代数学C / 代数学特論III

§1. 群

§1.1 モノイドと群の定義

Sを空でない集合とする. S上の**演算**とは, 写像 $S\times S \xrightarrow{f} S$ のことをいう.
例えば, $\mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ $(x,y)\longmapsto x+y$ は $\mathbb{Z}$ 上の演算である.

$x,y\in S$ について, $f(x,y)$ を単に $x\cdot y$ あるいは xy と書くことが多い.

定義 1.1.1. (半群) 空でない集合 G に演算 $\cdot$ が定まるとする. 任意の G の元 x,y,z に対し, $x\cdot(y\cdot z)=(x\cdot y)\cdot z$ が成り立つときに, $(G,\cdot)$ は**半群**であるという.

上の条件は**結合測**とよばれる. 半群において, 上の元を単に $x\cdot y\cdot z$ と書き, 矛盾なく定義されている.
同様に, $x_1,\dots,x_n\in G$ に対して, $x_1\cdots x_n$ は一意的に定まる.

半群 G において, 元 $e\in G$ が**単位元**であるとは, 任意の $x\in G$ に対して, $x\cdot e=e\cdot x=x$ が成り立つことをいう.

補題 1.1.2. e と e' を半群 G の単位元とする. このとき $e=e'$ である.

証明: $e=e\cdot e'=e'$ となる. □

定義 1.1.3. (モノイド) 単位元をもつ半群は**モノイド**とよぶ.

G をモノイドとし, G の単位元を e とおく. また, x を G の元とする.
元 $y\in G$ が x の**逆元**であるとは, $x\cdot y=y\cdot x=e$ が成り立つことをいう.
逆元をもつ元は**可逆元**とよばれる.

補題 1.1.4. y,y' を x の逆元とする. このとき, $y=y'$ である.

証明: $y=y\cdot e=y\cdot(x\cdot y')=(y\cdot x)\cdot y'=e\cdot y'=y'$. □

注意 1.1.5
(i) x が可逆元であるときに, x の逆元を x^{-1} で表す.
(ii) e は常に可逆元であり, $e^{-1}=e$ である.
(iii) x が可逆元ならば, x^{-1} も可逆元であり, $(x^{-1})^{-1}=x$ が成り立つ.
(iv) x,y が可逆元ならば, xy も可逆元であり, $(xy)^{-1}=y^{-1}x^{-1}$ である.

例 1.1.6.

- $(\mathbb{N}, +)$ はモノイドであり，可逆元全体は $\{0\}$ である
- $(\mathbb{Z}, \times)$ ―――――― $\{-1, 1\}$ ――
- X を集合とし，$Map(X,X)$ を写像 $X \to X$ 全体のなす集合とする．写像の合成に関してモノイドであり，可逆元全体は全単射である．
- モノイド $(M_n(\mathbb{C}), \times)$ の可逆元全体は $GL_n(\mathbb{C})$ である．

x をモノイド G の元とする．非負整数 n に対して，$x^n = \begin{cases} e & \text{if } n=0 \\ \underbrace{x \cdots x}_{n\text{個}} & \text{if } n>0 \end{cases}$
x が可逆元ならば，$x^n = (x^{-1})^n$ $(n>0)$ と定義する．

定義 1.1.7 (群) 任意の元が可逆元であるようなモノイドは**群**とよばれる．

ただ一つの元からなる群は**自明群**とよぶ．つまり，$G = \{e\}$ $(e$: 単位元$)$ である．

命題 1.1.8. H をモノイドとする．H の可逆元全体の集合は，H の演算に関して群をなす．

証明：$G = \{H$ の可逆元$\}$ とおく．
注意 1.1.5 (iv) より，G は H の演算について閉じている．
(ii) より，$e \in G$ である．
(iii) より，$x \in G \Rightarrow x^{-1} \in G$．
よって，G は群となる． □

定義 1.1.9 (可換モノイド，可換群，アーベル群) モノイド G において，任意の元 x, y に対して
$xy = yx$ が成り立つならば，G は**可換モノイド**であるという．群の場合は，**可換群**あるいは**アーベル群**という．

例 1.1.10

- n を自然数とすると，$(\mathbb{Z}/n\mathbb{Z}, +)$ はアーベル群である．(剰余類群)
- ―――――― $(\mathbb{Z}/n\mathbb{Z}, \times)$ は可換モノイドである $(\bar{0}$ は可逆元でない$)$
- $(\{z \in \mathbb{C} \mid |z|=1\}, \times)$ はアーベル群である．
- X を集合とし，X のべき集合を $\mathcal{P}(X)$ とおく．$A, B \in \mathcal{P}(X)$ に対して，$A \triangle B = (A \cup B) \setminus (A \cap B)$ と定義すると，$(\mathcal{P}(X), \triangle)$ がアーベル群となる．

注意 1.1.11
可換モノイド・アーベル群において，演算を $+$ で表すことが多い．この記合を使用するとき，合わせて
単位元 を 0 で，
x の逆元 を $-x$ で，
x の n 乗 を nx で表す．

定義 1.1.12 (直積)
G_1, G_2 を群とする．集合 $G_1 \times G_2$ に演算を $(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2')$ として定義する．
この演算に関して $G_1 \times G_2$ は群をなし，G_1 と G_2 の直積とよばれる．

§1.2. 部分群

定義 1.2.1(部分モノイド) G はモノイドで，G の部分集合 H は**部分モノイド**であるとは，以下が成り立つことをいう．

(i) $e \in H$

(ii) $x, y \in H \Rightarrow xy \in H$

定義 1.2.2(部分群) G を群とし，$H \subset G$ を部分集合とする．H が**部分群**であるとは，以下が成り立つことをいう．

(i) $e \in H$

(ii) $x, y \in H \Rightarrow xy \in H$

(iii) $x \in H \Rightarrow x^{-1} \in H$．

補題 1.2.3 G は群で，$H \subset G$ を部分集合とする．次の条件は互いに同値である

(i) H は G の部分群である．

(ii) H は空でなく，かつ $x, y \in H \Rightarrow xy^{-1} \in H$ が成り立つ．

証明：(i) $\Rightarrow$ (ii) は簡単である．

(ii) $\Rightarrow$ (i)：$H \neq \emptyset$ より，$x \in H$ がとれる．仮定より $xx^{-1} = e \in H$ である．

また，$x \in H$ に対して，$e \cdot x^{-1} = x^{-1} \in H$ となる．

最後に，$x, y \in H$ に対して，$x(y^{-1})^{-1} = xy \in H$ が成り立つ．

以上より H は部分群である．

Hが群$(G,\cdot)$の部分群であるときに，演算$\cdot$に関して閉じており，さらに$(H,\cdot)$は群となる．

例 1.2.4
- $(\mathbb{N},+)$は$(\mathbb{Z},+)$の部分モノイドである．
- nは自然数で，dをnの約数とする．$d\mathbb{Z}/n\mathbb{Z} = \{kd+n\mathbb{Z} \mid k\in\mathbb{Z}\}$は$\mathbb{Z}/n\mathbb{Z}$の部分群である．
- Gを群とする．$\{e\}$とGはGの部分群であり，自明な部分群とよばれる．

補題 1.2.5 Gを群とし，$\{H_i\}_{i\in I}$ $(I\neq\emptyset)$をGの部分群の族とする．共通部分$H=\bigcap_{i\in I} H_i$はGの部分群である．

証明: $\forall i\in I,\ e\in H_i$ より $e\in H$．
$x,y\in H$に対して，$xy^{-1}\in H_i$ $(\forall i\in I)$であるので，$xy^{-1}\in H$．よって，Hは部分群である． □

定義 1.2.6 (部分集合で生成される部分群) Gを群とし，$S\subset G$を部分集合とする．

Sで生成される部分群は$\langle S\rangle$で表し，次のように定義される：
$$\langle S\rangle = \bigcap_{\substack{H:\text{部分群}\\ S\subset H}} H .$$

つまり，$\langle S\rangle$はSを含むGの部分群全体のなす族の共通部分である．

注意 1.2.7
(i) GはSを含む部分群であるので，上の族は空でない．
(ii) 補題 1.2.5より，$\langle S\rangle$は部分群である．さらに，$\langle S\rangle$はSを含む最小の部分部である．つまり，Gの部分群Hに対して，次が成り立つ：
$$S\subset H \iff \langle S\rangle \subset H .$$
(iii) 同様に，Gはモノイドで，$S\subset G$が部分集合のとき，Sで生成される部分モノイドも定義できる．
(iv) $S=\{x_1,\dots,x_n\}$ $(x_1,\dots,x_n\in G)$のとき，$\langle S\rangle$を単に$\langle x_1,\dots,x_n\rangle$と書く．
(v) Sは群Gの部分集合で，$G=\langle S\rangle$のとき，GがSで生成されるという．

命題 1.2.8 Gは群で，$S\subset G$を空でない部分集合とする．$\langle S\rangle$は
$$x = s_1^{k_1} s_2^{k_2}\cdots s_n^{k_n} \quad (n\geq 1,\ s_1,\dots,s_n\in S,\ k_1,\dots,k_n\in\mathbb{Z}) \qquad (*)$$
として表されるGの元全体からなる．

注意

証明：A を $(*)$ の形の元全体の集合とする．

また，H を S を含む部分群とする．明かに，$(*)$ の形の任意の元は H に属するので，$A \subset H$ となる．
よって，$A \subset \bigcap_{\substack{H:\text{部分群} \\ S \subset H}} H = \langle S \rangle$．

逆に，$\langle S \rangle \subset A$ と示す．A は G の部分群であると説明する．$s \in H$ とすると $s^0 = e$ より，$e \in A$ である．
また，$x = s_1^{k_1} \cdots s_n^{k_n}$ かつ $y = t_1^{r_1} \cdots t_m^{r_m}$ $(k_i, r_i \in \mathbb{Z},\ s_i, t_i \in S)$ ならば，$xy^{-1} = s_1^{k_1} \cdots s_n^{k_n} t_m^{-r_m} \cdots t_1^{-r_1}$ となり
ゆえに $xy^{-1} \in A$ である．A が部分群であると明証できた．
このことより，$\langle S \rangle \subset A$ が成り立つ．
以上より $\langle S \rangle = A$ である． □

定義 1.2.9（対称群，置換群） X を集合とする．全単射 $X \to X$ 全体の集合は $Bij(X)$ とおくと，合成に関して群をなす．
この群は X の **対称群**（あるいは **置換群**）とよぶ．単位元は恒等写像である．
特に，$X = \{1, 2, \ldots, n\}$（n 自然数）の場合は $Bij(X)$ を S_n と書く．

例 1.2.10：n を自然数とする．
対称群 S_n は隣接互換で生成される．つまり，

$$S_n = \langle (12), (23), \ldots, (n-1\ n) \rangle \quad \text{である}$$

また，S_n は互換 (12) と長さが n の巡回置換 $\sigma = (1\ 2\ \cdots\ n)$ で生成される．つまり

$$S_n = \langle (12), \sigma \rangle \quad \text{である．}$$

（なぜかというと，
$$\sigma(12)\sigma^{-1} = (\sigma(1)\ \ \sigma(2)) = (2\ 3)$$
$$\sigma^2(12)\sigma^{-2} = (\sigma^2(1)\ \ \sigma^2(2)) = (3\ 4)$$
$$\vdots$$
$$\sigma^{n-2}(12)\sigma^{-(n-1)} = (\sigma^{n-2}(1)\ \ \sigma^{n-2}(2)) = (n-1\ \ n)$$
よって，$\langle (12), \sigma \rangle = S_n$ ）

定義 1.2.11（巡回群）：G を群とする．G は巡回群であるとは，ただ一つの元で生成されることをいう．つまり，$g \in G$ が存在し，$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ である．

§2. 準同型

§2.1. 定義

定義2.1.1 (モノイド準同型) : G_1, G_2 をモノイドとし, $f: G_1 \to G_2$ を写像とする.

f が **モノイド準同型** であるとは, f が以下の条件を満たすことをいう:

(i) $f(xy) = f(x)f(y)$ $\quad (x, y \in G_1)$
(ii) $f(e_1) = e_2$ $\quad (e_1 : G_1$ の単位元, $e_2 : G_2$ の単位元$)$

G_1, G_2 が群であるときに, 上の条件 (i) と (ii) を満たす写像 $f: G_1 \to G_2$ は **群準同型** であるという. 実は, 写像 f が (i) を満たすとすると, f は自動的に (ii) を満たすことが分かる. 実際に,

$f(e_1) = f(e_1 \cdot e_1) = f(e_1) \cdot f(e_1)$ より, $f(e_1) = e_2$ となる.

