

証明. $N = \mathrm{Ker}f$ とおく。

命題 2.2.1 より群準同型 $f' : G/N \to H$ $(gN \mapsto f(g))$ が得られる。$\mathrm{Im}f = \mathrm{Im}f'$ なので、値域を小さくすることができ、群準同型 $\overline{f} : G/\mathrm{Ker}f \to \mathrm{Im}f$ が定義される。また、値域を $\mathrm{Im}f$ としたので、これは全射である。

$\overline{f}$ が単射であることを示す。$aN \in \mathrm{Ker}\overline{f}$、すなわち $\overline{f}(aN) = 1_H$ とする。このとき $f(a) = 1_H$ であるから $a \in \mathrm{Ker}f$ であり、よって $aN = 1_G N$ である。したがって $\mathrm{Ker}\overline{f} = 1$ となり、$\overline{f}$ は単射である。

以上より $\overline{f}$ は同型である。 □

二つの群が同型であることを直接示すのは簡単ではないことが多く、多くの場合に準同型定理が用いられる。

例 2.2.3. $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ を $f(a+4\mathbb{Z}) = 2a+4Z$ で定める。このとき f は加法群の群準同型である (問 2.1.9 参照)。$a+4\mathbb{Z}$ を $\overline{a}$ で表すことにする。f の核と像は

$$\mathrm{Ker}f = \{\overline{0},\ \overline{2}\} = 2\mathbb{Z}/4\mathbb{Z}, \quad \mathrm{Im}f = \{\overline{0},\ \overline{2}\} = 2\mathbb{Z}/4\mathbb{Z}$$

である。したがって準同型定理より

$$(\mathbb{Z}/4\mathbb{Z})/(2\mathbb{Z}/4\mathbb{Z}) \cong 2\mathbb{Z}/4\mathbb{Z}$$

が成り立つ。

2.3 同型定理

ここでは準同型定理 (定理 2.2.2) から得られる、同型定理と呼ばれるいくつかの定理を紹介する。

定理 2.3.1 (同型定理)**.** H を G の部分群、N を G の正規部分群とする。このとき

$$HN/N \cong H/(H \cap N)$$

が成り立つ。

証明. 写像 $f : H \to HN/N$ を $f(h) = hN$ で定める。これが準同型であることはすぐに分かる。任意の $x \in HN$ に対して、ある $h \in H$ と $n \in N$ があって $x = hn$ となり、$xN = hnN = hN = f(h)$ なので f は全射である。

$f(h) = hN = 1N$ は $h \in N$ と同値なので $\mathrm{Ker}f = H \cap N$ である。よって準同型定理より $HN/N \cong H/(H \cap N)$ である。 □

例 2.3.2. $G = \mathbb{Z}$, $H = 4\mathbb{Z}$, $N = 6\mathbb{Z}$ とし、これらを加法群と見る。$H+N = 4\mathbb{Z}+6\mathbb{Z} = 2\mathbb{Z}$, $H \cap N = 12\mathbb{Z}$ となるので、同型定理より

$$2\mathbb{Z}/6\mathbb{Z} \cong 4\mathbb{Z}/12\mathbb{Z}$$

が得られる。実際、$f : 2\mathbb{Z}/6\mathbb{Z} \to 4\mathbb{Z}/12\mathbb{Z}$, $f(a+6\mathbb{Z}) = 2a+12\mathbb{Z}$ がこの同型を与えることが簡単に確認できる。

定理 2.3.3 (同型定理)**.** N と H を G の正規部分群とし $N \leq H$ とする。このとき

$$G/H \cong (G/N)/(H/N)$$

が成り立つ。

証明. $f : G \to G/H$ を自然な全準同型とする。$\mathrm{Ker}f = H \geq N$ であるから、準同型 $g : G/N \to G/H$, $g(xN) = xH$ が定義され、これも全準同型である。

$\mathrm{Ker}g = H/N$ が簡単に確かめられ、準同型定理から $G/H \cong (G/N)/(H/N)$ が成り立つ。 □

例 2.3.4. 例 2.2.3 で $(\mathbb{Z}/4\mathbb{Z})/(2\mathbb{Z}/4\mathbb{Z}) \cong 2\mathbb{Z}/4\mathbb{Z}$ であることを見たが、同型定理より $(\mathbb{Z}/4\mathbb{Z})/(2\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ が成り立つので、これらを合わせれば

$$\mathbb{Z}/2\mathbb{Z} \cong 2\mathbb{Z}/4\mathbb{Z}$$

が得られる。実際、$f : \mathbb{Z}/2\mathbb{Z} \to 2\mathbb{Z}/4\mathbb{Z}$, $f(a + 2\mathbb{Z}) = 2a + 4\mathbb{Z}$ がこの同型を与えることが簡単に確認できる。

$N \trianglelefteq G$ とし

$$p : G \to G/N$$

を自然な全準同型とする。$\mathscr{S}$ を G の部分群で N を含むもの全体の集合、$\mathscr{T}$ を G/N の部分群全体の集合とする。$H \in \mathscr{S}$ に対して $H/N = p(H) \in \mathscr{T}$ である。$X \in \mathscr{T}$ とすると、$p^{-1}(X) \in \mathscr{S}$ である。これらの対応が、互いに逆の対応になっていることも確認でき、次の定理が成り立つ。

定理 2.3.5. $N \trianglelefteq G$ とする。このとき G の部分群で N を含むもの全体の集合と G/N の部分群全体の集合の間には自然な全単射が存在する。またこれによって正規部分群同士が対応する。

問 2.3.6. 定理 2.3.5 を示せ。

2.4 自己同型

G を群とする。G から G への同型を G の**自己同型** (automorphism) という。G の自己同型の全体は写像の合成を演算として群をなす。これを G の**自己同型群**といい $\mathrm{Aut}(G)$ と表す。

例 2.4.1. 有限体 $GF(2)$ 上の 2 次元ベクトル空間 V を加法群と見る。

$$V = \{(0,0), (0,1), (1,0), (1,1)\}$$

である。このとき $V - \{(0,0)\}$ の任意の置換は V の自己同型となる。したがって $\mathrm{Aut}(V) \cong S_3$ が成り立つ。

$g \in G$ に対して、

$$f_g : G \to G, \quad x \mapsto gxg^{-1}$$

と定めると、f_g は G の自己同型となる。このように G の元から得られる自己同型を**内部自己同型** (inner automorphism) という。このとき、写像

$$f : G \to \mathrm{Aut}(G), \quad g \mapsto f_g$$

が得られ、これは群準同型となる。よって f の像、すなわち内部自己同型の全体は $\mathrm{Aut}(G)$ の部分群をなす。これを**内部自己同型群**といい $\mathrm{Inn}(G)$ と表す。f の核を求める。$g \in \mathrm{Ker}f$ ということは、$f_g = id_G$ ということで、これは「任意の $x \in G$ に対して $gxg^{-1} = x$」ということである。したがって $\mathrm{Ker}f$ は G の中心 $Z(G)$ に一致する。準同型定理より以下の命題が成り立つ。

命題 2.4.2. $\mathrm{Inn}(G) \cong G/Z(G)$ である。

更に次の命題が成り立つ。

命題 2.4.3. $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ である。

証明. $\sigma \in \mathrm{Inn}(G)$, $\tau \in \mathrm{Aut}(G)$ とする。ある $g \in G$ が存在して、$x \in G$ に対して $\sigma(x) = f_g(x) = gxg^{-1}$ である。ただし f_g は上で考えたものである。$y \in G$ とすると

$$(\tau\sigma\tau^{-1})(y) = \tau(g\tau^{-1}(y)g^{-1}) = \tau(g)y\tau(g)^{-1}$$

となる。これは $\tau\sigma\tau^{-1} = f_{\tau(g)} \in \mathrm{Inn}(G)$ を意味する。 □

$\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ であるから剰余群 $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ が考えられる。これを G の**外部自己同型群**といい $\mathrm{Out}(G)$ と表すこともある。

すぐに分かるように、G の部分群 H が G の正規部分群であることは、任意の $\sigma \in \mathrm{Inn}(G)$ に対して $\sigma(H) = H$ となることと同値である。条件を強くして次の定義をする。G の部分群 H が G の**特性部分群** (characteristic subgroup) であるとは、任意の $\sigma \in \mathrm{Aut}(G)$ に対して $\sigma(H) = H$ となることとする。明らかに特性部分群は正規部分群であるが、一般に逆は正しくない。

一般に $H \trianglelefteq G$, $K \trianglelefteq H$ であっても $K \trianglelefteq G$ とは限らない。次の定理が成り立つ。

定理 2.4.4. $H \trianglelefteq G$ とし K を H の特性部分群とするとき $K \trianglelefteq G$ である。

証明. $k \in K$, $g \in G$ とする。$gkg^{-1} = f_g(k)$ で $H \trianglelefteq G$ より $f_g \in \mathrm{Aut}(H)$ となるので、K が H の特性部分群であることから $gkg^{-1} \in K$ である。 □

定理 2.4.5. H を G の特性部分群、K を H の特性部分群とすると K は G の特性部分群である。

証明. $\sigma \in \mathrm{Aut}(G)$ とする。$\sigma|_H \in \mathrm{Aut}(H)$ なので $\sigma(K) = (\sigma|_H)(K) = K$ である。 □

例 2.4.6. 群の中心 $Z(G)$ は G の特性部分群である。

例 2.4.7. 巡回群の任意の部分群は特性部分群である。

演習問題

問 2.4.8. G, H を群とし $f : G \to H$ を同型とする。f は全単射なので、その逆写像 $f^{-1} : H \to G$ が定義される。このとき f^{-1} も同型であることを示せ。

問 2.4.9. $\mathscr{G}$ を群を要素とする集合とする。$\mathscr{G}$ に属する二つの群が同型であるという関係は $\mathscr{G}$ 上の同値関係となることを示せ。

