代数学C

§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，$\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$，$(x,y)\mapsto x+y$ 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 で表す．

定義1.1.1. 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．

上の条件が成り立つとき，演算が**結合的**であるという．半群において，元 $x\cdot(y\cdot z)$ はカッコの入れ方に依らないので，単に $x\cdot y\cdot z$（あるいは xyz）と書く．
同様に元 $x_1,x_2,\dots,x_n$ に対して，$x_1\cdot x_2\cdots x_n$ は一意的に定まる．

G を半群とし，$e\in G$ とする．任意の $x\in G$ に対して

$$x\cdot e=e\cdot x=x$$

が成り立つとき，e が**単位元**であるという．

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. 単位元をもつ半群を**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，$x \in G$ 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．逆元をもつ元を**可逆元**という．

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

x が可逆元であるときに，x の逆元を x^{-1} で表す．

注意 1.1.5
(i) e は常に可逆元であり，$e^{-1} = e$ が成り立つ．
(ii) 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．
(iii) 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
- $(\mathbb{Z}_{\geq 0}, +)$ はモノイドである．可逆元全体の集合は $\{0\}$ である．
- $(\mathbb{Z}, \times)$ ―――――――――― $\{\pm 1\}$ ――
- X を集合とする．写像 $X \xrightarrow{f} X$ 全体の集合を $\mathrm{Map}(X, X)$ と表す．
  写像の合成に関して $\mathrm{Map}(X, X)$ はモノイドをなし，その単位元は id_X （X の恒等写像）である．
  $\mathrm{Map}(X, X)$ の可逆元全体の集合は

$$G(X) = \{ X \xrightarrow{f} X \quad \text{全単射} \}$$ である．

- $(M(n, \mathbb{C}), \times)$ はモノイドである．その可逆元全体の集合は $GL(n, \mathbb{C})$ である．
  （正則行列）

- $(\mathbb{Z}/n\mathbb{Z}, \times)$ はモノイドである．可逆元全体の集合は $(\mathbb{Z}/n\mathbb{Z})^\times$ である．

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{ \overline{k} \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; k \text{と} n \text{は互いに素である} \right\}.$$

定義 1.1.7 任意の元が可逆元であるモノイドを **群** という．

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: $G = \{H\text{の可逆元}\}$ とおく．注意 1.1.5 (iii) より，G は H の演算について閉じている．
注意 1.1.5 (i) より $e \in G$ である．注意 1.1.5 (ii) より $x \in G \Rightarrow x^{-1} \in G$ が成り立つ．よって，G は群をなす． □

定義 1.1.9 G を群とする．任意の $x, y \in G$ に対して

$$x \cdot y = y \cdot x$$

が成り立つとき，G が可換群 (あるいはアーベル群) であるという．

例 1.1.10 命題 1.1.8 より

- $(\mathfrak{S}(X), \circ)$ は群である (X: 集合，$\circ$: 写像の合成)
- $(GL(n, \mathbb{C}), \times)$ は群である
- $\left((\mathbb{Z}/n\mathbb{Z})^\times, \times\right)$ はアーベル群である．

同様に，$(\mathbb{Z}/n\mathbb{Z}, +)$ はアーベル群である．

x を群 G の元とし，$n \in \mathbb{Z}$ とする．このとき

$$x^n = \begin{cases} e & \text{if} \quad n = 0 \\ \underbrace{x \cdots x}_{n\text{コ}} & \text{if} \quad n > 0 \\ \underbrace{x^{-1} \cdots x^{-1}}_{-n\text{コ}} & \text{if} \quad n < 0 \end{cases}$$

と定義する．

例えば，$x^{-2} = x^{-1} \cdot x^{-1} = (x^{-1})^2 = (x^2)^{-1}$

注意 1.1.11.

G がアーベル群のとき，その演算を「$+$」で表す場合がある．
合わせて以下の記号を使う：

演算	$\cdot$	$+$
単位元	e または 1	0
逆元	x^{-1}	$-x$
n 乗	x^n	nx
	xy^{-1}	$x-y$

定義 1.1.12 G_1, G_2 を群とする．$g_1, g_1' \in G_1$，$g_2, g_2' \in G_2$ に対して

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2')$$

とおくことによって直積 $G_1 \times G_2$ に演算を入れる．この演算に関して $G_1 \times G_2$ は群をなし，G_1 と G_2 の直積という．