補題2.1.2 $f: G_1 \to G_2$ を群準同型とする.
任意の $x \in G_1$ に対して, $f(x^{-1}) = f(x)^{-1}$ である.

証明 : $e_2 = f(e_1) = f(x x^{-1}) = f(x) \cdot f(x^{-1})$ より,
$f(x^{-1}) = f(x)^{-1}$ である. □

例 2.1.3 :

- n を自然数とする.
  $f: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto \overline{k}$ は群 $(\mathbb{Z}, +)$ から群 $(\mathbb{Z}/n\mathbb{Z}, +)$ への群準同型である.
- $GL_n(\mathbb{C}) \to \mathbb{C}^\times$, $A \mapsto \det(A)$ は群 $(GL_n(\mathbb{C}), \times)$ から群 $(\mathbb{C}^\times, \times)$ への群準同型である.

定義2.1.3. (核, 像) $f: G_1 \to G_2$ を群準同型とする.

(i) f の **核** は $\mathrm{Ker}(f) = \{x \in G_1 \mid f(x) = e_2\}$ (e_2 は G_2 の単位元である) で定義されている.
(ii) f の **像** は $\mathrm{Im}(f) = \{f(x) \mid x \in G_1\} = f(G_1)$ で定義されている.

補題2.1.4　$f : G_1 \to G_2$ を群準同型とする．このとき，$\mathrm{Ker}(f)$ は G_1 の部分群であり，$\mathrm{Im}(f)$ は G_2 の部分群である．

証明：$f(e_1) = e_2$ より，$e_1 \in \mathrm{Ker}(f)$ である．また，$x, y \in \mathrm{Ker}(f)$ に対して，
$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e_2 \cdot e_2 = e_2$ であるので，$xy^{-1} \in \mathrm{Ker}(f)$．
したがって，$\mathrm{Ker}(f)$ は G_1 の部分群である．

$f(e_1) = e_2$ より，$e_2 \in \mathrm{Im}(f)$ である．$g, g' \in \mathrm{Im}(f)$ とする．$\mathrm{Im}(f)$ の定義から，
$x, x' \in G_1$ が存在し，$g = f(x)$ かつ $g' = f(x')$ である．よって $gg'^{-1} = f(x)f(x')^{-1} = f(xx'^{-1})$
である．ゆえに，$gg'^{-1} \in \mathrm{Im}(f)$ となる．
以上より，$\mathrm{Im}(f)$ は G_2 の部分群である．　□

定義2.1.5（群同型，自己準同型，自己同型）

(i) $f : G_1 \to G_2$ を群準同型とする．f は**群同型**であるとは，f が全単射であることをいう．

(ii) G を群とする．群準同型 $f : G \to G$ は**G の自己準同型**とよぶ．

(iii) また，群同型 $G \to G$ は**G の自己同型**とよぶ．

命題2.1.6

$f : G_1 \to G_2$ を群同型とする．このとき，逆写像 $f^{-1} : G_2 \to G_1$ は群同型である．

証明：f^{-1} は全単射であるので，f^{-1} が群準同型であることを確認すれば十分である．
$x, y \in G_2$ とする．このとき，

$$f\left(f^{-1}(xy)\right) = xy = f(f^{-1}(x))\, f(f^{-1}(y)) = f\left(f^{-1}(x)\, f^{-1}(y)\right)$$ が成り立つ．

f が単射であるので，$f^{-1}(xy) = f^{-1}(x)\, f^{-1}(y)$ となる．命題が従う．　□

例 2.1.7 (自己同型群)

G_1, G_2, G_3 を群とし, $f: G_1 \to G_2$ と $g: G_2 \to G_3$ を群準同型とする.

合成写像 $g \circ f: G_1 \to G_3$ が群準同型であることは簡単に確められる.

特に, 群 G が与えられているときに, **G の自己同型群** $Aut(G)$ は次のように定義できる.

集合として, $Aut(G)$ は G の自己同型全体である. $Aut(G)$ の演算は合成により定まる.

命題 2.1.6 を使うことで, $Aut(G)$ が $Bij(G)$ の部分群であることが証明できる.

$(\mathbb{Z}/n\mathbb{Z}, +)$ の自己同型群を求めよ...

§2.2. 剰余群

G を群とし, $H \subset G$ を部分群とする. G の元 g に対して, 集合

$$gH = \{gh \mid h \in H\}$$
$$Hg = \{hg \mid h \in H\}$$

はそれぞれ (H による) **左剰余類**, **右剰余類** とよばれる.

補題 2.2.1

(i) 任意の $g_1, g_2 \in G$ に対して, $g_1H = g_2H$ または $g_1H \cap g_2H = \emptyset$ である.
(ii) G は左剰余類に分割される. つまり, G の元 $\{g_i\}_{i \in I}$ があり,

$$G = \bigsqcup_{i \in I} g_i H \quad (\text{直和})$$

証明:

(i) $g_1H \cap g_2H \neq \emptyset$ とする. このとき, $h_1, h_2 \in H$ が存在し, $g_1h_1 = g_2h_2$ である.
よって, 全ての $h \in H$ に対して, $g_1h = g_1h_1h_1^{-1}h = g_2h_2h_1^{-1}h \in g_2H$ である.
このことから $g_1H \subset g_2H$ となり, さらに同じく $g_2H \subset g_1H$ が成り立つ. ゆえに $g_1H = g_2H$ である.

(ii) 以上より, 任意の G の元 g がただ一つの左剰余類に属する (すなわち, gH である).
よって, (ii) が従う.

□

右剰余類の場合, 上と同様なことが成り立つ.
H による左剰余類全体の集合と 右剰余類全体の集合 はそれぞれ

G/H と $H\backslash G$

で表す.

例 2.2.2. $G=(\mathbb{Z},+)$ とし, $H=n\mathbb{Z}$ (n は自然数) とする. このとき,

$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ ただし, $\overline{k} = k+n\mathbb{Z}$ とおく.

定義 2.2.3.（正規部分群） Gを群とし，$H \subset G$を部分群とする．Hが**正規部分群**であるとは，

任意の$g \in G$に対して，$gH = Hg$ が成り立つことをいう．

補題 2.2.4. $H \subset G$を部分群とする．以下の条件は互いに同値である．

(i) Hが正規部分群である．
(ii) 任意の$g \in G, h \in H$に対して，$ghg^{-1} \in H$である．
(iii) Hによる左剰余類全体の集合と右剰余類全体の集合が一致する．

証明：

(i) $\Rightarrow$ (ii)：$g \in G, h \in H$とする．Hが正規部分群なので，$gh = h'g$ となる $h' \in H$ が存在する．よって，$ghg^{-1} = h'gg^{-1} = h' \in H$．

(ii) $\Rightarrow$ (i)：$g \in G, h \in H$とする．また，$h' = ghg^{-1}$ と書く．仮定より$h' \in H$である．よって，$gh = h'g \in Hg$．ゆえに，$gH \subset Hg$が成り立つ．

同様に，$h'' = g^{-1}hg$ とおくと，$h'' \in H$である．
よって，$hg = gh'' \in gH$ となる．ゆえに，$Hg \subset gH$である．
以上より，$gH = Hg$ である．

(i) $\Rightarrow$ (iii)：明かである．

(iii) $\Rightarrow$ (i)：$g \in G$とする．仮定より，$gH = Hg'$ となる$g' \in G$が存在する．
よって，$g \in Hg \cap Hg'$が成り立つ（とくに $Hg \cap Hg' \neq \emptyset$である）補題 2.2.1 より，
$Hg = Hg' = gH$ となる．

□

注意 2.2.5.

(i) Gと$\{e\}$はGの正規部分群である．

(ii) Gをアーベル群とする．Gの全ての部分群は正規部分群である．

(iii) Hが正規部分群であることは $H \triangleleft G$ で表す．

補題 2.2.6 $f: G \longrightarrow G'$ を群準同型とし，$H' \subset G'$ を G' の正規部分群とする．このとき，$H = f^{-1}(H')$ は G の正規部分群である．

とくに，$\mathrm{Ker}(f) = f^{-1}(\{e\})$ は G の正規部分群である．

証明： H が G の部分群であることは簡単に確認できる．

$g \in G$, $h \in H$ に対して，$f(ghg^{-1}) = f(g)\,f(h)\,f(g)^{-1}$ である．

$f(h) \in H'$ より，$f(ghg^{-1}) \in H'$ が成り立つ．

つまり，$ghg^{-1} \in H$ である．ゆえに，H は正規部分群である．

□

$H \subset G$ を正規部分群とする．$g_1, g_2 \in G$ に対して，g_1H と g_2H の積を

$$g_1H \cdot g_2H = g_1g_2H$$

で定義する．

定理 2.2.7.

(i) 上の定義によって，矛盾なく G/H 上の演算が定まる．

(ii) この演算に関して，G/H は群をなす．

(iii) $\pi: G \longrightarrow G/H$, $g \longmapsto gH$ は群準同型であり，$\mathrm{Ker}(\pi) = H$ である．

証明：

(i) $g_1, g_1', g_2, g_2' \in G$ とし，$g_1H = g_1'H$ かつ $g_2H = g_2'H$ とする．

$$g_1'g_2'H = g_1'(g_2'H) = g_1'(g_2H) \overset{\text{正規性}}{=} g_1'(Hg_2) = (g_1'H)g_2 = g_1Hg_2 \overset{\text{正規性}}{=} g_1g_2H.$$

(ii) 明かに，この演算が結合法則を満たす．
また，$eH = H$ は単位元である．
$g \in G$ に対して，$(gH)(g^{-1}H) = gg^{-1}H = eH = H$ より，gH は可逆元であり，
$(gH)^{-1} = g^{-1}H$ が成り立つ．よって，G/H は群をなす．

(iii) $\pi(gg') = gg'H = (gH)(g'H) = \pi(g)\pi(g')$ $(g, g' \in G)$ より，π は群準同型である．
$\mathrm{Ker}(\pi) = \{ g \in G \mid gH = H \} = H$ である．

□

π は自然な射影とよばれる．

§2.3 準同型定理

定理 2.3.1 $f : G \longrightarrow G'$ を群準同型とする．このとき，f が以下のように分解できる：

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ G/\mathrm{Ker}(f) & \xrightarrow[\tilde{f}]{} & \mathrm{Im}(f) \end{array} \qquad f = \iota \circ \tilde{f} \circ \pi \text{ である．}$$

ここで，π は自然な射影である
ι は自然な包含写像である
$\tilde{f}$ は $\tilde{f}(g\,\mathrm{Ker}(f)) = f(g)$ で定まり，さらに群同型である．

証明：
まず，$\tilde{f}$ が矛盾なく定義されていることを確認する．
$H = \mathrm{Ker}(f)$ とおき，$gH = g'H$ とする．
このとき，$g^{-1}g' \in H$ である．よって，$f(g^{-1}g') = f(g)^{-1}f(g') = e$ であり，ゆえに
$f(g) = f(g')$．よって，$\tilde{f}(gH) = f(g)$ とおくと，写像 $\tilde{f}$ が矛盾なく定まる．
$\tilde{f}$ は準同型である：
$\tilde{f}((gH)(g'H)) = \tilde{f}(gg'H) = f(gg') = f(g)f(g') = \tilde{f}(gH)\tilde{f}(g'H)$ $(g, g' \in G)$
より，$\tilde{f}$ は準同型である．
$\tilde{f}$ は単射である：$\tilde{f}(gH) = \tilde{f}(g'H)$ $(g, g' \in G)$ とする．

よって $f(g)=f(g')$ であり，$f(g^{-1}g')=f(g)^{-1}f(g')=e$ となる．

$\Rightarrow g^{-1}g'\in H \Rightarrow gH=g'H$ である．

$\tilde{f}$ が全射であることは明かである．

以上より，$\tilde{f}$ は群同型である．

最後に，$g\in G$ に対して，$(\iota\circ\tilde{f}\circ\pi)(g)=\iota(\tilde{f}(gH))=f(g)$ であることより，$f=\iota\circ\tilde{f}\circ\pi$ が成り立つ．

□

注意 2.3.2　$f : G \to G'$ を群準同型とする.