問 2.4.10. G, H を群とし $f : G \to H$ を準同型とする。$g \in G$ の位数について $o(g) < \infty$ であるとする。このとき $o(f(g)) < \infty$ であり、$o(f(g))$ は $o(g)$ の約数になることを示せ。(特に f が同型ならば $o(g) = o(f(g))$ となる。)

問 2.4.11. G を群とする。$a, b \in G$ に対して $[a, b] = aba^{-1}b^{-1}$ とおいて、これを a と b の**交換子** (commutator) という。G の交換子すべてで生成される部分群を G の**交換子群** (derived subgroup) といい $D(G)$ または $[G, G]$ と書く。

(1) $[a, b] = 1$ であることと $ab = ba$ が成り立つことは同値であることを示せ。

(2) $D(G)$ は G の特性部分群であることを示せ。

(3) $N \trianglelefteq G$ に対して、G/N がアーベル群であることと $D(G) \subset N$ であることは同値であることを示せ。

(4) $M \trianglelefteq G$, $N \trianglelefteq G$ とし、G/M, G/N はアーベル群であるとする。このとき $G/(M \cap N)$ もアーベル群であることを示せ。

問 2.4.12. G を群とする。$D^0(G) = G$ とし、帰納的に $D^{n+1}(G) = D(D^n(G))$ と定め、$D^n(G)$ を **n-次交換子群**という。ある自然数 n に対して $D^n(G) = 1$ となるとき、G を**可解群**[1] (solvable group) という。

G が可解群であるとき、その部分群と (ある正規部分群による) 剰余群もまた可解群であることを示せ。

問 2.4.13. n-次交換子群 $D^n(G)$ は G の特性部分群であることを示せ。

問 2.4.14. G を群とし A, B を G の正規部分群で $A \cap B = 1$ なるものとする。このとき $a \in A$ と $b \in B$ について $ab = ba$ となることを示せ。

問 2.4.15. G, A を群とする。準同型 $\varphi : A \to \mathrm{Aut}(G)$ が与えられているものとする。このとき集合としての直積 $G \times A$ に以下のように演算を定義する。$g, h \in G$, $a, b \in A$ に対して

$$(g, a)(h, b) = (g\varphi(a)(h), ab)$$

このとき、この演算は結合法則をみたし $G \times A$ は群になることを示せ。(これを G と A の**半直積** (semidirect product) といい $G \rtimes A$ と表す。)

問 2.4.16. 無限位数巡回群の自己準同型群は位数 2 の巡回群であることを示せ。

問 2.4.17. 位数 n の有限巡回群の自己準同型群の位数は $\varphi(n)$ であることを示せ。ただし $\varphi(n)$ は**オイラー関数**であり、n と互いに素である n 以下の自然数の個数を表す。

[1] 可解群でない有限群のうち、位数が最小のものは 5 次の交代群 A_5 である。可解群という用語は 5 次以上の方程式が解の公式をもたないことと関係している。

Chapter 3

群の作用

3.1 群の作用

X を集合とし G を群とする。写像 $f : G \times X \to X$ に対して $f(g, x)$ を gx と表すことにする。f が以下の条件をみたすとき f を G **の** X **への (左からの) 作用**という。

(A1) 任意の $x \in X$ に対して $1_G x = x$ が成り立つ。

(A2) $x \in X$, $g, h \in G$ に対して $(gh)x = g(hx)$ が成り立つ。

このとき f を省略して G **は** X **に (左から) 作用する**ともいう。また、このとき X を**左** G**-集合**ともいう。同様に右からの作用も定義される。右からの作用は xg のように群の元を右に書いて表される。左右の違いは、積 gh を作用させるときに g を先にするか h を先にするかの違いである。したがって、例えばアーベル群を考えるときには左右の違いを意識する必要はない。

群の作用が、何らかの積と紛らわしいときには gx や xg の代わりに ${}^g x$ や x^g のような記号も用いられる。

以下では主に左からの作用を考えるが、ほとんどのことが同様に右からの作用についても成り立つ。

例 3.1.1. K を体とする。一般線型群 $GL_n(K)$ (例 1.8.1 参照) は自然に線型空間 K^n に作用する。K^n を列ベクトルの集合と見たときには左からの作用を考え、K^n を行ベクトルの集合と見たときには右からの作用を考えるのが普通である。

例 3.1.2. K を体とする。一般線型群 $GL_n(K)$ の $M_n(K)$ への二つの作用を考える。$M \in M_n(K)$ と $P \in GL_n(K)$ に対して

$$ {}^P M = PMP^{-1}, \quad M^P = P^{-1}MP $$

とする。これらが、それぞれ左作用、右作用であることを確認する。いずれの場合も単位元に関する条件 (A1) は自明なので (A2) の条件を見る。まず

$$ {}^{(PQ)}M = (PQ)M(PQ)^{-1} = PQMQ^{-1}P^{-1} = {}^P(QMQ^{-1}) = {}^P({}^Q M) $$

であるから ${}^PM = PMP^{-1}$ は左作用を定める。同様に

$$M^{(PQ)} = (PQ)^{-1}M(PQ) = Q^{-1}P^{-1}MPQ = (P^{-1}MP)^Q = (M^P)^Q$$

となり $M^P = P^{-1}MP$ は右作用を定める。

例 3.1.3 (自明な作用)**.** 群 G の集合 X への作用を、任意の $g \in G$ と $x \in X$ に対して $gx = x$ で定めることが出来る。このような作用を**自明な作用**という。

問 3.1.4. S を $\mathbb{R}$ 上の n 次対称行列全体の集合とする。$O(n)$ は n 次直交群である (例 1.8.6 参照)。$M \in S$ と $T \in O(n)$ に対して ${}^TM = TMT^{-1}$ と定めれば、これは $O(n)$ の S への左からの作用を定めることを示せ。

$f : G \times X \to X$ を群 G の集合 X への作用とする。$g \in G$ を一つ固定すると、写像 $f_g : X \to X, f_g(x) = gx$ が定まる。作用の定義から $f_g \circ f_{g^{-1}} = f_{g^{-1}} \circ f_g = id_G$ がすぐに分かり、f_g は全単射、すなわち $f_g \in \mathrm{Sym}(X)$ となる。これによって写像 $F : G \to \mathrm{Sym}(X)$, $F(g) = f_g$ が得られる。$g, h \in G$ について、任意の $x \in X$ に対して

$$\begin{aligned} F(gh)(x) &= f_{gh}(x) = (gh)x = g(hx) = f_g(f_h(x)) \\ &= F(g)(F(h)(x)) = (F(g) \circ F(h))(x) = (F(g)F(h))(x) \end{aligned}$$

となるので $F(gh) = F(g)F(h)$ である。すなわち F は準同型となる。

逆に準同型 $F : G \to \mathrm{Sym}(X)$ が与えられると $f : G \times X \to X$ を $gx = f(g, x) = F(g)(x)$ で定めて G の X への作用が定まる。このように群 G の集合 X への作用を与えることと、準同型 $G \to \mathrm{Sym}(X)$ を与えることは同値である。準同型 $G \to \mathrm{Sym}(X)$ を群 G の X 上の**置換表現** (permutation representation) ともいう。

群 G は集合 X に左から作用するものとし、それによって得られる準同型を $f : G \to \mathrm{Sym}(X)$ とする。G の X への作用が**忠実** (faithful) であるとは、f が単射であることとする。

問 3.1.5. 群 G の集合 X への作用について、以下の条件は同値であることを示せ。

(1) 群 G の集合 X への作用は忠実である。

(2) $g \in G$ とするとき、任意の $x \in X$ に対して $gx = x$ ならば $g = 1$ である。

群 G の集合 X への作用が忠実であるならば、準同型 $f : G \to \mathrm{Sym}(X)$ は単射なので、これを同一視して $G \leq \mathrm{Sym}(X)$ と見ることが出来る。一般に対称群 $\mathrm{Sym}(X)$ の部分群を X 上の**置換群** (permutation group) という。特に S_n の部分群を n **次置換群**という。

集合 X 上の置換群 G は自然に X への作用を与える。逆に群 G の X への作用が与えられると、準同型 $f : G \to \mathrm{Sym}(X)$ の核を考えて、置換群 $G/\mathrm{Ker}f$ が得られる。

3.2 安定化部分群と軌道

群 G は集合 X に左から作用するものとする。$x, y \in X$ に対して $x \sim y$ という関係を、ある $g \in G$ があって $y = gx$ となることで定める。このときこの関係は同値関係である。

問 3.2.1. $\sim$ が X 上の同値関係であることを示せ。

この同値関係による同値類を X の G による**軌道** (orbit)、または G-**軌道**という。$x \in X$ を含む軌道 (同値類) C_x は

$$C_x = \{gx \mid g \in G\}$$

で与えられる。すなわち G の元で移りあう X の元全体の集合である。一つの軌道に含まれる元の数を軌道の**長さ**ともいう。軌道 C_x を Gx とも表す。(作用を ${}^g x$, x^g のように書く場合は ${}^G x$, x^G などと書く。) g は G 全体を動くので Gx は見掛け上 G の元と同じ数の要素をもつ。しかし、この中には同じものも含まれていて、実際には G の元の数よりも少ないこともある。そこで $g, h \in G$ に対して、いつ $gx = hx$ が成り立つのかを考える。$gx = hx$ とすると

$$x = 1x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}(hx) = (g^{-1}h)x$$

である。そこで

$$G_x = \{g \in G \mid gx = x\}$$

とおいて、これを x の G における**安定化部分群**とよぶ。実際 G_x は G の部分群になる。(G_x と Gx は違う意味で用いられるので注意して欲しい。)