§1.2. 部分群

定義 1.2.1 G を群とし，$H \subset G$ を部分集合とする．H が以下の3つの条件をみたすとき，**部分群**であるという．

(i) $e \in H$

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

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

補題 1.2.2 次の条件は互いに同値である

(i) H が G の部分群である．

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

証明: (i) $\Rightarrow$ (ii) は明らかである．

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

また，$x \in H$ とすると $x^{-1} = e \cdot x^{-1}$ と表せるので (ii) より $x^{-1} \in H$ である．

最後に $x, y \in H$ ならば

$$x \cdot y = x \cdot (y^{-1})^{-1}$$

と書ける．$x \in H$，$y^{-1} \in H$ より $x \cdot y \in H$ である．

以上より H は部分群である． □

例12.3

- 部分集合 $H \subset \mathbb{Z}$ が部分群である $\iff$ $H = n\mathbb{Z}$ $(n \geq 0)$ と書くことができる.
- 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12.4 G を群とし, $\mathcal{F} \neq \emptyset$ を G の部分群からなる集合とする. このとき, 共通部分

$$\bigcap_{H \in \mathcal{F}} H$$

は G の部分群である.

証明: $\forall H \in \mathcal{F}$, $e \in H$ より $e \in \bigcap_{H \in \mathcal{F}} H$ である.

$x, y \in \bigcap_{H \in \mathcal{F}} H$ とする. 全ての $H \in \mathcal{F}$ に対して $x, y \in H$ だから, $xy^{-1} \in H$ となる.

したがって $xy^{-1} \in \bigcap_{H \in \mathcal{F}} H$ となる. □

定義12.5 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

$$\langle S \rangle = \bigcap_{\substack{H: \text{部分群} \\ S \subset H}} H$$

によって定義される.

注意12.6

(i) すなわち, $\mathcal{F} = \{S$ を含む G の部分群$\}$ とすると, $\langle S \rangle = \bigcap_{H \in \mathcal{F}} H$ が成り立つ. 補題1.2.4より, $\langle S \rangle$ は部分群である.

(ii) $\langle S \rangle$ は S を含む G の部分群の中で最小のものである.

(iii) $S = \{x_1, \dots, x_n\}$ $(x_1, \dots, x_n \in G)$ のとき, $\langle S \rangle$ を単に $\langle x_1, \dots, x_n \rangle$ と書く.

(iv) $G = \langle S \rangle$ のとき, G が S で生成されるという.

命題1.2.7　$S \subset G$ を空でない部分集合とする．このとき，

$$\langle S \rangle = \left\{ s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n} \;\middle|\; n \geq 1,\ s_1, \ldots, s_n \in S,\ k_1, \ldots, k_n \in \mathbb{Z} \right\} \quad (*)$$

が成り立つ．

証明　$(*)$ の右辺を A とおき，$\langle S \rangle = A$ を示す．

H を S を含む部分群とする．$s_1, \ldots, s_n \in S$ について $s_1^{k_1} \cdots s_n^{k_n} \in H$ 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 が G の部分群であることを確認する．

$s \in H$ 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．したがって A が部分群である．

また，$S \subset A$ が成り立つので，$\langle S \rangle \subset A$ となる．以上より $\langle S \rangle = A$ である．　□

定義1.2.8　X を集合とする．$G(X)$ を X の対称群（あるいは置換群）という．$G(X)$ の単位元は恒等写像である．$X = \{1, 2, \ldots, n\}$ （n 自然数）の場合は $G(X) = G_n$ と書く．

例1.2.9：n を自然数とする．対称群 G_n は隣接互換で生成される．つまり，

$$G_n = \langle (12), (23), \ldots, (n-1\ n) \rangle$$

が成り立つ．

また，G_n は互換 (12) と　巡回置換 $\sigma = (1\ 2\ \cdots\ n)$ で生成される．つまり

$$G_n = \langle (12), \sigma \rangle$$

が成り立つ．

$G_n = \langle (12), \sigma \rangle$ を示す. 以下が成り立つ:

$$\begin{aligned}
\sigma(1\,2)\sigma^{-1} &= (\sigma(1)\ \ \sigma(2)) = (2\,3) \\
\sigma^2(1\,2)\sigma^{-2} &= (\sigma^2(1)\ \ \sigma^2(2)) = (3\,4) \\
&\vdots \qquad\qquad \vdots \\
\sigma^{n-2}(1\,2)\sigma^{-(n-2)} &= (\sigma^{n-2}(1)\ \ \sigma^{n-2}(2)) = (n-1\ \ n)
\end{aligned}$$

よって, $(1\,2), (2\,3), \ldots, (n-1\ n) \in \langle (12), \sigma \rangle$ である.
これらが G_n を生成するので, $\{(12), \sigma\}$ も G_n を生成する.