(i) f が単射である $\iff$ $\mathrm{Ker}(f) = \{e\}$

(ii) f が全射ならば, $G/\mathrm{Ker}(f) \simeq G'$ である.
($\simeq$: 同型)

例 2.3.3

$n \geq 2$ を自然数とし, S_n を置換群とする.

$\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}$　(符号)　は準同型であり,

$\mathrm{Ker}(\mathrm{sgn}) = A_n$ (偶置換全体のなす部分群).
$\mathrm{Im}(\mathrm{sgn}) = \{\pm 1\}$

よって, $A_n \lhd S_n$ であり, $S_n/A_n \simeq \{\pm 1\}$ となる.

(ii) G を群とする. G の中心 $Z(G)$ は以下のように定義されている.

$$Z(G) = \{ g \in G \mid \forall x \in G,\ gx = xg \}$$

$Z(G)$ は G の正規部分群である.

(iii) G を群とし, $\mathrm{Aut}(G)$ を G の自己同型群とする.

$x \in G$ に対して, $f_x : G \longrightarrow G$, $g \longmapsto xgx^{-1}$ と定義する.

f_x は G の自己同型である. このような自己同型は内部自己同型と呼ばれる.

$$\varphi : G \longrightarrow \mathrm{Aut}(G), \quad x \longmapsto f_x$$

とおくと, φ は群準同型である (つまり, $f_{xy} = f_x \circ f_y$ である).

- φ の像は内部自己同型全体のなす $\mathrm{Aut}(G)$ の部分群である. この部分群は $\mathrm{Inn}(G)$ で表す.
- $\mathrm{Ker}(\varphi) = Z(G)$ が成り立つ.

よって, $G/Z(G) \simeq \mathrm{Inn}(G)$ となる.

さらに, $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$ が成り立つ.

実際に, $x \in G$, $\varphi \in \mathrm{Inn}(G)$ とすると,

$$\begin{aligned}\varphi \circ f_x \circ \varphi^{-1}(g) &= \varphi\left(f_x(\varphi^{-1}(g))\right) \\ &= \varphi\left(x\varphi^{-1}(g)x^{-1}\right) \\ &= \varphi(x)\varphi(\varphi^{-1}(g))\varphi(x)^{-1} \\ &= \varphi(x)\, g\, \varphi(x)^{-1}\end{aligned}$$

よって, $\varphi \circ f_x \circ \varphi^{-1} = f_{\varphi(x)}$ である. 特に $\varphi \circ f_x \circ \varphi^{-1} \in \mathrm{Inn}(G)$ が成り立つので, $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$ である.

§3. 群の位数

§3.1. 定義

定義 3.1.1. (位数) G を群とする.

(i) G の位数とは, G の元の個数のことをいう. (G が無限集合ならば, その位数は無限である).

(ii) $g \in G$ とする. g の位数とは, g で生成された部分群 $\langle g \rangle$ の位数のことをいう.

命題 3.1.2. G を群とし, $g \in G$ とする.

(i) g の位数が有限である $\Leftrightarrow$ $g^n = e$ であるような $n \geq 1$ がある.

(ii) g の位数が有限であると仮定する. このとき, g の位数は $g^n = e$ を満たす最小の正の n に等しい.

証明：

(i) ($\Rightarrow$) $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$ である．

$\langle g\rangle$ が有限集合だから，$g^n = g^m$ となる整数 $n \neq m$ が存在する．また $n > m$ を仮定して良い．よって，$g^n \cdot g^{-m} = g^m \cdot g^{-m}$ であり，ゆえに $g^{n-m} = e$ となる．

($\Leftarrow$) $g^n = e$ $(n \neq 0)$ とする．このとき，$(g^n)^{-1} = g^{-n} = e$ なので，$n > 0$ を仮定して良い．よって，$A = \{n \geq 1 \mid g^n = e\}$ は空でない．

m を A の最小の自然数とする．このとき，

$$\langle g\rangle = \{e, g, \cdots, g^{m-1}\} \qquad (*)$$

が成り立つことを示す．$n \in \mathbb{Z}$ に対して，$\begin{cases} n = mq + r \\ 0 \leq r < m \end{cases}$ であるような $q, r \in \mathbb{Z}$ が存在する（除法の原理）．

したがって，$g^n = g^{mq+r} = g^{mq} \cdot g^r = (g^m)^q \cdot g^r$ である．

$g^m = e$ より，$g^n = e^q \cdot g^r = g^r \in \{1, g, \cdots, g^{m-1}\}$ となる．

よって，$\langle g\rangle$ は有限集合であり，ゆえに g の位数は有限である．

(ii) 上の $(*)$ より，$\langle g\rangle$ の元の個数は m である．

m が A の最小のものだから，(ii) が従う． □

系 3.1.3. G を群とし，$g \in G$ とする．写像

$$\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}$$

は群 $(\mathbb{Z}, +)$ から G への群準同型である．さらに，$\mathrm{Im}(\varphi) = \langle g\rangle$ である．

(i) g の位数が無限である $\Leftrightarrow$ $\mathrm{Ker}(\varphi) = 0$ である $\Leftrightarrow$ φ が単射である．

(ii) g の位数が有限ならば，$\mathrm{Ker}(\varphi) = m\mathbb{Z}$ $(m = g$ の位数$)$．

証明：(i) は 命題 3.1.2(i) から分かる.

(ii) $\mathrm{Ker}(\varphi)$ は $\mathbb{Z}$ の部分群だから, $\mathrm{Ker}(\varphi) = d\mathbb{Z}$ となる $d \geq 1$ が存在する. 命題 3.1.2 (ii) より, $d = m$ である.

□

系 3.1.4. g を有限位数の元とする. g の位数を m とおくと, 任意の $n \in \mathbb{Z}$ に対して, $g^n = e \iff m \mid n$ である.

証明：$g^n = e \iff n \in \mathrm{Ker}(\varphi)$

$\iff n \in m\mathbb{Z}$

$\iff m \mid n$.

□

§3.2. ラグランジュの定理

補題 3.2.1. Gを群とし，Hを部分群とする．写像

$$\Psi : G/H \longrightarrow H\backslash G \ , \ gH \longmapsto Hg^{-1}$$

は well-defined であり，さらに全単射である．

証明： $g_1H = g_2H$ $(g_1, g_2 \in G)$ ならば，$H = g_1^{-1}g_2H$ であり
ゆえに $g_1^{-1}g_2 \in H$ が成り立つ．よって，$Hg_1^{-1}g_2 = H$ となる．
したがって，$Hg_1^{-1} = Hg_2^{-1}$ である．このことより，Ψ は well-defined である．

単射：$g_1, g_2 \in G$ に対して，
$$\begin{aligned} Hg_1^{-1} = Hg_2^{-1} &\Leftrightarrow Hg_1^{-1}g_2 = H \\ &\Leftrightarrow g_1^{-1}g_2 \in H \\ &\Leftrightarrow H = g_1^{-1}g_2H \\ &\Leftrightarrow g_1H = g_2H \end{aligned}$$

全射：明かである．　□

定義 3.2.2.（指数） Gを群とし，$H \subset G$を部分群とする．
Hによる左剰余類の個数はGにおけるHの指数とよび，$[G:H]$で表す．
つまり，$[G:H] = |G/H|$ である．

補題3.2.1より，$[G:H] = |H\backslash G|$ も成り立つ．

定理 3.2.3（ラグランジュの定理） Gを有限群とする（つまり，$|G|$が有限である）．
このとき，$|G| = [G:H] \cdot |H|$ が成り立つ．

証明： 補題 2.2.1 より，G は左剰余類に分割される．つまり，

$$G/H = \{g_1H, g_2H, \dots, g_nH\} \quad (g_1H, \dots, g_nH \text{は互いに相異なる})$$

とおくと，$G = \bigsqcup_{i=1}^{n} g_iH$ （直和）である．さらに，$[G:H] = n$ である．

よって，$|G| = |g_1H| + \dots + |g_nH|$ である．

$g \in G$ とすると，写像 $H \longrightarrow gH$, $h \longmapsto gh$ は全単射である．

特に，$|gH| = |H|$ が成り立つ．

以上より，$|G| = \underbrace{|H| + \dots + |H|}_{n\text{個}} = n|H| = [G:H] \cdot |H|$ となる．

□

命題 3.2.4. G を有限群とし，G の位数を n と書く．
このとき，任意の元 $g \in G$ に対して，$g^n = e$ である．

証明： $H = \langle g \rangle$ とおき，g の位数を m と書く
（つまり，$m = |H|$ である）．命題 3.1.2 (ii) より，$g^m = e$ である．
定理 3.2.3 より，$n = m \cdot d$ である（$d = [G:H]$）．よって，
$g^n = g^{m \cdot d} = (g^m)^d = e^d = e$ である □

例 3.2.5 モノイド $(\mathbb{Z}/n\mathbb{Z}, \times)$ において，次が成り立つ．
任意の $k \in \mathbb{Z}$ に対して，

$\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ が可逆元である $\iff$ k と n は互いに素である．

$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k} \mid \gcd(k,n) = 1\}$ とおくと，$(\mathbb{Z}/n\mathbb{Z})^\times$ は位数 $\varphi(n)$（オイラーの φ 関数）の群をなす．

命題 3.2.4 より，$\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対して，$\overline{k}^{\varphi(n)} = 1$ が成り立つ．

よって，任意の $k \in \mathbb{Z}$ に対して，

$\gcd(k,n)=1$ ならば, $k^{\varphi(n)} \equiv 1 \pmod{n}$ である.

n が素数 p ならば, $\gcd(k,p)=1 \Rightarrow k^{p-1} \equiv 1 \pmod{p}$ となる

(フェルマーの小定理).

§3.3. 巡回群

$G=\langle g \rangle$ のとき, g は G の生成元であるという.

命題 3.3.1 G を巡回群とし, $G=\langle g \rangle$ $(g \in G)$ とする.

(i) G の位数が無限ならば, G はただ二つの生成元をもつ.
となわち, $G=\langle h \rangle \Leftrightarrow (h=g$ または $h=g^{-1})$ である.

(ii) G の位数 n が有限ならば, 任意の $k \in \mathbb{Z}$ に対して,
g^k が G の生成元である $\Leftrightarrow \gcd(k,n)=1$.

証明:

(i) $\varphi : \mathbb{Z} \to G$, $k \mapsto g^k$ を考える. G は無限だから, $\mathrm{Ker}(\varphi)=0$ である (系 3.1.3.).

よって, φ は群同型である. $(\mathbb{Z},+)$ の生成元全体は $\{1,-1\}$ である.
したがって, g^k が G を生成する $\Leftrightarrow k \in \{-1,1\}$ であり, (i) が従う.

(ii) このとき, $\mathrm{Ker}(\varphi)=n\mathbb{Z}$ である. 準同型定理より, $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} G$, $\bar{k} \mapsto g^k$ は群同型である.

よって, g^k が G を生成する $\Leftrightarrow \bar{k}$ が $(\mathbb{Z}/n\mathbb{Z},+)$ を生成する
$\Leftrightarrow \gcd(k,n)=1$. □

補題 3.3.2. G_1, G_2 を有限巡回群とし, G_1, G_2 の位数をそれぞれ n_1, n_2 と書く. n_1 と n_2 が互いに素ならば, $G_1 \times G_2$ は位数 $n_1 n_2$ の巡回群である.

証明: $G_1 \simeq \mathbb{Z}/n_1\mathbb{Z}$, $G_2 \simeq \mathbb{Z}/n_2\mathbb{Z}$ である.