問 3.2.2. G_x が G の部分群になることを示せ。

例 3.2.3. S_4 の部分群 $G = \langle (1\ 2),\ (3\ 4) \rangle = \{(\ ),\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4)\}$ を考える。G は $X = \{1, 2, 3, 4\}$ に自然に左から作用する。このとき X の G による軌道は $\{1, 2\}$, $\{3, 4\}$ であり、X の軌道への分解は

$$X = \{1, 2\} \cup \{3, 4\}$$

となる。安定化部分群は

$$G_1 = G_2 = \{(\ ),\ (3\ 4)\}, \quad G_3 = G_4 = \{(\ ),\ (1\ 2)\}$$

である。

以下のことが分かる。

$$gx = hx \iff x = (g^{-1}h)x \iff g^{-1}h \in G_x \iff gG_x = hG_x$$

定理 3.2.4. 群 G は集合 X に左から作用するものとし、$x \in X$ とする。このとき写像 $f : G/G_x \to Gx,\ f(gG_x) = gx$ は全単射である。特に $|G : G_x| < \infty$ ならば $|G : G_x| = |Gx|$ である。

証明. 上に述べたことから $gG_x = hG_x$ ならば $gx = hx$ となるので f は矛盾なく定義されている。Gx の元は、ある $g \in G$ を用いて gx と書けるので f は全射である。また $f(gG_x) = f(hG_x)$ ならば $gx = hx$ で、上に述べたことから $gG_x = hG_x$ である。よって f は単射でもある。 □

X が唯一つの軌道からなるとき、G の作用は**可移である** (transitive) という。すなわち G の X への作用が可移であるとは、「任意の $x, y \in X$ に対して、ある $g \in G$ が存在して $y = gx$ となる」ということである。このとき X を**可移な G-集合** (transitive G-set) ともいう。

一般に G が X に作用するとき、$x \in X$ として軌道 Gx を考えると、G は Gx に作用していると見ることが出来る。すなわち $f : G \times X \to X$ を作用とするとき f を $G \times Gx$ に制限すると、その像に関して $\mathrm{Im}(f|_{G\times Gx}) \subset Gx$ である。よって写像 $f' : G \times Gx \to Gx$ が定まり、これが G の Gx への作用を与える。このとき、この作用は可移である。

このようにして、任意の G-集合は共通部分のない可移な G-集合の和集合として書くことができる。したがって G-集合を考えるには、本質的には可移なものだけを考えればよい。次の節で可移な作用がどのように与えられるかを見る。

例 3.2.5 (正則 G-集合)**.** G を群とする。G 自身への G の作用を元を左からかけること、すなわち $(g, x) \mapsto gx$ で定めれば、G 自身は可移な G-集合となる。これを (左) **正則 G-集合**という。

群 G は集合 X に作用するとする。$Y \subset X$ が G **の作用で閉じている**とは、任意の $y \in Y$ と $g \in G$ に対して $gy \in Y$ となることである。このとき $y \in Y$ を含む軌道はすべて Y に含まれ、したがって Y はいくつかの G-軌道の和集合となる。また、前と同様の議論で G は Y に作用すると見ることが出来る。

3.3 群の左剰余類への作用

G を群とし H をその部分群とする。H による左剰余類の集合

$$G/H = \{aH \mid a \in G\}$$

を考える。G の G/H への作用を

$$g(aH) = (ga)H$$

で定めることが出来る。このとき、この作用は可移である。実際 $aH, bH \in G/H$ とすると $bH = (ba^{-1})(aH)$ が成り立つ。

以下ではこれとは逆に、可移な作用はこのように左剰余類への作用と本質的に同じであることを示す。これをいうには “作用が本質的に同じである” とはどういうことかをきちんと理解する必要がある。それは次の定義による。

左 G-集合 X と Y を考える。X と Y が G-集合として**同型**であるとは、全単射 $f : X \to Y$ が存在して、$x \in X$, $g \in G$ に対して

$$gf(x) = f(gx)$$

が成り立つことである。このときの f を G-集合としての**同型**という。これは次の図式が可換[1] であることを意味し、X と Y への G の作用が “本質的に同じである” ことを意味する。

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ {\scriptstyle id_G \times f}\downarrow & & \downarrow{\scriptstyle f} \\ G \times Y & \longrightarrow & Y \end{array}$$

定理 3.3.1. G は X に可移に作用するとする。$x \in X$ とする。このとき $f : G/G_x \to X$ を $f(aG_x) = ax$ で定めれば f は G-集合としての同型である。

したがって任意の可移な G-集合は、ある部分群に対する剰余類の定める G-集合と同型である。

証明. $aG_x = bG_x$ ならば前に見たように $ax = bx$ が成り立ち、これは f が矛盾なく定義されることを意味する。$ax = bx$ ならば $aG_x = bG_x$ なので f は単射である。G の作用を可移と仮定しているので f は全射である。したがって f は全単射である。

$g \in G$, $aG_x \in G/G_x$ とする。このとき

$$gf(aG_x) = g(ax) = (ga)x = f((ga)G_x) = f(g(aG_x))$$

であるから f は G-集合としての同型である。 □

3.4 共役による作用

G を群とし、G の G 自身への作用を以下のように定める。$g \in G$ と $x \in G$ に対して

$$^g x = gxg^{-1}$$

と定めれば G は左 G-集合となる。この作用を G の G への**共役による作用**という。同様に

$$x^g = g^{-1}xg$$

は G の G への右からの作用を定める。

共役による (左) 作用の安定化部分群を考える。$x \in G$ とする。$g \in G_x$ であるならば $x = {}^g x = gxg^{-1}$ となり $xg = gx$ である。G_x を $C_G(x)$ と書いて、これを G における x の**中心化群** (centralizer) という。

$$C_G(x) = \{g \in G \mid xg = gx\}$$

$S \subset G$ に対しては

$$C_G(S) = \bigcap_{s \in S} C_G(s)$$

[1] いくつかの集合とその間の写像を図示するとする。ある集合 A からある集合 B への経路が複数あるとき、どの経路をたどっても結果が同じ、すなわち合成写像が一致するとき、その図式は**可換**であるという。

とおいて、これを G における S の**中心化群**という。特に $C_G(G)$ は G の中心 $Z(G)$ に一致する。

共役による左作用の $x \in G$ を含む軌道は

$$^Gx = \{^gx \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$$

である。これを G の x を含む**共役類** (conjugacy class) という。

定理 3.4.1. G を有限群とし $x \in G$ とする。x を含む共役類 ^Gx に含まれる元の数は $|G : C_G(x)|$ である。

証明. 定理 3.2.4 より直ちに分かる。 □

群 G の正規部分群 N を考える。正規部分群の定義より N は G の共役による作用で閉じている。したがって N は G のいくつかの共役類の和集合となる。逆にいくつかの共役類の和集合が部分群になっているならば、それは正規部分群である。

G を有限群とする。G への共役による作用は同値関係を定め、その同値類が共役類なので、それは G の類別を定める。$\{x_1 = 1, x_2, \cdots, x_r\}$ を類別の完全代表系とすると

$$G = {}^Gx_1 \cup {}^Gx_2 \cup \cdots \cup {}^Gx_r$$

は共通部分のない和で、したがって

$$|G| = |{}^Gx_1| + |{}^Gx_2| + \cdots + |{}^Gx_r|$$

が成り立つ。これを G の**類等式** (class equation) という。特に $C_G(1) = G$ となるので $|{}^Gx_1| = |{}^G1| = 1$ である。また、各 $|{}^Gx_i|$ は $|G : C_G(x_i)|$ に等しく、したがって $|G|$ の約数であることに注意しておく。

問 3.4.2. $|{}^Gx| = 1$ であることと $x \in Z(G)$ であることは同値であることを示せ。

例 3.4.3. 3 次対称群 S_3 の共役類は

$$C_1 = \{1\}, \quad C_2 = \{(1\ 2\ 3),\ (1\ 3\ 2)\}, \quad C_3 = \{(1\ 2),\ (1\ 3),\ (2\ 3)\}$$

である。したがって類等式は

$$6 = 1 + 2 + 3$$

となる。S_3 に自明でない正規部分群があるとすれば、単位元を含まなければならないことから、それは $C_1 \cup C_2$ または $C_1 \cup C_3$ でなければならない。また部分群の位数は S_3 の位数 6 の約数でなければならないので $C_1 \cup C_2$ のみ可能性がある。実際 $C_1 \cup C_2$ は積で閉じていることが確認でき、正規部分群となっている。また単位元のみからなる共役類以外の共役類の元数が 1 でないことから、その中心について $Z(S_3) = 1$ が確認される。

類等式はそれほどよく用いられる訳ではないが、利用できるときには強力である。次の定理はその典型的な場合である。

定理 3.4.4. p を素数とし G は位数が p^n の群とする。また N を 1 でない G の正規部分群とする。このとき $N \cap Z(G) \neq 1$ である。

証明. N は G の正規部分群なので、G のいくつかの共役類の和集合である。N に含まれる G の共役類を $C_1 = \{1_G\}, C_2, \cdots, C_\ell$ とする。$x_i \in C_i$ とすると $|{}^G x_i| = |G : C_G(x_i)|$ なので、これは $|G|$ の約数で、したがって p^{n_i} と書ける。特に $|{}^G x_1| = 1$ である。したがって

$$|N| = \sum_{i=1}^{\ell} p^{n_i} = 1 + \sum_{i=2}^{\ell} p^{n_i}$$

と書ける。ここで $|N|$ も $|G|$ の約数で $N \neq 1$ なので、$|N|$ は p で割り切れる。$p^{n_1} = 1$ なので、もし他のすべての i について $n_i > 0$ ならば、右辺は p で割り切れない。したがって、ある $i \neq 1$ について $n_i = 0$ となる。このとき $1 \neq x_i \in Z(G) \cap N$ である。 □