$G_1 \times G_2 \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \simeq \mathbb{Z}/n_1n_2\mathbb{Z}$ (中国の剰余定理). □

補題 3.3.3　G を群とし，$g \in G$ を有限位数の元とする．
g の位数を n とおくと，g^m $(m \in \mathbb{Z})$ の位数は $\frac{n}{\gcd(n,m)}$ である．

証明：$n' = \frac{n}{\gcd(n,m)}$ と $m' = \frac{m}{\gcd(n,m)}$ とおく．
$(g^m)^{n'} = g^{\frac{nm}{\gcd(n,m)}} = (g^n)^{m'} = e$ である．よって，g^m の位数は n' の約数である．
また，$(g^m)^d = e$ $(d \in \mathbb{Z})$ ならば，$g^{md} = e$ となり，ゆえに $n \mid md$ である．
よって，$n' \mid m'd$ である．n' と m' が互いに素なので，$n' \mid d$ となる．
以上より，g^m の位数は $n' = \frac{n}{\gcd(n,m)}$ である．
□

命題 3.3.4. G を位数 n の巡回群とし，d を n の正の約数とする．
G において，位数 d の部分群は一意的に存在する．つまり，

$$\{G\text{の部分群}\} \longrightarrow \{n\text{の正の約数}\} \quad \text{は全単射である．}$$
$$H \longmapsto H\text{の位数}$$

さらに，G の任意の部分群は巡回群である．

証明： g を G の生成元とする（つまり，$G=\langle g\rangle$）．
H を G の部分群とし，H の位数を d とおく．

$\varphi : \mathbb{Z} \longrightarrow G,\ k \longmapsto g^k$ を考える．$\varphi^{-1}(H)$ は $\mathbb{Z}$ の部分群だから，
$\varphi^{-1}(H) = m\mathbb{Z}$ となる $m \geqslant 1$ がある．よって，$\varphi^{-1}(H)$ が m で生成されるので，
$H = \varphi(\varphi^{-1}(H))$ は $\varphi(m) = g^m$ で生成される．このことより，H は巡回群である．
（$=$ の上：φ は全射）

$\mathrm{Ker}(\varphi) = n\mathbb{Z} \subset \varphi^{-1}(H) = m\mathbb{Z}$ より，$m \mid n$ である．
補題 3.3.3 より，g^m の位数は $\frac{n}{m}$ である．したがって，$d = \frac{n}{m}$ である．

よって，$H = \langle g^{n/d} \rangle$ である．（一意性）

逆に，d を n の約数とし，$H = \langle g^{n/d} \rangle$ とおくと，補題 3.3.3 より
H は位数 d の部分群である．（存在性）

補題が従う． □

§4. 群作用

§4.1. 定義と例

定義 4.1.1. (群作用) G を群とし，X を集合とする．また，写像

$$f : G \times X \longrightarrow X, \quad (g, x) \longmapsto f(g,x)$$

が与えられているとする．$f(g,x)$ を単に $g \cdot x$ と書くことにしよう．

このとき，f が **G の X への作用** であるとは，以下の条件が成り立つことをいう．

(i) 任意の $x \in X$ に対して，$e \cdot x = x$ である

(ii) 任意の $g, g' \in G$ と $x \in X$ に対して，$g \cdot (g' \cdot x) = (gg') \cdot x$ である．

G が集合 X に作用しているとする．このとき，$g \in G$ に対して，写像

$$\varphi_g : X \longrightarrow X, \quad x \longmapsto g \cdot x$$

と定義する．

φ_g が全単射であることを説明する．$x \in X$ に対して，

$$\varphi_g \circ \varphi_{g^{-1}}(x) = \varphi_g(\varphi_{g^{-1}}(x)) = g \cdot (g^{-1} \cdot x) \overset{\text{定義 4.1.1 (ii)}}{=} (gg^{-1}) \cdot x = e \cdot x \overset{\text{定義 4.1.1 (i)}}{=} x$$

よって，$\varphi_g \circ \varphi_{g^{-1}} = id_X$ (X の恒等写像)．同様に，$\varphi_{g^{-1}} \circ \varphi_g = id_X$ が成り立つ．

このことから，φ_g は全単射である．つまり，$\varphi_g \in Bij(X)$ である．

また，次が成り立つ：

(i) $\varphi_e = id_X$

(ii) $\varphi_{g^{-1}} = (\varphi_g)^{-1}$ (すなわち φ_g の逆写像)

(iii) $\varphi_{gg'} = \varphi_g \circ \varphi_{g'}$ $(g, g' \in G)$

補題 4.1.2　G を群とし，X を集合とする．

(i) $f : G \times X \longrightarrow X$ を G の X への作用とする．
このとき，$\varphi : G \longrightarrow Bij(X)$，$g \longmapsto \varphi_g$ は群準同型である

(ii) 逆に，$\varphi : G \longrightarrow Bij(X)$ を群準同型とする．
このとき，写像 $G \times X \longrightarrow X$，$(g, x) \longmapsto [\varphi(g)](x)$ は G の X への作用である

(iii) 上の(i)と(ii)より，G の X への作用全体 と 群準同型 $G \to Bij(X)$ 全体の間に一対一対応が得られる．

証明：

(i) は 上 に確認した．

(ii) $\varphi : G \to Bij(X)$ を群準同型とし，$g \cdot x = [\varphi(g)](x)$ とおく．

このとき，$e \cdot x = [\varphi(e)](x) = id_X(x) = x$ である．また，$g, g' \in G$，$x \in X$ に対して，

$$g \cdot (g' \cdot x) = \varphi(g)\left((\varphi(g'))(x)\right) = (\varphi(g) \circ \varphi(g'))(x) = (\varphi(gg'))(x) = (gg') \cdot x$$

である．よって，$(g, x) \mapsto g \cdot x$ は X への作用を与える．

(iii) 以下の写像は全単射であり，互いに逆写像である．

$$\left\{ \begin{array}{l} G \text{ の } X \text{ への作用} \\ G \times X \to X \end{array} \right\} \rightleftarrows \left\{ \text{群準同型 } G \to Bij(X) \right\}$$

$$f : G \times X \to X \quad \longmapsto \quad \varphi : G \to Bij(X),\ g \mapsto (\varphi_g : x \mapsto g \cdot x)$$

$$f : G \times X \to X,\ (g, x) \mapsto [\varphi(g)](x) \quad \longmapsfrom \quad \varphi$$

□

例 4.1.3 G を群とする.

(i) $X = G$ とする.

$g \cdot h = gh \quad (g, h \in G)$ とおくと,

G の G への作用が与えられる. この作用は**左移動**とよばれる.

(ii) $g \cdot h = ghg^{-1}$ と定義する. これは, G の自分自身への作用であり,

共役作用とよばれる.

(iii) X を集合とする.

$g \cdot x = x \quad (g \in G, x \in X)$ で定まる G の X への作用は

自明作用とよばれる.

(iv) $GL_n(\mathbb{R})$ は自然に $\mathbb{R}^n$ に作用する. 実際に,

$A \in GL_n(\mathbb{R}), X \in \mathbb{R}^n$ に対して, $A \cdot X = \underbrace{AX}_{\in \mathbb{R}^n}$ とおくことによって作用が定まる.

(v) 群 G が集合 X に作用しているとする. このとき, G が自然に

X のべき集合 $\mathcal{P}(X)$ に作用する. すなわち, $g \in G$, $S \subset X$ とすると,

$g \cdot S = \{ g \cdot s, s \in S \}$ とおくと G の $\mathcal{P}(X)$ への作用が与えられる.

§4.2. 軌道

定義 4.2.1. (軌道) $x \in X$ に対して,

$$Gx = \{ g \cdot x \mid g \in G \}$$ と定義し, x の群 G による軌道とよぶ.

注意 4.2.2 G が X に作用するとき, X 上の同値関係が次のように定義できる.

$$x \sim x' \iff \exists g \in G,\ x' = g \cdot x$$

$\sim$ が同値関係であることを確認する.

- $x = e \cdot x$ より, $x \sim x$ である.
- $x' = g \cdot x$ ならば, $x = g^{-1} \cdot x'$ となる.
  よって, $x \sim x' \Rightarrow x' \sim x$ である.
- $x' = g' \cdot x'$ かつ $x' = g \cdot x$ $(g, g' \in G,\ x, x', x'' \in X)$ ならば, $x'' = g' \cdot (g \cdot x) = (g'g) \cdot x$ である.
  よって, $x' \sim x''$ かつ $x \sim x' \Rightarrow x \sim x''$

この同値関係の同値類は軌道にほかならない. とくに, $\{x_i\}_{i \in I}$ が $\sim$ の完全代表系ならば,

$$X = \bigsqcup_{i \in I} Gx_i$$

が成り立つ.

例 4.2.3

(i) $G = GL_n(\mathbb{R})$ が自然に $\mathbb{R}^n$ に作用する.

ただ二つの軌道がある. すなわち,

- $x \in \mathbb{R}^n \setminus \{0\}$ に対して $Gx = \mathbb{R}^n \setminus \{0\}$
- $x = 0$ の軌道は $\{0\}$ である.

(ii) Gを群とする．Gが共役によって自分自身に作用する．

このとき，Gの元gの軌道は$\{hgh^{-1} \mid h \in G\}$であり，$g$の**共役類**とよばれる．

例えば，$G = S_n$とする（対称群）．$\sigma, \tau \in S_n$に対して，

σとτが共役である $\Leftrightarrow$

$\sigma = c_1 \cdots c_r$　（$c_1, \dots, c_r$：互いに素な巡回置換）
$\tau = c_1' \cdots c_s'$　（$c_1', \dots, c_s'$：〃）

と書くと，$r = s$かつ$c_1, \dots, c_r$の長さと$c_1', \dots, c_r'$の長さが順番を除いて一致する．

（例えば，$n = 5$のとき，$(12)\cdot(354)$ と $(132)\cdot(45)$ は共役である）
c_1　c_2　　c_1'　c_2'

したがって，S_3においては，3つの共役類がある．

- $\{id\}$
- $\{(12), (13), (23)\}$
- $\{(123), (132)\}$

S_4の共役類：

- $\{id\}$
- (ab) の形の置換全体
- (abc)
- $(ab)(cd)$
- $(abcd)$

§4.3. 安定部分群

定義 4.3.1 (安定部分群) 群 G が集合 X に作用しているとする.

$x \in X$ に対して, $G_x = \{ g \in G \mid g \cdot x = x \}$ と定義し, x の**安定部分群**という.

G_x が部分群であることを示す.

定義より $e \cdot x = x$ なので, $e \in G_x$ である. また, $g, g' \in G_x$ に対して,
$(gg'^{-1}) \cdot x = (gg'^{-1}) \cdot (g' \cdot x) = (gg'^{-1}g') \cdot x = g \cdot x = x$ によって, $gg'^{-1} \in G_x$ である. ゆえに, G_x は部分群である.

補題 4.3.2. $x \in X$, $g \in G$ とする. このとき, $G_{g \cdot x} = g G_x g^{-1}$ が成り立つ.

証明: $g' \in G$ に対して, 次が成り立つ

$$
\begin{aligned}
g' \in G_{g \cdot x} &\iff g' \cdot (g \cdot x) = g \cdot x \\
&\iff (g'g) \cdot x = g \cdot x \\
&\iff g^{-1} \cdot ((g'g) \cdot x) = e \cdot x = x \\
&\iff (g^{-1}g'g) \cdot x = x \\
&\iff g^{-1}g'g \in G_x
\end{aligned}
$$

よって, $G_{g \cdot x} = g G_x g^{-1}$ である. □

群 G において, H, H' が部分群で $H' = gHg^{-1}$ $(g \in G)$ が成り立つとき, H と H' が**共役部分群**であるという.

例 4.3.3. G を群とし，G の G への共役作用を考える．

$x \in G$ に対して，x の安定部分群は

$G_x = \{ g \in G \mid gxg^{-1} = x \}$ である．つまり，G_x が $gx = xg$ を満たす $g \in G$ 全体からなる部分群である．この部分群は x の中心化といい，$\mathrm{Cent}_G(x)$ で表す．

例えば，S_3 における (123) の中心化を求める．

$\sigma \in S_3$ に対して，$\sigma(123)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3))$ である．

これより，

$$\mathrm{Cent}_G((123)) = \{ id, (123), (132) \}$$

同様に，$\sigma(12)\sigma^{-1} = (\sigma(1)\ \sigma(2))$ だから，

$$\mathrm{Cent}_G((12)) = \{ \sigma \in S_3 \mid (\sigma(1)\ \sigma(2)) = (12) \}$$

$$= \{ id, (12) \}$$

例 4.3.3. G を群とし，G の G への共役作用を考える．

$x \in G$ に対して，x の安定化部分群は

$G_x = \{ g \in G \mid gxg^{-1} = x \}$ である．つまり，G_x が $gx = xg$ を満たす $g \in G$ 全体からなる部分群である．この部分群は x の **中心化群** といい，$Cent_G(x)$ で表す．

例えば，S_3 における (123) の中心化群を求める．

$\sigma \in S_3$ に対して，$\sigma(123)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3))$ である．

これより，任意の置換 $\sigma \in Cent_{S_3}((123))$ は $\sigma(1)$ から一意的に定まる．よって，$|Cent_{S_3}((123))| \leq 3$ である．ゆえに，

$$Cent_{S_3}((123)) = \{ id, (123), (132) \}$$

一般に，S_n においては，n 次巡回置換 σ の中心化群 $Cent_{S_n}(\sigma)$ は $\langle \sigma \rangle$ と一致する．

群 G が集合 X に作用しているとする．

補題 4.3.4. $x \in X$ とする．このとき，写像

$$\varphi : G/G_x \longrightarrow Gx, \quad gG_x \longmapsto g \cdot x$$

は全単射である．

証明：まず，φ が well-defined であることを示す．

$gG_x = g'G_x$ ならば，$g' = gh$ $(h \in G_x)$ と書ける．

よって，$g' \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$ である．したがって，φ は well-defined である．

φ は単射である：
$$\begin{aligned} g \cdot x = g' \cdot x &\Rightarrow g'^{-1} \cdot (g \cdot x) = g'^{-1} \cdot (g' \cdot x) \\ &\Rightarrow (g'^{-1}g) \cdot x = (g'^{-1}g') \cdot x = e \cdot x = x \\ &\Rightarrow g'^{-1}g \in G_x \\ &\Rightarrow gG_x = g'G_x \end{aligned}$$

$H \subset G$ を部分群とすると，
$gH = g'H \Leftrightarrow g'^{-1}g \in H$
$\Leftrightarrow g^{-1}g' \in H$

φ が全射であることは明かである．

以上より，φ は全単射である． □

命題 4.3.5. X が有限集合であるとする．また，$C_1, \dots, C_r$ を X における群 G の作用に関する軌道全体とし，各 $i = 1, \dots, r$ について $x_i \in C_i$ をとる．このとき，

$$|X| = \sum_{i=1}^{r} [G : G_{x_i}]$$

が成り立つ．

証明：

注意 4.2.2 より，$X = C_1 \sqcup C_2 \sqcup \dots \sqcup C_r$ （直和）

よって，$|X| = \sum_{i=1}^{r} |C_i|$ となる．補題 4.3.4 より，

$G/G_{x_i} \longrightarrow C_i$ は全単射であり，ゆえに $|C_i| = [G : G_{x_i}]$ である．

$gG_{x_i} \longmapsto g \cdot x_i$ □

（軌道 C の元 $x \in C$ をとるときに，x は C の代表元であるという．）

例 4.3.5

$G = S_3$ とし，S_3 の自分自身への共役作用を考える．

例 4.2.3 (ii) より，3つの軌道がある：

$C_1 = \{id\}$

$C_2 = \{(12), (13), (23)\}$

$C_3 = \{(123), (132)\}$

$x_1 = id$, $x_2 = (12)$, $x_3 = (123)$ とすると，$\{x_1, x_2, x_3\}$ は軌道の完全代表系である．

例 4.3.3 より，$G_{x_2} = \{id, (12)\}$

$G_{x_3} = \{id, (123), (132)\}$ である．

また，明かに $G_{x_1} = S_3$ である．よって，

$[G : G_{x_1}] = 1$

$[G : G_{x_2}] = |G|/|G_{x_2}| = 6/2 = 3$

$[G : G_{x_3}] = |G|/|G_{x_3}| = 6/3 = 2$

命題 4.3.5. の等式は以下の通りになる.

$$|G| = [G : G_{x_1}] + [G : G_{x_2}] + [G : G_{x_3}]$$
$$6 = 1 + 3 + 2$$

§4.4. p 群

定義 4.4.1. p を素数とする. **p群**とは, 位数 p^n $(n \geq 1)$ の群のことをいう.

群 G が集合 X に作用しているとする. X の**固定点**とは,
任意の $g \in G$ に対して $g \cdot x = x$ を満たす元 $x \in X$ のことをいう.
X の固定点全体の集合を X^G と書く.

命題 4.4.2. p 群 G が有限集合 X に作用しているとする. このとき,
$|X| \equiv |X^G| \mod p$ が成り立つ.

証明: $\{x_1, \dots, x_s\}$ を X の軌道の完全代表系とする. よって,
$|X| = \sum_{i=1}^{s} [G : G_{x_i}]$ である.
また, x_i が固定点である $\iff G_{x_i} = G$
$\iff [G : G_{x_i}] = 1$
G は p 群より, $G_{x_i} \neq G$ ならば, $[G : G_{x_i}] \equiv 0 \pmod p$.
よって, $|X| \equiv \sum_{x_i \text{ 固定点}} 1 = |X^G|$.
つまり, $x_i \in X^G$

□

命題 4.4.3. G を p 群とする. G の中心 $Z(G)$ は自明でない.

証明: G の自分自身への共役作用を考える.

g は固定点である $\iff \forall h \in G,\ ghg^{-1} = h$
$\iff \forall h \in G,\ gh = hg$
$\iff g \in Z(G)$

よって, 命題 4.4.2 より, $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$.

とくに, $Z(G) \neq \{e\}$ である. □

例 4.4.4.

(i) p を素数とする.

> 位数 p の群 G は常に巡回群である.

実際に $x \in G \setminus \{e\}$ とするとラグランジュの定理より, $\langle x \rangle$ の位数は p の約数である. よって $\langle x \rangle = G$ となる.

(ii)

> G を位数 p^2 の群とする. このとき, G はアーベル群である.

証明: 命題 4.4.3. より $Z(G) \neq \{e\}$ である. よって, $|Z(G)| = p$ または $|Z(G)| = p^2$ となる. $Z(G) \neq G$ が成り立つと仮定し, $x \notin Z(G)$ を満たす元 x を考える.

x の中心化群 $Cent_G(x)$ を考える.

明かに, $x \in Cent_G(x)$ かつ $Z(G) \subset Cent_G(x)$ である

よって, $|Cent_G(x)| > p$ となり, $Cent_G(x) = G$ が成り立つ. したがって, $x \in Z(G)$

となり矛盾する. ゆえに $Z(G) = G$ が成り立つ. つまり, G はアーベル群である.

□

§5 シローの定理

§5.1. コーシーの定理

> 定理 5.1.1. (コーシーの定理)
>
> G を有限群とし, p を G の位数の約数とする.
> このとき, G においては, 位数 p の元が存在する.

証明：次の集合を考える

$$X = \left\{ (x_1, \dots, x_p) \in G^p \;\middle|\; x_1 \cdots x_p = e \right\}$$

$\mathbb{Z}/p\mathbb{Z}$ の X への作用を次のように定める．巡回置換 $\sigma = (1\,2\,\cdots\,p)$ を考える．

$\overline{k} \in \mathbb{Z}/p\mathbb{Z}$，$(x_1, \dots, x_p) \in X$ について，

$$\overline{k} \cdot (x_1, \dots, x_p) = (x_{\sigma^k(1)}, x_{\sigma^k(2)}, \dots, x_{\sigma^k(p)})$$

と定義する．この作用に関して，

例えば
$\overline{1} \cdot (x_1, \dots, x_p) = (x_2, \dots, x_p, x_1)$
$\overline{2} \cdot (x_1, \dots, x_p) = (x_3, \dots, x_p, x_1, x_2)$
等

$(x_1, \dots, x_p)$ が固定点である $\iff x_1 = x_2 = \dots = x_p$ が成り立つ．

命題 4.4.2 より，$|X| \equiv |X^G| \mod p$ である．

明かに，写像 $G^{p-1} \longrightarrow X$

$$(x_1, \dots, x_{p-1}) \longmapsto (x_1, \dots, x_{p-1}, (x_1 \cdots x_{p-1})^{-1})$$

は全単射である．ゆえに，$|X| = |G|^{p-1} \equiv 0 \pmod p$．

したがって，$(e, \dots, e)$ と異なる X^G の元 $(g, \dots, g)$ が存在する．

$g^p = e$ かつ $g \neq e$ より，g は位数 p の元である．

□

§5.2. 正規化群

定義 5.2.1.（正規化群） G を群とし，H を G の部分群とする．

H の**正規化群**とは，部分群 $N_G(H) = \left\{ g \in G \mid gHg^{-1} = H \right\}$ のことをいう．

- G は G の部分群全体の集合に共役によって作用する．すなわち，元 $g \in G$，部分群 $H \subset G$ に対して，

  $g \cdot H = gHg^{-1}$ とおくことで，G の G の部分群全体の集合への作用が定まる．

  言い換えれば，H の正規化とは，この作用を考えたときの H の安定化部分群のことである．

- 明かに, $H \subset N_G(H)$ であり, さらに H は $N_G(H)$ の正規部分群である.

補題 5.2.2 G を群とし, H, K を G の部分群とする. 集合

$$HK = \{hk \mid h \in H, k \in K\}$$ を考える.

$K \subset N_G(H)$ ならば, HK は G の部分群である. また, このときに $HK = KH$ が成り立つ.

証明: 明かに, $e \in HK$ が成り立つ.

$x, x' \in HK$ とし, $x = hk$, $x' = h'k'$ $(h, h' \in H,\ k, k' \in K)$ とする.

$xx'^{-1} = hkk'^{-1}h'^{-1}$ である. $k_1 = kk'^{-1}$ とおく. $K \subset N_G(H)$ より,

$h_1 = k_1 h'^{-1} k_1^{-1} \in k_1 H k_1^{-1} = H$ である. よって, $k_1 h'^{-1} = h_1 k_1$ となる.

($k_1 \in N_G(H)$)

したがって, $xx'^{-1} = hk_1 h'^{-1} = \underbrace{hh_1}_{\in H}\underbrace{k_1}_{\in K} \in HK$. よって, HK は G の部分群である.

最後に, $g \in HK$ ならば $g^{-1} \in KH$ が成り立つので, $HK = KH$ となる. □

命題 5.2.3 H, K を群 G の部分として, $K \subset N_G(H)$ が成り立つとする.

このとき, H は HK の正規部分群であり, さらに $H \cap K$ は K の正規部分群である. また, 写像

$$K/H\cap K \xrightarrow{\sim} HK/H \qquad k(H\cap K) \longmapsto kH$$

は well-defined であり, 群同型である.

証明： 補題5.2.2. より, HK は部分群である.

$K \subset N_G(H)$ かつ $H \subset N_G(H)$ より, $HK \subset N_G(H)$ が成り立つ. よって, $H \lhd HK$ である.

また, $k \in K$, $x \in H \cap K$ とすると, $kxk^{-1} \in H \cap K$ が成り立つ. よって, $H \cap K \lhd K$ である. 準同型写像

$$f : K \longrightarrow HK/H \quad \text{を考える.}$$
$$k \longmapsto kH$$

$x \in HK$ とする. $HK = KH$ (補題5.2.2. 参照) より, $x = kh$ $(k \in K, h \in H)$ と書ける. よって, $xH = khH = kH$ である. ゆえに, f は全射である. また,

$$\begin{aligned} \mathrm{Ker}(f) &= \{k \in K \mid kH = H\} \\ &= \{k \in K \mid k \in H\} \\ &= H \cap K \qquad \text{である.} \end{aligned}$$

準同型定理より, 群同型 $K/H \cap K \xrightarrow{\sim} HK/H$ が得られる.

□

§5.3. pシローの定理

定義 5.3.1. (pシロー部分群) G を有限群とし, p を G の位数 n を割り切る素数とする. また, $n = p^k n'$ $(\gcd(n', p) = 1)$ とする (つまり, k は p^k が n を割り切るような最大の自然数である) G の **pシロー部分群** とは, 位数 p^k の部分群のことをいう.