この定理のように位数が素数 p のべきである有限群を **p-群**という。

定理 3.4.5. p-群の中心は 1 ではない。

証明. 定理 3.4.4 で $G = N$ とすればよい。 □

$A \subset G$ とする。$g \in G$ に対して

$${}^g A = gAg^{-1} = \{gag^{-1} \mid a \in A\}$$

と定めれば G は G のべき集合 (部分集合の全体) 2^G に作用する。この作用による A の安定化部分群を A の**正規化群** (normalizer) といい $N_G(A)$ と表す。

$$N_G(A) = \{g \in G \mid {}^g A = A\} = \{g \in G \mid gAg^{-1} = A\} = \{g \in G \mid gA = Ag\}$$

である。明らかに $|A| = |{}^g A|$ である。

命題 3.4.6. $N_G(A) \leq G$ である。$H \leq G$ ならば $H \leq N_G(H) \leq G$ である。

証明. $N_G(A)$ は 2^G への G の作用についての安定化部分群であるから、G の部分群である。

$H \leq G$ とすると $h \in H$ に対して $hH = H = Hh$ なので $H \subset N_G(H)$ である。 □

命題 3.4.7. $H \leq G$ ならば ${}^g H \leq G$ である。

証明. $x, y \in {}^g H$ とする。ある $a, b \in H$ があって $x = gag^{-1}$, $y = gbg^{-1}$ と書くことができる。このとき

$$xy^{-1} = (gag^{-1})(gbg^{-1})^{-1} = gag^{-1}gb^{-1}g^{-1} = g(ab^{-1})g^{-1}$$

で $ab^{-1} \in H$ なので $xy^{-1} \in {}^g H$ である。 □

この命題の ${}^g H$ を H と**共役な部分群**という。これによって G はこの作用で G の部分群の全体にも作用することが分かる。すぐに分かるように $H \leq G$ のとき、$N_G(H) = G$ であることと $H \trianglelefteq G$ であることは同値である。また $H \leq N_G(H)$ であり $H \trianglelefteq N_G(H)$ である。

定理 3.4.8. $H \leq G$ に対して H と共役な G の部分群の個数は $|G : N_G(H)|$ である。

証明. H と共役な G の部分群の全体が、この作用による H を含む軌道となるので、定理 3.2.4 より明らかである。 □

演習問題

問 3.4.9. n を自然数とする。$\mathbb{Z}/n\mathbb{Z}$ を乗法に関するモノイドと見て、その単数群を G とする。

(1) $g \in G$ と $a+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ に対して、$g(a+n\mathbb{Z})$ を $ga+n\mathbb{Z}$ で定めれば、これは G の $\mathbb{Z}/n\mathbb{Z}$ への作用となることを示せ。

(2) $n = 5, 6, 8$ に対して (1) の作用を考え、その軌道を求めよ。

問 3.4.10. K を体とする。$V = K^n$ を K 上の n 次元列ベクトル全体のなすベクトル空間とする。一般線形群 $GL_n(K)$ は自然に V に左から作用する。このとき、この作用の軌道を求めよ。また、第一成分が 1 で他の成分がすべて 0 であるベクトル e に対し、e の $GL_n(K)$ における安定化部分群を求めよ。

問 3.4.11. 位数 8 の二面体群 $G = D_8 = \langle x, y \mid x^4 = y^2 = 1,\ yx = x^3y \rangle$ の共役類を求めよ。また、部分群 $H = \langle y \rangle$ に対して、その D_8 における正規化群 $N_G(H)$ を求めよ。

問 3.4.12. 4 次の交代群 A_4 について、以下の問いに答えよ。

(1) A_4 の共役類を求めよ。

(2) A_4 の類等式を書け。

(3) A_4 は位数 12 の部分群をもたないことを示せ。

問 3.4.13. 四元数群 Q_8 の共役類を求めよ。

問 3.4.14. p を素数とするとき、位数 p^2 の群はアーベル群であることを示せ。

問 3.4.15. G を n 次置換群とする。任意の $a_i, b_i \in \{1, \cdots, n\}$, $a_i \neq b_i$ $(i = 1, 2)$ に対して、ある $g \in G$ が存在して $g(a_1) = a_2$, $g(b_1) = b_2$ となるとき、G は 2 **重可移**であるという。(同様に t 重可移置換群も定義される。)

G を n 次可移置換群とし安定化部分群 $G_1 = \{\sigma \in G \mid \sigma(1) = 1\}$ を考える。G_1 は自然に $\{2, 3, \cdots, n\}$ に作用する。G が 2 重可移であることと G_1 の $\{2, 3, \cdots, n\}$ への作用が可移であることは同値であることを示せ。

Chapter 4

シローの定理

4.1 シローの定理

ここでは有限群論においてもっとも重要な定理の一つであるシロー (Sylow) の定理について説明する。

この章では p は常に素数を表すものとし、群は有限群のみを考える。いくつかの準備から始める。

補題 4.1.1. G を有限アーベル群とし、素数 p は G の位数を割り切ると仮定する。このとき G は位数 p の元をもつ。

証明. $|G|$ に関する帰納法で示す。$|G| = p$ のときは G は巡回群で、位数 p の元をもつ。

$|G| > p$ とする。$1 \neq g \in G$ とし、$n = o(g)$ とおく。$p \mid n$ ならば $o(g^{n/p}) = p$ である。$p \nmid n$ とする。このとき $H = \langle g \rangle$ とおくと $1 < H < G$ である。$p \nmid |H|$ なので $p \mid |G/H|$ である。$|G/H| < |G|$ かつ p は G/H の位数を割り切るので、帰納法の仮定が適用でき G/H には位数 p の元 $\overline{a}$ が存在する。$\overline{a}^{\ell} = \overline{1}$ となるための必要十分条件は $p \mid \ell$ なので、特に $a^{\ell} = 1$ ならば $p \mid \ell$ である。したがって $p \mid o(a)$ であり、このとき $o(a^{o(a)/p}) = p$ である。 □

補題 4.1.2. 有限群 G $(\neq 1)$ のすべての真の部分群の指数が p で割り切れるならば G の中心 $Z(G)$ の位数は p で割り切れる。特に、このとき $Z(G) \neq 1$ である。

証明. 類等式

$$|G| = |^G 1| + |^G x_1| + \cdots + |^G x_r|$$

を考える。$|^G x_i| = |G : C_G(x_i)|$ なので、仮定より $C_G(x_i) \neq G$ ならば $|^G x_i|$ は p で割り切れる。また $|G| = |G : 1|$ も p で割り切れる。$C_G(1) = G$ なので $|^G 1| = 1$ である。したがって、両辺を p で割って考えれば、p の倍数だけ $|^G x_i| = 1$ となる i がある。このとき $C_G(x_i) = G$ となり、したがって $x_i \in Z(G)$ であるから補題が成立する。 □

前に定義したように、位数が素数 p のべきである有限群を **p-群**という。有限群 G の部分群で p-群であるものを **p-部分群**という。

有限群 G の位数について $|G| = p^a q,\ p \nmid q$ であるとき、G の部分群でその位数が p^a であるものを G の**シロー p-部分群**という。部分群の位数は元の群の位数の約数なので、シロー p-部分群は、存在すれば位数が最大の G の p-部分群である。

定理 4.1.3 (シローの定理 (1))**.** p^r が有限群 G の位数を割り切るならば G は位数 p^r の部分群をもつ。特に G のシロー p-部分群が存在する。

証明. $|G|$ に関する帰納法で示す。$|G| = 1$ のときは明らかである。

$|G| > 1$ とし p^r が $|G|$ を割り切るものとする。$r = 0$ ならば自明なので $r > 0$ とする。もし G の真の部分群 H で指数 $|G : H|$ が p で割り切れないものがあれば、帰納法の仮定から H は位数 p^r の部分群をもち、それは G の部分群でもある。したがって、すべての真の部分群の指数は p で割り切れると仮定してよい。このとき補題 4.1.2 より $|Z(G)|$ は p で割り切れ、補題 4.1.1 より $Z(G)$ に位数 p の元 a がある。$N = \langle a \rangle$ とおくと $a \in Z(G)$ より $N \trianglelefteq G$ である。$|N| = p$ なので、剰余群 G/N の位数は p^{r-1} で割り切れる。G/N に帰納法の仮定を適用すれば G/N は位数 p^{r-1} の部分群 H/N をもつ。このとき $|H| = p^r$ であり、G は位数 p^r の部分群をもつ。 □

有限群 G のシロー p-部分群の全体の集合を $\mathrm{Syl}_p(G)$ と表す。任意の有限群 G と任意の素数 p に対して $\mathrm{Syl}_p(G) \neq \emptyset$ である。

定理 4.1.4 (シローの定理 (2))**.** G を有限群とする。

(1) $P \in \mathrm{Syl}_p(G)$ と G の任意の p-部分群 Q に対して、ある $g \in G$ が存在して $Q \leq {}^gP$ となる。

(2) $P, Q \in \mathrm{Syl}_p(G)$ ならば P と Q は共役である。

(3) $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$ である。

証明. (1) G の (Q, P)-両側剰余類分解を考える。命題 1.5.1 より

$$|G| = \sum_{i=1}^{r} |Qa_iP| = \sum_{i=1}^{r} |Q : Q \cap a_iPa_i{}^{-1}| \cdot |P|$$

である。また $|G| = |P| \cdot |G : P|$ で $P \in \mathrm{Syl}_p(G)$ より $|G : P| \not\equiv 0 \pmod{p}$ である。よって

$$0 \not\equiv |G : P| = \sum_{i=1}^{r} |Q : Q \cap a_iPa_i{}^{-1}| \pmod{p}$$

となる。ここで Q は p-群なので $|Q : Q \cap a_iPa_i{}^{-1}|$ は p-べきである。したがって、ある i について $|Q : Q \cap a_iPa_i{}^{-1}| = 1$ が成り立つ。これは $Q \leq a_iPa_i{}^{-1} = {}^{a_i}P$ を意味する。