定理 5.3.2 G を有限群とし, p を $|G|$ の素因数とする. G においては, pシロー部分群が存在する.

証明: 帰納法によって証明する.

- $H \subsetneq G$ は G の部分群で, 指数 $[G:H]$ が p で割り切れないものとする.
  帰納法の仮定より, H は pシロー部分群 K をもつ.
  $|G| = |H| \cdot [G:H]$ かつ $\gcd(p, [G:H]) = 1$ より, K は G の pシロー部分群になる.
- したがって, 任意の部分群 $H \subsetneq G$ に対して, $[G:H]$ が p で割り切れると仮定して良い. (*)
  G の自分自身への共役作用を考える. $x_1, \dots, x_r \in G$ を軌道の完全代表系とする.
  $$|G| = \sum_{i=1}^{r} [G : G_{x_i}] \quad \text{が成り立つ.}$$
  G の固定点全体の集合は, G の中心 $Z(G)$ である. よって,
  $$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} [G : G_{x_i}] \quad \text{である.}$$
  $x_i \notin Z(G)$ のとき, $G_{x_i} \subsetneq G$ が成り立つ. 仮定 (*) より,
  $$|Z(G)| \equiv |G| \equiv 0 \mod p.$$

したがって, $Z(G) \neq \{e\}$ である. また, 定理5.1.1. より, 位数pの元 $x \in Z(G)$ がとれる.

$H = \langle x \rangle$ とおく. $H \subset Z(G)$ だから, 明かに $H \lhd G$ である.

$G' = G/H$ とおき, 自然な準同型 $\pi : G \to G'$ を考える. $|G'| < |G|$ であることを注意する.

帰納法の仮定より, G' においては pシロー部分群 $K' \subset G'$ が存在する.

$K = \pi^{-1}(K')$ とおくと, K は G のpシロー部分群になることを説明する.

π を制限された準同型 $\pi' : K \longrightarrow K'$ を考える. 明かに π' は全単射であり,

$\mathrm{Ker}(\pi') = H$ である. よって, 群同型 $K/H \simeq K'$ が得られる.

ゆえに, $|K| = |H| \cdot |K'| = p \cdot |K'|$ である.

同様に $|G| = |H| \cdot |G'| = p|G'|$ が成り立つので, K は G のpシロー部分群である.

□

定理5.3.3. G を有限群とし, p を $|G|$ の素因数とする.

(i) $H \subset G$ を p部分群とすると, $H \subset K$ となるpシロー部分群 K が存在する.

(ii) K, K' をpシロー部分群とする. このとき, $K' = gKg^{-1}$ となる $g \in G$ が存在する. (つまり, K と K' は共役部分群である.

(iii) pシロー部分群の個数は p を法として 1 と合同である.

証明: (i) 定理5.3.2. より, pシロー部分群 $S \subset G$ が存在する.

$X = \{ xSx^{-1} \mid x \in G \}$ とおく. G は共役によって X に作用する.

この作用を H に制限することで, H の X への作用が得られる.

命題4.4.2. より, $|X| \equiv |X^H| \mod p$ である. $|X|$ を求める.

X は共役作用に関する S の軌道である. 補題4.3.4 より,

$|X| = [G : N_G(S)]$ である. $S \subset N_G(S) \subset G$ より, $[G : N_G(S)]$ は

$[G : S]$ の約数である. S がpシロー部分群なので, $[G:S]$ は p で割り切れない.

$[G : N_G(S)] \cdot [N_G(S) : S]$

よって，$|X|$ は p で割り切れない．ゆえに，$|X^H| \not\equiv 0 \mod p$ であり，とくに $X^H \neq \emptyset$ である．$S' \in X^H$ をとる．任意の $h \in H$ に対して $hS'h^{-1} = S'$ である．つまり，$H \subset N_G(S')$ が成り立つ．

命題 5.2.3. より，HS' は G の部分群であり，群同型

$$HS'/S' \simeq H/H \cap S' \quad \text{が存在する．}$$

よって，$|HS'| = \dfrac{|H| \cdot |S'|}{|H \cap S'|}$ であり，ゆえに HS' は p 部分群である．

S' が p シロー部分群なので，$HS' = S'$ となる．

したがって，$H \subset S'$ が成り立つ．以下のことを証明した．

> H を p 部分群とし，S を G の p シロー部分群とする．このとき，
> $H \subset gSg^{-1}$ を満たす $g \in G$ が存在する． (**)

(ii) K, K' を p シロー部分群とする．(**) より，$K' \subset gKg^{-1}$ となる $g \in G$ が存在する．$|K'| = |K| = |gKg^{-1}|$ より，$K' = gKg^{-1}$ となる．

(iii) S を p シロー部分群とし，$X = \{gSg^{-1} \mid g \in G\}$ を考える．S の X への共役作用を考える．(i) の証明より，$|X| \equiv |X^S| \mod p$．また，$S' \in X^S$ とすると，$S \subset N_G(S')$ が成り立つ．このとき，$S \subset S'$ となることを (i) の証明で示した．$|S| = |S'|$ より，$S = S'$ となる．このことから，$X^S = \{S\}$ が成り立つ．したがって，

$$|X| \equiv |X^S| = 1 \mod p \qquad \square$$

注意 5.3.4

H を G の p シロー部分群とする．$H \lhd G$ ならば，H は G の唯一の p シロー部分群である．とくに，有限アーベル群においては p シロー部分群は一意的に存在する．

例 5.3.5. $G = S_4$ とする. $|G| = 4! = 2^3 \cdot 3$ である.

$\sigma = (1\ 2\ 3\ 4)$ とする. $H = \langle \sigma \rangle$ は位数4の部分群で, 2シロー部分群 S に含まれる. S が2群なので, $Z(S) \neq \{e\}$ である (命題4.4.3参照).

$Z(S)$ を求める. 例4.3.3. より, $Cent_{S_4}(\sigma) = \langle \sigma \rangle$ である. よって,

- $Z(S) \subset Cent_{S_4}(\sigma) = \langle \sigma \rangle$
- $\sigma \notin Z(S)$, $\sigma^{-1} \notin Z(S)$ といえる.

よって, $Z(S) = \langle \sigma^2 \rangle$ でないといけない (とくに $S \subset Cent_{S_4}(\sigma^2)$ である).

$$\sigma^2 = (13)(24)$$ である.

明かに, $(13) \in Cent_{S_4}(\sigma^2)$ かつ $\langle \sigma \rangle \subset Cent_{S_4}(\sigma^2)$ である.

ゆえに, $Cent_{S_4}(\sigma^2) \supset \langle \sigma \rangle \cup (13)\langle \sigma \rangle$ であり, $|Cent_{S_4}(\sigma^2)| \geq 8$ となる. S_4 の中心は自明ただから, $Cent_{S_4}(\sigma^2) \neq S_4$. したがって,

$$Cent_{S_4}(\sigma^2) = \langle \sigma, (13) \rangle$$

であり, これは位数8の部分群である. つまり, $Cent_{S_4}(\sigma^2)$ は S_4 の2シロー部分群である.

全ての2シロー部分群は互いに共役である. 置換 τ に対して,

$\tau\, Cent_{S_4}(\sigma^2)\, \tau^{-1} = Cent_{S_4}(\tau\sigma^2\tau^{-1})$ が成り立つので, 全ての2シロー部分群は

- $Cent_{S_4}((13)(24)) = \langle (1234), (13) \rangle$
- $Cent_{S_4}((12)(34)) = \langle (1324), (12) \rangle$
- $Cent_{S_4}((14)(23)) = \langle (1243), (14) \rangle$ である.

2シロー部分群の個数は3である ($3 \equiv 1 \pmod 2$).

3シロー部分群は4つ存在する. これらは

$\langle (123) \rangle$, $\langle (124) \rangle$, $\langle (134) \rangle$, $\langle (234) \rangle$ である.

命題 5.3.6 G を有限群とし，p を $|G|$ を割り切る最小の素数とする．
H は G の部分群で，G における H の指数が p ならば，H は正規部分群である．

証明：G における H の正規化群を $K = N_G(H)$ とおく．

$K = G$ を示せば良い．$K \neq G$ であると仮定する．$H \subset K \subset G$ だから，

$$[G:H] = [G:K] \cdot [K:H]$$ が成り立つ．

$[G:H]$ は素数なので，$[K:H] = 1$ となる．よって，$K = H$ である．

集合 $X = \{ gHg^{-1} \mid g \in G \}$ を考える．

X は共役作用に関する H の軌道である．補題 4.3.4. より，

$|X| = [G:K] = [G:H] = p$ が成り立つ．G は共役作用によって X に作用する．補題 4.1.2. から，この作用に対応する群準同型

$$\varphi : G \longrightarrow Bij(X)$$

が得られる．$|X| = p$ より，$Bij(X) \simeq S_p$ であり，$|Bij(X)| = p!$ である．

また，$g \in Ker(\varphi)$ とすると，$gHg^{-1} = H$ であり，ゆえに $g \in K = H$．

よって，$Ker(\varphi) \subset H$ である．

準同型定理より，$G/_{Ker(\varphi)} \xrightarrow{\sim} Im(\varphi)$ である．

- よって，$[G:Ker(\varphi)]$ は $p!$ の約数である．
- また，$[G:Ker(\varphi)]$ は $|G|$ を割り切る．

p は $|G|$ の最小の素因数であるので，$[G:Ker(\varphi)] = p$ といえる．

よって，$\underbrace{[G:Ker(\varphi)]}_{=p} = \underbrace{[G:H]}_{=p} \times [H:Ker(\varphi)]$ であり，ゆえに $H = Ker(\varphi)$

が成り立つ．準同型の核は常に正規部分群だから，$H \lhd G$ となり，

$H = K$ に矛盾する．よって，$K = G$ であり，H は G の正規部分群である．□

例 5.3.7 : G を位数 35 の群とする.

H_7, H_5 をそれぞれ G の 7 シロー部分群, 5 シロー部分群とする.

命題 5.3.6 より, $H_7 \triangleleft G$ である. よって, G は共役によって H_7 に作用する.

この作用を制限し, H_5 の H_7 への共役作用を考える. この作用に対応する準同型

$$\varphi : H_5 \longrightarrow Bij(H_7) \qquad \text{を考える.}$$
$$g \longmapsto \varphi_g$$

ここで, φ_g は $\varphi_g(x) = gxg^{-1}$ で定まる全単射である.

明かに, φ_g は H_7 の自己同型である. よって, φ の像は

部分群 $Aut(H_7) \subset Bij(H_7)$ に含まれる.

> $Aut(\mathbb{Z}/7\mathbb{Z})$ を求める. $\gcd(k,7)=1$ のとき,
>
> $$v_k : \mathbb{Z}/7\mathbb{Z} \longrightarrow \mathbb{Z}/7\mathbb{Z} \quad \text{は自己同型である.}$$
> $$\bar{n} \longmapsto \bar{k}\cdot\bar{n}$$
>
> 写像
>
> $$v : (\mathbb{Z}/7\mathbb{Z})^\times \longrightarrow Aut(\mathbb{Z}/7\mathbb{Z})$$
> $$\bar{k} \longmapsto v_{\bar{k}}$$
>
> は明かに単射である. また, $f \in Aut(\mathbb{Z}/7\mathbb{Z})$ とすると, $f(\bar{1})$ は $\mathbb{Z}/7\mathbb{Z}$ の生成元である. ゆえに, $f(\bar{1}) = \bar{k}$ $(\gcd(7,k)=1)$ と書ける.
>
> よって, $f(\bar{n}) = f(n\bar{1}) = n\bar{k} = v_k(\bar{n})$ であり, ゆえに $f = v_{\bar{k}}$ である.
>
> したがって, v は全単射である (実は, v は群同型である)

とくに, $|Aut(H_7)| = |(\mathbb{Z}/7\mathbb{Z})^\times| = 6$ である.