(2) (1) を P, Q で考えれば $|Q| = |{}^gP|$ より $Q = {}^gP$ である。

(3) $N = N_G(P)$ とする。(2) より $|\mathrm{Syl}_p(G)| = |G : N|$ である。また $P \in \mathrm{Syl}_p(N)$ でもあり、N に (2) を適用すれば P は N に含まれる唯一の G のシロー p-部分群である。G の (P, N)-両側分解を

$$G = \bigcup_{j=1}^{\ell} Pb_jN$$

とし $b_1 = 1$ とする。元数については

$$|G : N| \cdot |N| = |G| = \sum_{j=1}^{\ell} |Pb_jN| = \sum_{j=1}^{\ell} |P : P \cap b_jNb_j{}^{-1}| \cdot |N|$$

が成り立っている。このとき $P \leq N$ より $|P : P \cap N| = 1$ である。また $|P : P \cap b_j N {b_j}^{-1}| = 1$ ならば ${b_j}^{-1} P b_j \leq N$ となるので、${b_j}^{-1} P b_j = P$、すなわち $b_j \in N$ となり、これは $j = 1$ のときに限る。したがって $j \neq 1$ に対して $|P : P \cap b_j N {b_j}^{-1}|$ は 1 でない p-べきとなる。

$$|G : N| = 1 + \sum_{j=2}^{\ell} |P : P \cap b_j N {b_j}^{-1}|$$

を考えれば $|\mathrm{Syl}_p(G)| = |G : N| \equiv 1 \pmod{p}$ である。 □

この定理から、位数が p-べきである元はあるシロー p-部分群に含まれることが分かる。特に G のシロー p-部分群が正規部分群ならば、それは G のただ一つのシロー p-部分群であり、G の位数が p-べきである元のすべてからなる。したがって正規シロー p-部分群は特性部分群となる。

系 4.1.5. p, q を素数とし $p < q, p \nmid q - 1$ とする。また $|G| = pq$ とする。このとき G は巡回群である。(例えば位数 15, あるいは 35 の群は巡回群である。)

証明. $P \in \mathrm{Syl}_p(G), Q \in \mathrm{Syl}_q(G)$ とする。$N = N_G(P)$ とすると $P \leq N \leq G$ より、$|N|$ は p の倍数で pq の約数である。したがって $|N| = p$ または pq である。$|N| = p$ とすると

$$|\mathrm{Syl}_p(G)| = |G : N| = q \not\equiv 1 \pmod{p}$$

でシローの定理に反する。よって $|N| = pq$、すなわち $N = G$ となり $P \trianglelefteq G$ である。同様にして $Q \trianglelefteq G$ も示される。以上より P, Q はそれぞれ G のただ一つのシロー p-部分群、シロー q-部分群である。

$1 \neq x \in G$ として x の位数 $o(x)$ を考える。$o(x)$ は $|G|$ の約数なので、$o(x) = 1$ なる元は単位元しかないことに注意して、$o(x) \in \{p, q, pq\}$ である。$o(x) = pq$ なる元 x が存在すれば $\langle x \rangle = G$ となるので、G は巡回群である。$o(x) = pq$ となる x が存在しないとする。$o(x) = p$ とすると $|\langle x \rangle| = p$ は p-群なので、あるシロー p-部分群に含まれるが、P がただ一つのシロー p-部分群なので $x \in P$ となる。したがって、この様な元は $p - 1$ 個しかない。同様に $o(x) = q$ となる元は $q - 1$ 個しかない。しかし、$p \geq 2, q \geq 2$ に注意して

$$1 + (p - 1) + (q - 1) = p + q - 1 < 2q \leq pq = |G|$$

なので、これは矛盾である。したがって $o(x) = pq$ なる元が存在し、G は巡回群となる。 □

系 4.1.6. $n \leq 7$ のとき、n 次対称群 S_n は位数 15 の部分群をもたない。

証明. 位数 15 の部分群があれば、それは巡回部分群で、したがって位数 15 の元が存在する。7 次以下のすべての置換の型を考えれば、定理 1.8.14 より、S_n $(n \leq 7)$ は位数 15 の元をもたないことが分かる。(S_8 には $[5, 3]$ という型の元があり、その位数は 15 である。) □

シローの定理には様々な応用があるが、ここで簡単な命題を一つ示す。

命題 4.1.7. G を有限群とする。p を素数とし $P \in \mathrm{Syl}_p(G)$ とする。G の部分群 H が $N_G(P)$ を含むとき $N_G(H) = H$ である。

証明. $N_G(H) \supset H$ は一般に成り立つ。

$x \in N_G(H)$ とする。${}^xH = H$ である。${}^xP \subset {}^xH = H$ なので、$P, {}^xP \in \mathrm{Syl}_P(H)$ である。シローの定理により P と ${}^xP$ は H で共役である。すなわち、ある $h \in H$ が存在して ${}^xP = {}^hP$ となる。このとき $h^{-1}x \in N_G(P) \subset H$ となるので $x \in hH = H$ である。よって $N_G(H) \subset H$ も成り立つ。 □

演習問題

問 4.1.8. $p = 2, 3, 5$ について、5 次対称群 S_5 のシロー p-部分群の位数を求めよ。またシロー p-部分群の個数の可能性を答えよ。

問 4.1.9. G を有限群、p を素数、$P \in \mathrm{Syl}_p(G)$ とする。P が G の正規部分群であるならば P は G の特性部分群であることを示せ。

問 4.1.10. p を素数、G を有限群、H は G の正規部分群、$P \in \mathrm{Syl}_p(H)$ とする。P が H の正規部分群であるならば P は G の正規部分群であることを示せ。

問 4.1.11. G を有限群とし H を G の正規部分群とする。p を素数とし $P \in \mathrm{Syl}_p(H)$ とする。このとき $G = HN_G(P)$ となることを示せ。

問 4.1.12. p を奇素数とするとき、位数 $2p$ の群は、巡回群 C_{2p} か二面体群 D_{2p} に同型であることを示せ。

問 4.1.13. p を素数とする。有限群 G の位数が p べきである元の全体が部分群をなすならば、それは G の正規シロー p-部分群であることを示せ。

Chapter 5

群の直積

5.1 外部直積

G, H を群とする。集合としての直積 $G \times H$ を考え、これに演算を

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

で定める。このとき、結合法則はみたされ、$(1_G, 1_H)$ が単位元、$(g, h)^{-1} = (g^{-1}, h^{-1})$ が成り立ち、$G \times H$ は群となる。これを G と H の (外部) **直積**という。三つ以上の群に対しても同様である。無限個の群に対しても直積は定義できるが、ここでは主に有限個の群の直積について考える。

$$\begin{aligned} G \times H &\cong H \times G, \\ G \times H \times K &\cong (G \times H) \times K \cong G \times (H \times K) \end{aligned}$$

が成り立つ。

問 5.1.1. 上の同型を確認せよ。

これによって複数の群の直積を考えるときには、その順序は重要ではない。そこで

$$\prod_{i=1}^{r} G_i, \quad \prod_{\lambda \in \Lambda} G_\lambda$$

のような記号も用いられる。

群の直積は、集合としては集合の直積なのでその位数 (濃度) について

$$\left| \prod_{i=1}^{r} G_i \right| = \prod_{i=1}^{r} |G_i|$$

が成り立つ。

群の直積 $G \times H$ において $G \times 1 = \{(g, 1_H) \mid g \in G\}$ を考えると、これは部分群となり、自然な対応で $G \times 1 \cong G$ である。これを同一視して $G \subset G \times H$ と見ることができる。$H \subset G \times H$ も同様である。このように見たとき、定義から以下のことが成り立つ。

(1) $G \times H$ において、G の元と H の元は可換である。

(2) $G \times H$ の任意の元は G の元と H の元の積として一意的に表される。

問 5.1.2. 上のことを証明せよ。

群の直積 $G = \prod_{i=1}^{r} G_i$ を考える。G の元は $g = (g_1, \cdots, g_r)$ $(g_i \in G_i)$ と一意的に表される。そこで

$$\pi_i : G \to G_i, \quad \pi_i(g) = g_i$$

なる写像を考えれば、これは全準同型となる。これを G から G_i への**射影**という。また、自然な埋め込み

$$\iota_i : G_i \to G, \quad \iota_i(g_i) = (1, \cdots, 1, g_i, 1, \cdots, 1)$$

は単準同型で、これを G_i から G への**入射**という。定義から明らかに

$$\begin{aligned} \pi_i \circ \iota_i(g_i) &= g_i, \\ (\iota_1 \circ \pi_1(g))(\iota_2 \circ \pi_2(g)) \cdots (\iota_r \circ \pi_r(g)) &= g \end{aligned}$$

が成り立つ。記号の乱用を許せば

$$\pi_i \circ \iota_i = id_{G_i}, \quad \prod_{i=1}^{r} (\iota_i \circ \pi_i) = id_G$$

である。

問 5.1.3. G, H を群とする。直積とその中心について

$$Z(G \times H) = \{(a, b) \mid a \in Z(G),\ b \in Z(H)\} \cong Z(G) \times Z(H)$$

となることを示せ。

5.2 内部直積

G を群とし、$H_1, H_2, \cdots, H_r$ を G の部分群とする。G が $H_1, H_2, \cdots, H_r$ の (内部) **直積**であるとは、以下の条件をみたすこととする。

(D1) $i \neq j$ のとき H_i の元と H_j の元は可換である。

(D2) 任意の G の元は $h_1 h_2 \cdots h_r$ $(h_i \in H_i)$ と一意的に表される。

このとき、外部直積の場合と同じ記号を用いて $G = H_1 \times \cdots H_r$ と表す。

命題 5.2.1. G が $H_1, H_2, \cdots, H_r$ の直積であることと、以下の三つの性質が成り立つことは同値である。

(E1) すべての i について $H_i \trianglelefteq G$ である。

(E2) $G = H_1 \cdots H_r$ である。

(E3) すべての i について $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_r) = 1$ である。