このことから, $Im(\varphi)$ の位数は 6 の約数である. また, $H_5/Ker\varphi \simeq Im(\varphi)$ より, $|Im(\varphi)|$ は $|H_5| = 5$ の約数である. よって, $|Im(\varphi)| = 1$, $Im(\varphi) = \{id\}$

である．つまり，

任意の $g \in H_5$, $h \in H_7$ に対して，$\varphi_g(x) = gxg^{-1} = x$ である． (*)

$H_5 = \langle a \rangle$, $H_7 = \langle b \rangle$ となる元 $a, b \in G$ をとる．

(*) より，$\langle a, b \rangle$ はアーベル群となる．

a と b の位数が互いに素であるので，ab の位数は $5 \cdot 7 = 35$ である．以上より，$G = \langle ab \rangle$ となる．よって，

位数 35 の群は巡回群である．

§6. 有限生成アーベル群

§6.1. アーベル群の直和

- $(A_i)_{i\in I}$ をアーベル群の族とする. $(A_i)_{i\in I}$ の直和 $\bigoplus_{i\in I} A_i$ は以下のように定義される.

$$\bigoplus_{i\in I} A_i = \left\{ (x_i)_{i\in I} \in \prod_{i\in I} A_i \;\middle|\; \text{有限個の } i\in I \text{ を除いて } x_i = 0 \right\}$$

  I が有限ならば, $\bigoplus_{i\in I} A_i = \prod_{i\in I} A_i$ である.

- A をアーベル群とし, 全ての $i\in I$ に対して $A_i = A$ とする. このとき, $\bigoplus_{i\in I} A_i$ を単に $A^{(I)}$ と書く.

- A をアーベル群とし, B, C を A の部分群とする. 任意の $a\in A$ が一意に
  $a = b + c$ $(b\in B, c\in C)$ と表されるときに, $A = B\oplus C$ と書く.
  明かに, $A = B\oplus C \iff A = B+C$ かつ $B\cap C = 0$.

定義 6.1.1 (自由アーベル群) A をアーベル群とし, $\{x_i\}_{i\in I}$ を A の元の族とする.
$\{x_i\}_{i\in I}$ は A の **基底** であるとは, 任意の $x\in A$ が一意に $x = \sum_{i\in I} a_i x_i$
($a_i\in\mathbb{Z}$ であり, 有限個を除いて $a_i = 0$) と表されることをいう. このとき,
A は **自由アーベル群** であるという.

A を自由アーベル群とし, $\{x_i\}_{i\in I}$ を A の基底とする. 写像

$$\varphi : \mathbb{Z}^{(I)} \longrightarrow A, \quad (a_i)_{i\in I} \longmapsto \sum_{i\in I} a_i x_i$$

は群同型である. よって, $A \simeq \mathbb{Z}^{(I)}$ である.

逆に, I を集合とすると, $\mathbb{Z}^{(I)}$ は自由アーベル群である. $j\in I$ に対して,

$$e_j = (\delta_{ij})_i \quad \left(\text{ただし } \delta_{ij} = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{if } i\neq j \end{cases}\right) \text{ とおくと,}$$

$\{e_j\}_{j\in I}$ は $\mathbb{Z}^{(I)}$ の基底をなす.

例 6.1.2.

正の有理数全体の集合を $\mathbb{Q}_{>0}$ と書く.

明かに, $\mathbb{Q}_{>0}$ は乗法に関して群をなす. $\mathcal{P}$ を素数全体の集合とする.

任意の $x \in \mathbb{Q}_{>0}$ は一意に $x = \prod_{p \in \mathcal{P}} p^{v_p(x)}$ $\left(v_p(x) \in \mathbb{Z},\ \text{有限個の } p \text{ を除いて } v_p(x) = 0\right)$

と表される. ゆえに, $\mathbb{Q}_{>0}$ は自由アーベル群であり, $\mathcal{P}$ はその基底をなす.

補題 6.1.3. A をアーベル群とする. このとき, 準同型 $\mathbb{Z}^{(I)} \to A$ と写像 $I \to A$ は一対一で対応している. すなわち, 以下の写像は全単射である.

$$\{\text{群準同型 } \mathbb{Z}^{(I)} \xrightarrow{f} A\} \longrightarrow \{\text{写像 } I \xrightarrow{\varphi} A\}$$

$$f \longmapsto \left(\varphi : I \to A,\ i \mapsto f(e_i)\right)$$

$$\left(\mathbb{Z}^{(I)} \to A,\ (a_i)_i \mapsto \sum_{i \in I} a_i \varphi(i)\right) \longleftarrow \varphi$$

証明: 容易に確認できる. □

明かに, $\mathbb{Z}^{(I)}$ が有限生成である $\iff$ I が有限である.

命題 6.1.4. n, m を自然数とする. $\mathbb{Z}^n$ と $\mathbb{Z}^m$ が同型ならば, $n = m$ となる.

証明: 群同型 $f : \mathbb{Z}^n \to \mathbb{Z}^m$ が存在すると仮定する.

$2\mathbb{Z}^n = \{2x \mid x \in \mathbb{Z}^n\}$ を考える. 明かに, $f(2\mathbb{Z}^n) = 2f(\mathbb{Z}^n) = 2\mathbb{Z}^m$ である.

ゆえに, f は同型 $\mathbb{Z}^n/2\mathbb{Z}^n \to \mathbb{Z}^m/2\mathbb{Z}^m$ を誘導する.

準同型 $\mathbb{Z}^n \xrightarrow{\pi} (\mathbb{Z}/2\mathbb{Z})^n$ は全射であり，$\mathrm{Ker}(\pi) = 2\mathbb{Z}^n$ が成り立つ．

$(k_1, \cdots, k_n) \longmapsto (\overline{k_1}, \cdots, \overline{k_n})$

よって，$\mathbb{Z}^n/2\mathbb{Z}^n \simeq (\mathbb{Z}/2\mathbb{Z})^n$ である．したがって，群同型 $(\mathbb{Z}/2\mathbb{Z})^n \to (\mathbb{Z}/2\mathbb{Z})^m$ が得られる．とくに，濃度を比べれば，$2^n = 2^m$ となり，ゆえに $n = m$ が成り立つ． □

定義 6.1.5 (階数)

A を有限生成自由アーベル群とする．命題 6.1.4 より，A の基底を構成する元の個数は基底の取り方によらない．この個数は A の**階数**という．

補題 6.1.6 A, A' をアーベル群とし，$f : A \to A'$ を全準同型とする．また，A' が自由アーベル群であるとする．このとき，$A = B \oplus \mathrm{Ker}(f)$ となる部分群 $B \subset A$ が存在する．さらに，f の B への制限は群同型 $B \xrightarrow{f} A'$ である．

証明：$\{x_i'\}_{i \in I}$ を A' の基底とする．また，$f(x_i) = x_i'$ $(i \in I)$ となる A の元 x_i をとる．補題 6.1.3 より，$g(x_i') = x_i$ を満たすただ一つの準同型

$$g : A' \longrightarrow A$$

が存在する．よって，$f \circ g(x_i') = f(g(x_i')) = f(x_i) = x_i'$ である．

これより $f \circ g\left(\sum_i k_i x_i'\right) = \sum_i k_i x_i'$ であり，ゆえに $f \circ g = id_{A'}$ である．

$B = \mathrm{Im}(g) = \langle \{x_i \mid i \in I\} \rangle$ とおく．

$x \in B \cap \mathrm{Ker}(f)$ とし，$x = g(y)$ $(y \in A')$ とすると，$0 = f(x) = f(g(y)) = y$ となる．よって $x = 0$ となる．したがって，$B \cap \mathrm{Ker}(f) = 0$ である．

また，$x \in A$ とする．$x = g(f(x)) + (x - g(f(x)))$ と書ける．

$b = g(f(x))$，$c = x - g(f(x))$ とおく．

$f(c) = f(x) - f(g(f(x))) = f(x) - f(x) = 0$ より，$c \in \mathrm{Ker}(f)$

よって，$x = b + c \in B + \mathrm{Ker}(f)$ である．したがって，$A = B + \mathrm{Ker}(f)$ である．

以上より，$A = B \oplus \mathrm{Ker}(f)$ が成り立つ．

f の B への制限が群同型 $B \to A'$ であることは簡単に確認できる．

□

定理 6.1.7

A を階数 n の有限生成自由アーベル群とし，$B \subset A$ を部分群とする．

このとき，B は有限生成自由アーベル群であり，さらに B の階数は $\leq n$ である．

証明：n に関する数学的帰納法によって証明する．

$n = 1$ のとき，$\mathbb{Z}$ の部分群は $n\mathbb{Z}$ $(n \in \mathbb{Z})$ であるので，主張が成り立つ．

$n > 1$ とし，$\{x_1, \dots, x_n\}$ を A の基底とする．よって，$A = \mathbb{Z}x_1 \oplus \dots \oplus \mathbb{Z}x_n$ と書ける．

射影 $f : A \to \mathbb{Z}x_1$ $\left(\sum_{i=1}^{n} k_i x_i \mapsto k_1 x_1\right)$ を考えて，$B_1 = B \cap \mathrm{Ker}(f)$ とおく．

B_1 が $\mathbb{Z}x_2 \oplus \dots \oplus \mathbb{Z}x_n$ に含まれるので，帰納法の仮定より B_1 は自由群であり，さらに B_1 の階数は $\leq n-1$ である．$B' = f(B)$ とおくと，f が全準同型 $B \to B'$ を誘導する．補題 6.1.6 より，$B = B_1 \oplus C$ となる部分群 $C \subset B$ が存在し，さらに $C \simeq B'$ である．よって，C は自由アーベル群であり，C の階数は ≤ 1 である．

以上より，B は自由群であり，その階数は $\leq n$ である．

□

§6.2. 有限アーベル群

Aを有限アーベル群とする. 素数 p について, 部分集合 $A(p)$ を

$A(p) = \{x \in A \mid x$の位数は pのべき数である$\}$ で定義する.

Aにおいては, ただ一つの pシロー部分群 Sが存在する (注意 5.3.4 参照).

明かに, $S \subset A(p)$ が成り立つ. 逆に, xの位数が pのべきであるなら代, $H = \langle x \rangle$ は p部分群になる. 定理 5.3.3. (i) より, $H \subset S$ である.

これより, $A(p) = S$ となり,

> $A(p)$は Aの (唯一の) pシロー部分群である

定理 6.2.1. Aの位数を nとおき, $n = p_1^{k_1} \cdots p_r^{k_r}$ を nの素因数分解とする. このとき,

$$A = A(p_1) \oplus A(p_2) \oplus \cdots \oplus A(p_r)$$

が成り立つ.

証明: 写像

$$\varphi : A(p_1) \oplus \cdots \oplus A(p_r) \longrightarrow A \qquad (x_1, \cdots, x_r) \longmapsto x_1 + \cdots + x_r$$

を考える.

φが単射であることを示す. $(x_1, \cdots, x_r) \in \mathrm{Ker}(\varphi)$ とする.

$$x_1 + x_2 + \cdots + x_r = 0 \quad \text{である.}$$

$D = p_2 \cdots p_r$ とおくと, $D^N x_2 = \cdots = D^N x_r = 0$ となる $N \geq 1$ が存在する.

よって, $D^N x_1 = -(D^N x_1 + \cdots + D^N x_r) = 0$ となる.

Dと p_1が互いに素だから, $x_1 = 0$ といえる. 同様に $x_2 = \cdots = x_r = 0$ が成り立つ. したがって, φは単射である.