証明. G が $H_1, H_2, \cdots, H_r$ の直積であるとする。任意の G の元 g は $h_1 h_2 \cdots h_r$ $(h_i \in H_i)$ と書くことができる。ここで、任意の $f_i \in H_i$ について、

$$g f_i g^{-1} = h_1 h_2 \cdots h_r f_i {h_r}^{-1} \cdots {h_2}^{-1} {h_1}^{-1} = h_i f_i {h_i}^{-1} \in H_i$$

となるので $H_i \trianglelefteq G$ である。よって (E1) が成り立つ。任意の G の元が $h_1 h_2 \cdots h_r$ $(h_i \in H_i)$ と表されるので (E2) は成り立つ。$x \in H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_r)$ とする。このとき $x = h_1 \cdots h_{i-1} h_{i+1} \cdots h_r$ と書くことができて

$$x = 1_{H_1} \cdots 1_{H_{i-1}} x 1_{H_{i+1}} \cdots 1_{H_r} = h_1 \cdots h_{i-1} 1_{H_i} h_{i+1} \cdots h_r$$

となる。よって (D2) の記述の一意性より $x = 1$ となる。(E3) が成り立つ。

(E1), (E2), (E3) が成り立つとする。$i \neq j$ とする。$H_j \subset H_1 \cdots H_{i-1} H_{i+1} \cdots H_r$ なので $H_i \cap H_j = 1$ である。$h_i \in H_i$, $h_j \in H_j$ とする。このとき $h_i h_j {h_i}^{-1} {h_j}^{-1} = (h_i h_j {h_i}^{-1}) {h_j}^{-1} \in (h_i H_j {h_i}^{-1}) {h_j}^{-1} \subset H_j {h_j}^{-1} \subset H_j$ である。同様にして $h_i h_j {h_i}^{-1} {h_j}^{-1} \in H_i$ も成り立つ。よって $h_i h_j {h_i}^{-1} {h_j}^{-1} \in H_i \cap H_j = 1$ となり $h_i h_j {h_i}^{-1} {h_j}^{-1} = 1$ である。これは $h_i h_j = h_j h_i$ を意味し、(D1) が成り立つ。(E2) より、任意の G の元 g は $h_1 h_2 \cdots h_r$ $(h_i \in H_i)$ と表される。一意性を示すために $h_1 h_2 \cdots h_r = k_1 k_2 \cdots k_r$ $(h_i, k_i \in H_i)$ とする。このとき (D1) に注意すれば

$$1 = (h_1 h_2 \cdots h_r)(k_1 k_2 \cdots k_r)^{-1} = (h_1 {k_1}^{-1})(h_2 {k_2}^{-1}) \cdots (h_r {k_r}^{-1})$$

となる。よって (E3) より

$$k_1 {h_1}^{-1} = (h_2 {k_2}^{-1}) \cdots (h_r {k_r}^{-1}) \in H_1 \cap (H_2 \cdots H_r) = 1$$

となり $h_1 = k_1$ である。同様に $h_i = k_i$ がすべての i に対して成り立ち、記述の一意性が得られる。以上より (D2) が成り立つ。 □

群 G が部分群 H, K の直積として $G = H \times K$ と表されるとき、H (または K) を G の**直積因子**という。直積因子が自明なもの、すなわち G と 1、しかないとき G は**直既約** (indecomposable) であるという。直既約でないとき**直可約** (decomposable) であるという。

群 G が、群 $H_1, \cdots, H_r$ の外部直積であるとき、前述のように H_i を G の部分群と考えると、$H_1, \cdots, H_r$ は内部直積の条件をみたし、G はこれらの部分群の内部直積となる。したがって、その意味を十分に理解していれば、内部直積と外部直積はほぼ同じように扱うことができる。

例 5.2.2. $G = \langle a \mid a^6 = 1 \rangle$ とし、$H = \langle a^2 \rangle$, $K = \langle a^3 \rangle$ とする。G, H, K はそれぞれ位数 6, 3, 2 の巡回群で

$$H = \{1, a^2, a^4\}, \quad K = \{1, a^3\}$$

である。このとき $G = H \times K$ である。したがって $C_6 \cong C_3 \times C_2$ である。

この例より一般に次の命題が成り立つ。

命題 5.2.3. 互いに素な自然数 m, n に対して $C_{mn} \cong C_m \times C_n$ が成り立つ。

証明. $C_{mn} = \langle a \rangle, C_m = \langle b \rangle, C_n = \langle c \rangle$ とおく。$f : C_{mn} \to C_m \times C_n$ を $f(a^i) = (b^i, c^i)$ と定めれば、これは群準同型となる。$f(a^i) = (b^i, c^i) = 1$ と仮定すると i は m と n の公倍数で、したがって最小公倍数 mn の倍数となる。よって、このとき $a^i = 1$ で、$\mathrm{Ker} f = 1$ となる。すなわち f は単射となるが $|C_{mn}| = mn = |C_m \times C_n|$ なので、f は全単射となる。よって f は同型である。 □

例 5.2.4. p を素数とする。G を n 個の巡回群 C_p の直積とする。このような G を**基本可換 (p-) 群**という。基本可換 p-群は有限体 $GF(p)$ 上 n 次元ベクトル空間を加法群と見たものと同型である。

演習問題

問 5.2.5. $C_6 \times C_4 \cong C_{12} \times C_2$ を示せ。

問 5.2.6. C_4 と $C_2 \times C_2$ は同型ではないことを示せ。

問 5.2.7. $(g, h) \in G \times H$ とし、$g \in G$ と $h \in H$ は共に位数が有限であるとする。このとき (g, h) の位数は有限で、$o(g)$ と $o(h)$ の最小公倍数となることを示せ。

問 5.2.8. 交換子群について $D(G \times H) = D(G) \times D(H)$ を示せ。これを使って、G と H がそれぞれ可解群であるならば $G \times H$ も可解群であることを示せ。

Chapter 6

有限生成アーベル群

アーベル群は交換法則をみたす演算をもつ群であり、一般の群と比べて扱いやすいものである。しかし一般のアーベル群の構造を考えることは難しい。ここでは有限生成アーベル群に限って考え、基本的かつ重要な「有限生成アーベル群の基本定理」を解説することを目標とする。

6.1 有限アーベル群

次の「有限アーベル群の基本定理」を示すことがこの節の目標である。

定理 6.1.1 (有限アーベル群の基本定理)**.** 有限アーベル群はいくつかの巡回群の直積

$$C_{e_1} \times C_{e_2} \times \cdots \times C_{e_r}$$

と同型である。ここで $e_{i+1} \mid e_i$ $(i = 1, 2, \cdots, r-1)$, $e_i > 1$ $(i = 1, 2, \cdots, r)$ とすることができ、この仮定の下で、数列 $\{e_i\}$ は一意的である。

簡単な例を見てみよう。例えば、位数 12 の有限アーベル群を分類することを考える。定理 6.1.1 によって、巡回群の直積 $C_{e_1} \times C_{e_2} \times \cdots \times C_{e_r}$ と書くことができ、位数を見れば $\prod_{i=1}^{r} e_i = 12$ である。$e_{i+1} \mid e_i$ に注意すれば、このような数列は

$$\{12\}, \quad \{6, 2\}$$

以外にはないことが分かる。したがって位数 12 の有限アーベル群は

$$C_{12}, \quad C_6 \times C_2$$

のいずれかと同型である。

問 6.1.2. 位数 16, 36 の有限アーベル群を分類せよ。

定理 6.1.1 の証明のためにいくつかの準備をする。まずは p-群に対してのみ定理を示す。

補題 6.1.3. p を素数とする。a をアーベル p-群 G の位数最大の元とするとき、G のある部分群 H があって $G = \langle a \rangle \times H$ となる。

証明. G をアーベル p-群とする。a を G の位数最大の元とする。G のある部分群 H があって $G = \langle a \rangle \times H$ となることを G の位数に関する帰納法を用いて示す。$G = 1$ ならば主張は明らかなので $G \neq 1$ とする。

$G = \langle a \rangle$ ならば $H = 1$ として主張は成り立つので、$G \neq \langle a \rangle$ とし、$b \notin \langle a \rangle$ とする。剰余群 $G/\langle a \rangle$ を考えれば、これも p-群なので $o(b\langle a \rangle)$ は p-べきで $o(b\langle a \rangle) = p^s$ とおくことができる。このとき $c = b^{(p^{s-1})}$ とおくと $o(c\langle a \rangle) = p$ である。よって $c \notin \langle a \rangle$, $c^p \in \langle a \rangle$ である。このとき $c^p = a^m$ と書くことが出来るが、もし $p \nmid m$ とすると $o(a^m) = o(a)$ となり、よって $o(c) = p \cdot o(a) > o(a)$ となる。これは $o(a)$ の最大性に反するので $p \mid m$ である。$m = m'p$ とおく。$d = ca^{-m'}$ とおく。このとき $d \notin \langle a \rangle$ で $d^p = 1$ が成り立つ。$\langle d \rangle$ の位数が素数であることから $\langle d \rangle \cap \langle a \rangle = 1$ である。

自然な全射 $\pi : G \to G/\langle d \rangle$ を考える。π を $\langle a \rangle$ に制限すれば、これは単射となるので $|\pi(\langle a \rangle)| = |\langle \pi(a) \rangle| = |\langle a \rangle|$ である。したがって $\pi(a)$ は $G/\langle d \rangle$ の位数最大の元である。ここで帰納法の仮定から、$G/\langle d \rangle$ のある部分群 U が存在して $G/\langle d \rangle = \langle \pi(a) \rangle \times U$ となる。