$A(p_i)$ は A の p_i シロー部分群だから，その位数は $p_i^{k_i}$ である．よって，
$A(p_1)\oplus\cdots\oplus A(p_r)$ の位数は $p_1^{k_1}\cdots p_r^{k_r}=n$ である．ゆえに，φ は全単射である．

□

定理 6.2.2. A をアーベル p 群とする．このとき，

$$A \simeq \mathbb{Z}/p^{r_1}\mathbb{Z} \times \mathbb{Z}/p^{r_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_m}\mathbb{Z} \quad \text{かつ} \quad r_1 \geq r_2 \geq \cdots \geq r_m \geq 1$$

を満たす自然数 $r_1,\ldots,r_m$ が存在する．さらに，$r_1,\ldots,r_m$ は一意に定まる．

注意

補題 6.2.3. A をアーベル p 群とする．a_1 を A の最大位数の元とし，$A_1=\langle a_1\rangle$ とおく．
自然な写像 $A\to A/A_1$ を π とおく．このとき，A/A_1 の任意の元 $\bar{y}$ に対して，

$$\pi(x)=\bar{y} \quad \text{かつ} \quad 「x\text{の位数} = \bar{y}\text{の位数}」$$

を満たす $x\in A$ が存在する．

証明： a_1 の位数を p^{r_1} とおく．A/A_1 が p 群なので，$\bar{y}$ の位数は p のべき p^r $(r\geq 1)$ である．$\pi(y)=\bar{y}$ となる $y\in A$ をとる．

$\pi(p^r y)=p^r\bar{y}=0$ より，$p^r y\in A_1$ である．よって，$p^r y=n a_1$ となる $0\leq n<p^{r_1}$ がある．

$n=p^k n'$ $(\gcd(p,n')=1)$ とする．補題 3.3.3 より，$na_1=p^k n' a_1$ の位数は p^{r_1-k} である．よって，y の位数は p^{r+r_1-k} である．a_1 が最大位数の元だから，

$r+r_1-k\leq r_1$ であり，よって $r\leq k$ が成り立つ．

したがって，$p^r y=p^r(p^{k-r}n'a_1)$ と書ける．

$x=y-p^{k-r}n'a_1$ と定めると，$\pi(x)=\bar{y}$ かつ $p^r x=0$ が成り立つ．

ゆえに x の位数は p^r の約数である．また，$mx=0$ ならば，$m\bar{y}=\pi(mx)=0$ より，

m は p^r の倍数である．よって，x の位数は p^r である．

□

$p^{r_1}/\gcd(p^{r_1},n)$

定理6.2.2 の証明：

まず，分解の存在性を示す． A の位数に関する数学的帰納法において証明する．

a_1 を A の最大位数の元とし，$A_1 = \langle a_1 \rangle$ とおく．帰納法の仮定より，

$$A/A_1 = \overline{A}_2 \oplus \overline{A}_3 \oplus \dots \oplus \overline{A}_m \qquad (*)$$

となる巡回部分群 $\overline{A}_2, \overline{A}_3, \dots, \overline{A}_m \subset A/A_1$ が存在する．

さらに，$\overline{A}_i$ $(2 \le i \le m)$ の位数は p^{r_i} $(r_i \ge 1)$ であり，$p^{r_2} \ge p^{r_3} \ge \dots \ge p^{r_m}$ が成り立つ．

$\overline{a}_i \in \overline{A}_i$ $(2 \le i \le m)$ を $\overline{A}_i$ の生成元とする．補題 6.2.3 より，$\overline{a}_i$ と同じ位数の代表元 $a_i \in A$ がとれる．

$A_i = \langle a_i \rangle$ と定義する $(2 \le i \le m)$． $A = A_1 \oplus A_2 \oplus \dots \oplus A_m$ を示せば良い．

$x \in A$ に対して，A_1 による x の剰余類 $\overline{x}$ は $(*)$ より

$$\overline{x} = d_2 \overline{a}_2 + \dots + d_m \overline{a}_m \qquad (d_1, \dots, d_m \in \mathbb{Z})$$

と書ける．よって，$x - (d_2 a_2 + \dots + d_m a_m) \in A_1$ であり，ゆえに

$$x = d_1 a_1 + d_2 a_2 + \dots + d_m a_m$$

となる $d_1 \in \mathbb{Z}$ がある．したがって，$A = A_1 + A_2 + \dots + A_m$ である．

$(*)$ より，A/A_1 の位数は $p^{r_2} \times \dots \times p^{r_m}$ である．

$|A| = |A_1| \cdot [A : A_1]$ より，A の位数は $p^{r_1} \times p^{r_2} \times \dots \times p^{r_m}$ である．これより，写像

$$\varphi : A_1 \oplus \dots \oplus A_m \longrightarrow A \qquad \text{は}$$
$$(x_1, \dots, x_m) \longmapsto x_1 + \dots + x_m$$

濃度が等しい集合の間の全射である．よって，φ は全単射になる．

以上より，$A = A_1 \oplus A_2 \oplus \dots \oplus A_m$ である．

$r_1, r_2, \dots, r_m$ の一意性を示す．帰納法によって証明する．

$A = A_1 \oplus \dots \oplus A_m$ （A_i の位数は p^{r_i}，$r_1 \geq r_2 \geq \dots \geq r_m \geq 1$）かつ

$A = A_1' \oplus \dots \oplus A_{m'}'$ （A_i' の位数は $p^{r_i'}$，$r_1' \geq r_2' \geq \dots \geq r_{m'}' \geq 1$）

と書けるとする．よって，$pA = pA_1 \oplus \dots \oplus pA_m = pA_1' \oplus \dots \oplus pA_{m'}'$ である．

pA_i は位数 p^{r_i-1} の巡回群である．よって，$pA_i = 0 \Leftrightarrow r_i = 1$ である．

- $r_m, r_{m'}' > 1$ ならば，帰納法の仮定より，$m = m'$ かつ $r_i - 1 = r_i' - 1$ $(i = 1, \dots, m)$ が成り立つ．よって，$r_i = r_i'$ となり，主張が従う．
- 一般の場合に，

$r_1 \geq \dots \geq r_j > 1$ かつ $r_{j+1} = r_{j+2} = \dots = r_m = 1$

$r_1' \geq \dots \geq r_{j'}' > 1$ かつ $r_{j'+1}' = r_{j'+2}' = \dots = r_{m'}' = 1$

とする．よって，$pA = pA_1 \oplus \dots \oplus pA_j = pA_1' \oplus \dots \oplus pA_{j'}'$ である．

帰納法の仮定より，$j = j'$ かつ $r_i - 1 = r_i' - 1$ $(1 \leq i \leq j)$ が成り立つ．

$(**)$

したがって，A の位数は

$$|A| = p^{r_1} \times \dots \times p^{r_j} \times \underbrace{p \times \dots \times p}_{m-j\text{個}} = p^{r_1'} \times \dots \times p^{r_{j'}'} \times \underbrace{p \times \dots \times p}_{m'-j'\text{個}}$$

$$= p^{r_1} \times \dots \times p^{r_j} \times \underbrace{p \times \dots \times p}_{m'-j\text{個}}$$

（$=$ は $(**)$ より）

ゆえに，$m = m'$ であり，主張が従う．

□

系 6.2.4. A を有限アーベル群とする.

$A \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ となる $n_1, \ldots, n_k \geq 2$ が存在する.

証明：定理 6.2.1. と定理 6.2.2. から分かる. □

$\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ などが成り立つので, 必ずしも $n_1, \ldots, n_k$ が一意に定まるとは限らない.

§6.3. 有限生成アーベル群

定義 6.3.1.（ねじれ元, ねじれ部分群）. A をアーベル群とする. A の元 x が**ねじれ元**であるとは, x の位数が有限であることをいう. A のねじれ元全体の集合は A の**ねじれ部分群**といい, A_{tor} と書く.

A のねじれ部分群は実際に部分群である. なぜならば,

- 明かに $0 \in A_{tor}$ である.
- $x, y \in A_{tor}$ とし, $nx = my = 0$ $(n, m \geq 1)$ とすると, $nm(x-y) = nmx - nmy = 0 - 0 = 0$ となる.

よって, A_{tor} は A の部分群である.

$A_{tor} = \{0\}$ のとき, A は**ねじれのない群**とよぶ.

例 6.3.2. A を自由アーベル群とし，$A \simeq \mathbb{Z}^{(I)}$ となる集合 I をとる．
$x=(x_i)_{i\in I} \in \mathbb{Z}^{(I)}$ とする．
$x \neq 0$ のとき，$x_j \neq 0$ となる $j \in I$ がある．よって，任意の $n \geq 1$ に対して，$nx = (nx_i)_{i\in I} \neq 0$ となる．これより，$A_{tor} = \{0\}$ である．

したがって，自由アーベル群はねじれのない群である．

定理 6.3.3. A をねじれのない有限生成アーベル群とする．
このとき，A は自由アーベル群である．

証明：S を A の有限生成系とする．A の元 $x_1,\dots,x_n$ に対して，次の条件を考える．

「$a_1x_1+\dots+a_nx_n=0$ $(a_1,\dots,a_n\in\mathbb{Z})$ ならば，$a_1=a_2=\dots=a_n=0$ である」 (*)

つまり，$x_1,\dots,x_n$ が「$\mathbb{Z}$ 上線型独立である」という条件である．

$\{x_1,\dots,x_n\}$ は S の部分集合で，上の条件 (*) を満たす最大のものとする．つまり，$x_1,\dots,x_n$ は (*) を満たすが，任意の $y \in S\setminus\{x_1,\dots,x_n\}$ に対して，$\{x_1,\dots,x_n,y\}$ は (*) を満たさない．

B を $x_1,\dots,x_n$ で生成された部分群とする．$x_1,\dots,x_n$ が (*) を満たすので，

$$B = \mathbb{Z}x_1 \oplus \dots \oplus \mathbb{Z}x_n$$ である（とくに，B は自由アーベル群である）．

$y \in S\setminus\{x_1,\dots,x_n\}$ とする．このとき，$my+a_1x_1+\dots+a_nx_n=0$ となる $m,a_1,\dots,a_n\in\mathbb{Z}$ $(m\neq 0)$ が存在する．
とくに，$my \in B$ となる．よって，$S=\{y_1,y_2,\dots,y_N\}$ とおくと，
任意の $1\leq i\leq N$ に対して，$m_iy_i \in B$ となる $m_i \neq 0$ が存在する．

$m = m_1 m_2 \cdots m_N$ とおくと，全ての $1 \leq i \leq N$ に対して，$m y_i \in B$ である．

S が A を生成するので，任意の $x \in A$ に対して，$mx \in B$ が成り立つ．

ゆえに，写像 $\varphi : A \longrightarrow B$，$x \longmapsto mx$ が得られる．

A がねじれのない群だから，φ は単射である．したがって，A は B の部分群 $\varphi(A) = mA$ と同型である．B が自由アーベル群であるので $\varphi(A)$ は自由アーベル群である（定理 6.1.7 参照）．主張が従う．

□

定理 6.3.4 A を有限生成アーベル群とする．

(i) A_{tor} は有限アーベル群である．

(ii) A/A_{tor} は有限生成自由アーベル群である．

(iii) $A = B \oplus A_{tor}$ となる有限生成自由アーベル部分群 B が存在．

(iv) $A \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z}$ となる $r \geq 0$，$d_1, \ldots, d_m \geq 1$ が存在．

証明：

(i) $\{x_1, \ldots, x_n\}$ を A の生成系とする．写像

$$\varphi : \mathbb{Z}^n \longrightarrow A,\quad (a_1, \ldots, a_n) \longmapsto a_1 x_1 + \ldots + a_n x_n$$

は全射である．

$\varphi^{-1}(A_{tor})$ は $\mathbb{Z}^n$ の部分群である．定理 6.1.7 より，$\varphi^{-1}(A_{tor})$ は有限生成自由アーベル群である．

とくに，$\varphi^{-1}(A_{tor}) = \langle s_1, \ldots, s_k \rangle$ となる $s_1, \ldots, s_k \in \mathbb{Z}^n$ が存在する．

よって，$A_{tor} = \varphi(\varphi^{-1}(A_{tor})) = \langle \varphi(s_1), \ldots, \varphi(s_k) \rangle$ であり，ゆえに A_{tor} は有限生成である．

A_{tor} がねじれ元からなるので，A_{tor} は有限群である．

(ii) 明かに，A/A_{tor} は有限生成である．A/A_{tor} はねじれのない群であることを示す．

$x + A_{tor}$ $(x \in A)$ を A/A_{tor} のねじれ元とする．

A/A_{tor} の単位元

$m(x+A_{tor}) = mx + A_{tor} = A_{tor}$ となる $m \geq 1$ が存在する.

よって, $mx \in A_{tor}$ となる. ゆえに, $m' \geq 1$ が存在し, $m'mx = 0$ である.

これより, $x \in A_{tor}$ であり, $x + A_{tor} = A_{tor}$ となる. したがって, A/A_{tor} はねじれのない群である.

定理 6.3.3. より, A/A_{tor} は有限生成自由アーベル群である.

(iii) 全準同型 $\pi : A \to A/A_{tor}$ に補題 6.1.6 を適用することによって, 主張が従う.

(iv) は (iii) から分かる.

□