$U' = \pi^{-1}(U)$ とおいて $G = \langle a \rangle \times U'$ となることを示す。G はアーベル群なので $\langle a \rangle \trianglelefteq G$, $U' \trianglelefteq G$ であることは明らかである。$x \in \langle a \rangle \cap U'$ とすると、$\pi(x) \in \langle \pi(a) \rangle \cap U = 1$ である。よって $x \in \langle a \rangle \cap \mathrm{Ker}\pi = 1$ となり $\langle a \rangle \cap U' = 1$ である。$g \in G$ とする。$\pi(g) = \pi(a)^i u$ となる整数 i と $u \in U$ がある。π が全射であることから $u' \in U'$ で $\pi(u') = u$ なるものがある。このとき $\pi(a^i u') = \pi(a)^i u = \pi(g)$ より $g \in a^i u' \langle d \rangle$ なので $g \in a^i u' d^j$ となる整数 j がある。$\pi(d^j) = 1 \in U$ なので $u' d^j \in U'$ となり、$G = \langle a \rangle U'$ である。以上より $G = \langle a \rangle \times U'$ となる。 □

補題 6.1.4. p を素数とする。アーベル p-群はいくつかの巡回群の直積と同型である。

証明. G をアーベル p-群とし、a を G の位数最大の元とする。補題 6.1.3 より $G = \langle a \rangle \times H$ なる部分群 H が存在し、H もアーベル p-群である。これを繰り返せば G は巡回群の直積と同型となる。 □

補題 6.1.5. 有限アーベル群はいくつかの巡回群の直積と同型である。

証明. $p_1, \cdots, p_\ell$ を $|G|$ を割り切る素因数のすべてであるとし、$P_i \in \mathrm{Syl}_{p_i}(G)$ とする。このとき $G = \prod_{i=1}^{\ell} P_i$ が成り立つことがすぐに分かる。補題 6.1.4 より各 P_i は巡回群の直積であり、よって G も巡回群の直積となる。 □

問 6.1.6. 上の証明で $G = \prod_{i=1}^{\ell} P_i$ となることを確認せよ。

補題 6.1.7. 有限アーベル群 G は

$$C_{e_1} \times C_{e_2} \times \cdots \times C_{e_r}$$

で $e_{i+1} \mid e_i$ $(i = 1, 2, \cdots, r-1)$ をみたすように表すことができる。

証明. 補題 6.1.5 の証明のように、$p_1, \cdots, p_\ell$ を $|G|$ を割り切る素因数のすべてであるとし、$P_i \in \mathrm{Syl}_{p_i}(G)$ とする。各 P_i を巡回群の直積として

$$C_{f_{i,1}} \times C_{f_{i,2}} \times \cdots \times C_{f_{i,\ell(i)}}$$

と表す。ここで各 $f_{i,j}$ は p_i のべきなので、$f_{i,1} \geq f_{i,2} \geq \cdots \geq f_{i,\ell(i)}$ としておけば $f_{i,j+1} \mid f_{i,j}$ である。$\ell(i)$ $(i = 1, 2, \cdots, r)$ のうち、最大のものを ℓ とし、$\ell(i) < \ell$ なる i については $f_{i,\ell(i)+1} = \cdots = f_{i,\ell} = 1$ を補って、長さを一定にしておく。

$G_j = \prod_{i=1}^r C_{f_{i,j}}$ とおくと、直積因子の巡回群の位数が互いに素であることから G_j は位数 $\prod_{i=1}^r f_{i,j}$ の巡回群に同型である。また、各 i について $f_{i,j+1} \mid f_{i,j}$ なので $|G_{j+1}|$ は $|G_j|$ の約数である。よって $G = G_1 \times \cdots \times G_\ell$ が求める条件をみたす分解である。 □

補題 6.1.8. 有限アーベル群 G を補題 6.1.7 のように表すとき、数列 $e_1, \cdots, e_r$ は一定である。

証明. 一意性を示すために

$$\begin{aligned} G &\cong C_{e_1} \times C_{e_2} \times \cdots \times C_{e_r} \\ &\cong C_{f_1} \times C_{f_2} \times \cdots \times C_{f_s} \end{aligned}$$

で $e_{i+1} \mid e_i$ $(i = 1, 2, \cdots, r-1)$, $f_{j+1} \mid f_j$ $(j = 1, 2, \cdots, s-1)$ とする。自然数 m に対して

$$(G, m) = \{g \in G \mid g^m = 1\}$$

とおく。$a = (a_1, \cdots, a_r) \in C_{e_1} \times \cdots \times C_{e_r}$ に対して $a \in (G, m)$ であることと、各 i について $a_i \in (C_{e_i}, m)$ となることは同値である。また、巡回群に対しては $|(C_n, m)| = \gcd(m, n)$ である。

自然数 m に対して、$S(m)$ で、$m \mid e_i$ なる i の数を、$T(m)$ で、$m \mid f_j$ なる j の数を表すものとする。$e_{i+1} \mid e_i$ という仮定から、$i < j$ で $m \mid e_j$ ならば $m \mid e_i$ であることに注意しておく。f_i についても同様である。

p を素数とする。(G, p) を考えると、上記のことから $|(G, p)| = p^{S(p)} = p^{T(p)}$ である。よって $S(p) = T(p)$ が成り立つ。また

$$|(G, p^2)| = p^{2S(p^2)} + p^{S(p)} = p^{2T(p^2)} + p^{T(p)}$$

となるので、$S(p^2) = T(p^2)$ も成り立つ。同様に繰り返して、任意の ℓ に対して $S(p^\ell) = T(p^\ell)$ である。$e_{i+1} \mid e_i$, $f_{j+1} \mid f_j$ に注意すれば、$p^\ell \mid e_i$ と $p^\ell \mid f_i$ が同値になることが分かる。

上記のことがすべての素数 p に対して成り立つので、$e_i = f_i$ となる。 □

以上の補題を合わせて定理 6.1.1 は証明される。

6.2 有限生成アーベル群

この節では必要な定義を与え、「有限生成アーベル群の基本定理」を紹介する。($^{(*)}$ の付いている部分は、講義の際には省略して結果のみを紹介する場合もある。)

ここではアーベル群の演算を加法的に表すことにする。この場合、直積を**直和**といい、アーベル群 A と B の直和を $A \oplus B$ で表す。(正確には直和と直積は厳密に区別されるものであるが、ここで用いる範囲では同じものと思っても構わない。) 演算を加法的に書く場合、無限位数巡回群は $\mathbb{Z}$、有限位数 n の巡回群は $\mathbb{Z}/n\mathbb{Z}$ と同型になるので、これらの表記を用いる。

6.2.1 有限生成自由アーベル群

有限個の無限位数巡回群 $\mathbb{Z}$ の直和に同型な群

$$F \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

を**有限生成自由アーベル群** という。このときの直和因子の個数を F の**階数**、または**ランク**という。

命題 6.2.1. 有限生成自由アーベル群の階数はその分解によらず一定である。

証明. $F = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_r$ を有限生成自由アーベル群とする。$2F = \{2f \mid f \in F\}$ とおくと $2F$ は F の部分群である。剰余群 $F/2F$ を考えると、

$$F/2F \cong \mathbb{Z}x_1/2\mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_r/2\mathbb{Z}x_r \cong \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z}$$

が成り立ち、特に $|F/2F| = 2^r$ となる。$|F/2F|$ は F の分解の仕方によらないから、階数 r は一定である。 □

補題 (*) **6.2.2.** $f : A \to F$ をアーベル群 A から有限生成自由アーベル群 F への全準同型とする。このとき $B = \mathrm{Ker}f$ とおけば、B は A の直和因子である。

証明. $F = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_r$ とする。各 x_i に対して $f(c_i) = x_i$ となる $c_i \in A$ が存在する。$C = \mathbb{Z}c_1 + \cdots + \mathbb{Z}c_r$ とおいて $A = B \oplus C$ となることを示す。

$a \in A$ とする。$f(a) = \sum_{i=1}^{r} k_i x_i$ と書くことができて、このとき $c = \sum_{i=1}^{r} k_i c_i$ とおけば $f(c) = f(a)$ である。$a = (a - c) + c$ であって $f(a - c) = f(a) - f(c) = 0$ より $a - c \in B$ で $c \in C$ となるので $a \in B + C$ である。よって $A = B + C$ である。

$b \in B \cap C$ とする。$c \in C$ なので $c = \sum_{i=1}^{r} k_i c_i$ と書くことができて、このとき $c \in B$ より $0 = f(c) = \sum_{i=1}^{r} k_i x_i$ である。F は自由群なので $k_1 = \cdots = k_r = 0$ となり $c = 0$ である。よって $B \cap C = 0$ となり $A = B \oplus C$ である。 □

命題 6.2.3. 有限生成自由アーベル群 F の部分群 A は、また有限生成自由アーベル群で、A の階数は F の階数以下である。

証明 (*)**.** $F = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_r$ とし、F の階数 r に関する帰納法によって命題を示す。まず $r = 1$ の場合は、0 でない任意の部分群は無限位数巡回群となるので命題は成り立つ。

$r > 1$ とする。$a \in A$ は $a = \sum_{i=1}^{r} a_i x_i$ と書くことが出来るので、準同型 $f : A \to \mathbb{Z}x_r$ を $f(a) = a_r x_r$ で定める。$\mathrm{Im}f = 0$ ならば $A \subset \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_{r-1}$ となるので、帰納法の仮定から A は階数が $r - 1$ 以下の自由アーベル群である。$\mathrm{Im}f \neq 0$ とする。このとき、ある $0 \neq m \in \mathbb{Z}$ が存在して $\mathrm{Im}f = m\mathbb{Z}x_r$ となる。これは有限生成自由アーベル

群だから、$f : A \to m\mathbb{Z}x_r$ と見て、補題 6.2.2 を適用すれば、$A = \mathrm{Ker}f \oplus C$ となる部分群 C が存在する。$C \cong A/\mathrm{Ker}f \cong \mathrm{Im}f = m\mathbb{Z}x_r$ は $\mathbb{Z}$ と同型である。f の定義より $\mathrm{Ker}f \subset \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_{r-1}$ となるので、帰納法の仮定から B は階数が $r-1$ 以下の自由アーベル群である。したがって A は階数が r 以下の自由アーベル群である。 □

6.2.2 トーション部分群

A をアーベル群とする。$T(A)$ で A の位数有限な元の全体を表すことにすると、これは A の部分群となる。これを A の**トーション部分群**、または**ねじれ部分群**という。$T(A) = 0$ であるとき A は**トーション (ねじれ) のないアーベル群**であるという。

命題 6.2.4. アーベル群 A に対して、剰余群 $A/T(A)$ はトーションのないアーベル群である。

証明. $a \in A$ とし $\overline{a} \in T(A/T(A))$ とする。ある $0 \neq m \in \mathbb{Z}$ が存在して $m\overline{a} = \overline{0}$ である。このとき $ma \in T(A)$ である。よって、ある $0 \neq n \in \mathbb{Z}$ が存在して $0 = n(ma) = (nm)a$ となる。したがって $a \in T(A)$ となり $\overline{a} = \overline{0}$ である。 □

補題 (*) **6.2.5.** 有限生成アーベル群の部分群は有限生成である。

証明. A を有限生成アーベル群とし、生成系を $a_1, \cdots, a_r$ とする。$A = \sum_{i=1}^{r} \mathbb{Z}a_i$ である。$F = \bigoplus_{i=1}^{r} \mathbb{Z}x_i$ を $x_1, \cdots, x_r$ を生成系とする自由アーベル群とし、$\pi : F \to A$ を $f(\sum_{i=1}^{r} k_i x_i) = \sum_{i=1}^{r} k_i a_i$ で定めれば、これは全準同型である。

B を A の部分群とする。$\pi^{-1}(B)$ は F の部分群で、よって命題 6.2.3 より有限生成自由アーベル群である。$y_1, \cdots, y_s$ を $\pi^{-1}(B)$ の生成系とすれば B は $\pi(y_1), \cdots, \pi(y_s)$ で生成され、よって有限生成である。 □

命題 6.2.6. 有限生成アーベル群 A に対して、$T(A)$ は有限アーベル群である。

証明 (*)**.** 補題 6.2.5 より $T(A)$ は有限生成である。$a_1, \cdots, a_r$ を $T(A)$ の生成系とする。このとき $T(A)$ の任意の元は $\sum_{i=1}^{r} k_i a_i$ $(k_i \in \mathbb{Z})$ と表されるが、a_i の位数を n_i $(< \infty)$ とすれば、$0 \leq k_i < n_i$ とすることができ、よって有限個の元しなかいことが分かる。 □

命題 (*) **6.2.7.** 有限生成でトーションのないアーベル群は自由アーベル群である。

証明. A をトーションのない有限生成アーベル群とする。$x_1, \cdots, x_r$ を A の生成系とする。$x_1, \cdots, x_r$ の部分集合 $y_1, \cdots, y_m$ で、$\sum_{i=1}^{m} \mathbb{Z}y_i = \bigoplus_{i=1}^{m} \mathbb{Z}y_i$ となるようなものを考え、そのうち、一番個数の多いものを考える。適当に番号を付け替えれば、それを $x_1, \cdots, x_m$ としてよい。また $B = \bigoplus_{i=1}^{m} \mathbb{Z}x_i$ とおく。

剰余群 A/B を考える。A/B は $\overline{x_1}, \cdots, \overline{x_r}$ で生成されるが、$1 \leq i \leq m$ に対しては $x_i \in B$ なので $\overline{x_i} = \overline{0}$ である。よって A/B は $\overline{x_{m+1}}, \cdots, \overline{x_r}$ で生成される。もし、ある j $(m + a \leq j \leq r)$ に対して $\overline{x_j}$ の位数が無限であるならば、$\mathbb{Z}x_j \cap B = 0$ となるので $\sum_{i=1}^{m} \mathbb{Z}x_i + \mathbb{Z}x_j = \bigoplus_{i=1}^{m} \mathbb{Z}x_i \oplus \mathbb{Z}x_j$ となり、個数の最大性に反する。よって $\overline{x_j}$ $(m+a \leq j \leq r)$ は有限位数をもつ。$\overline{x_j}$ $(m+a \leq j \leq r)$ の位数の最小公倍数を ℓ とする。このとき A/B の任意の元は ℓ 倍すれば $\overline{0}$ になる。よって A の部分群 $A^{(\ell)} = \{a^\ell \mid a \in A\}$ を考えれば、$A^{(\ell)} \leq B$ となる。B は有限生成自由アーベル群なので、命題 6.2.3 より $A^{(\ell)}$ も有限生成自由アーベル群である。

準同型 $f : A \to A^{(\ell)}$ を $f(a) = a^\ell$ で定める。f は全射であり、また A が自由アーベル群であることから単射である。よって $A \cong A^{(\ell)}$ が成り立ち A は自由アーベル群である。 □

6.2.3 有限生成アーベル群の基本定理

定理 6.2.8 (有限生成アーベル群の基本定理)**.** A を有限生成アーベル群とする。このとき

$$A = F \oplus T(A)$$

で F は有限生成自由アーベル群、$T(A)$ は有限アーベル群と書くことができる。ここで F の階数は分解によらず一定であり、$T(A)$ に対しては有限アーベル群の基本定理のような分解が一定に定まる。

証明$^{(*)}$**.** $A/T(A)$ はトーションのない有限生成アーベル群なので、命題 6.2.7 より自由アーベル群である。$f : A \to A/T(A)$ を自然な全準同型とすると $\mathrm{Ker} f = T(A)$ で、補題 6.2.2 より $A = T(A) \oplus B$ となる B が存在する。このとき $B \cong A/T(A)$ であるから、B は有限生成自由アーベル群である。命題 6.2.6 より $T(A)$ は有限アーベル群なので主張が成り立つ。 □

この定理の F を A の**自由部分**、$T(A)$ を A の**トーション部分**ともいう。これによって有限生成アーベル群は

$$\mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}/e_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/e_r\mathbb{Z}$$

で $e_{i+1} \mid e_i$ となるように書くことができ、分解は一意的ではないが、この形は一定となる。

A のトーション部分群 $T(A)$ は位数有限な元のすべてであるから A の特性部分群となる。しかし自由部分は一意的に定まるものではない。

演習問題

問 6.2.9. 位数 18, 24, 30 の有限アーベル群を分類せよ。

問 6.2.10. $C_4 \times C_6 \times C_{10}$ を有限アーベル群の基本定理の形、すなわち $C_{e_1} \times \cdots \times C_{e_r}$ で $e_{i+1} \mid e_i$ $(i = 1, 2, \cdots, r-1)$ をみたすようなの形、に書け。

問 6.2.11. p を素数とするとき、位数 p^2 の群を分類せよ。

問 6.2.12. p を素数とするとき、位数 p^3 のアーベル群を分類せよ。

問 6.2.13. $A = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ とし、その元を (a, b) $(a \in \mathbb{Z},\ b \in \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\})$ と表す。$x = (1, \overline{1})$, $y = (0, \overline{1})$ とすると $A = \langle x \rangle \oplus \langle y \rangle$ であることを示せ。(この例から有限生成アーベル群の自由部分が一意的でないことが分かる。)

参考文献

[1] 代数概論, 森田康夫, 裳華房

[2] 代数学, 永尾汎, 朝倉書店

Akihide Hanaki (hanaki@math.shinshu-u.ac.jp)
2011/02/08

索引

2 重可移, 34
G-軌道, 29
G-集合, 27
n 次置換群, 28
p-群, 33
p-部分群, 35

アーベル群, 7
安定化部分群, 29

位数, 7, 10
一般線形群, 14

オイラー関数, 26

可移, 30
階数, 46
外部自己同型群, 25
可解群, 26
可換群, 7
可換半群, 7
可換モノイド, 7
核, 20
型, 16
加法群, 7

奇置換, 16
軌道, 29
基本可換群, 42
基本関係式, 13
逆元, 7
共役, 31
共役な部分群, 33
共役類, 32

偶置換, 16
クラインの四元群, 18
群, 7
群準同型, 19

結合法則, 7

語, 12
交換子, 26
交換子群, 26
交換法則, 7
交代群, 16
恒等置換, 15
互換, 15

サイクル, 15
作用, 27
作用で閉じている, 30

四元数群, 18
自己同型, 24
自己同型群, 24
指数, 9
自然な全準同型, 21
自明な作用, 28
自明な部分群, 8
射影, 40
自由群, 12
自由部分, 48
巡回群, 13
巡回置換, 15
巡回部分群, 10
準同型, 19
準同型定理, 22
剰余群, 12
剰余類, 10
シロー p-部分群, 35
シローの定理, 36

正規化群, 33

正規部分群, 10
生成系, 13
生成される部分群, 9
正則 G-集合, 30
正則元, 7
全行列環, 14
全準同型, 20

像, 20

対称群, 15
単位元, 7
単元, 7
単元群, 17
単純群, 16
単準同型, 20
単数, 7

置換, 15
置換群, 28
置換表現, 28
忠実, 28
中心, 9
中心化群, 31, 32
直積, 39, 40
直積因子, 41
直和, 46
直可約, 41
直既約, 41
直交行列, 14
直交群, 14

同型, 20, 30, 31
同型写像, 20
同型定理, 23
トーションのないアーベル群, 47
トーション部分, 48
トーション部分群, 47
特殊線形群, 14
特性部分群, 25

内部自己同型, 24
内部自己同型群, 24
長さ, 15

二項演算, 7
二面体群, 13
入射, 40

ねじれ部分群, 47

半群, 7
半直積, 26

左剰余類, 9
左剰余類分解, 9

符号, 16
部分群, 8

右剰余類, 10
右剰余類分解, 10

無限群, 7
無限巡回群, 12

モノイド, 7

有限アーベル群の基本定理, 43
有限群, 7
有限生成アーベル群の基本定理, 48
有限生成自由アーベル群, 46
ユニタリー行列, 14
ユニタリー群, 14

ラグランジェ, 9
ランク, 46

両側剰余類, 11
両側剰余類分解, 11

類等式, 32