§2. 準同型

§2.1. 定義

定義 2.1.1 G_1, G_2 を群とし，$f: G_1 \to G_2$ を写像とする．任意の $x, y \in G_1$ に対して

$$f(xy) = f(x)f(y)$$

が成り立つとき，f を群準同型という．

補題 2.1.2 $f: G_1 \to G_2$ を群準同型とする．

(i) 任意の $x \in G_1$ に対して，$f(x^{-1}) = f(x)^{-1}$ である．

(ii) $f(e_1) = e_2$ （ただし e_1, e_2 はそれぞれ G_1 と G_2 の単位元である）

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

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

定義 2.1.3 $f: G_1 \to G_2$ を群準同型とする．f の核 $\mathrm{Ker}(f)$，f の像 $\mathrm{Im}(f)$ は次のように定義される．

$$\mathrm{Ker}(f) = \{ x \in G_1 \mid f(x) = e_2 \}$$

$$\mathrm{Im}(f) = \{ f(x) \mid x \in G_1 \} = f(G_1).$$

例 2.1.4

- n を自然数とする.
  $f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ は 群 $(\mathbb{Z},+)$ から群 $(\mathbb{Z}/n\mathbb{Z},+)$ への群準同型である.
  $k \longmapsto \overline{k}$
  $\mathrm{Im}(f) = \mathbb{Z}/n\mathbb{Z}$, $\mathrm{Ker}(f) = n\mathbb{Z}$.

- $GL(n,\mathbb{C}) \xrightarrow{f} \mathbb{C}^*$ は 群 $(GL(n,\mathbb{C}),\times)$ から群 $(\mathbb{C}^*,\times)$ への群準同型である.
  $A \longmapsto \det(A)$

  $\mathrm{Im}(f) = \mathbb{C}^*$, $\mathrm{Ker}(f) = SL(n,\mathbb{C}) = \{ A \in GL(n,\mathbb{C}) \mid \det A = 1 \}$

- $\mathbb{R} \xrightarrow{f} U = \{ z \in \mathbb{C} \mid |z| = 1 \}$ は $(\mathbb{R},+)$ から $(U,\times)$ への準同型である.
  $x \longmapsto e^{2\pi i x}$
  $\mathrm{Im}(f) = U$, $\mathrm{Ker}(f) = \mathbb{Z}$.

補題 2.1.5 $f : G_1 \to G_2$ を群準同型とする. このとき, $\mathrm{Ker}(f)$ と $\mathrm{Im}(f)$ はそれぞれ G_1 と 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 2.1.6

(i) $f : G_1 \to G_2$ を群準同型とする. f が全単射であるとき, **群同型** であるという.

(ii) G を群とする. 群準同型 $f : G \to G$ を **G の自己準同型** という.

(iii) また, 群同型 $G \to G$ を **G の自己同型** という.

命題 2.1.7

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

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，

$$f\left(f^{-1}(xy)\right) = xy = f\left(f^{-1}(x)\right) f\left(f^{-1}(y)\right) = f\left(f^{-1}(x) f^{-1}(y)\right)$$ 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． □

群同型 $G_1 \longrightarrow G_2$ が存在するとき，$G_1 \simeq G_2$ と書く．

注意 2.1.8

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．

例 2.1.9

群 G が与えられているときに，G の自己同型群 $Aut(G)$ を

$$Aut(G) = \{ f: G \to G \quad \text{自己同型} \}$$

とおくことで定義する．$Aut(G)$ は $G(G)$ の部分群である．

（∵ $id_G \in Aut(G)$，　$f \in Aut(G) \Rightarrow f^{-1} \in Aut(G)$　（補題 2.1.7.）
$f, g \in Aut(G) \Rightarrow f \circ g \in Aut(G)$　（注意 2.1.8））

例えば，$G = \mathbb{Z}/n\mathbb{Z}$ とすると $Aut(G) \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$ である．

§2.2. 剰余類

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 と Hg を

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

と定義し，それぞれ（H による）左剰余類，右剰余類という．また，

$G/H = \{H$ による左剰余類$\}$，$H\backslash G = \{H$ による右剰余類$\}$

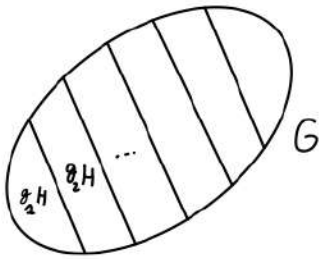
と定義する．

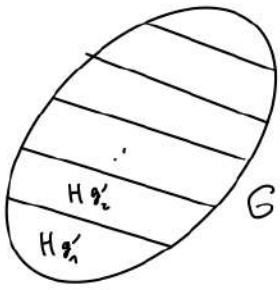
補題 2.2.1

(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．

同様に $Hg_1 = Hg_2$ または $Hg_1 \cap Hg_2 = \emptyset$ である．

(ii) G は左剰余類に分割される．同様に右剰余類に分割される．





証明：(i) $g_1H \cap g_2H \neq \emptyset$ とする．このとき，$h_1, h_2 \in H$ を用いて，$g_1h_1 = g_2h_2$ と書ける．よって，全ての $h \in H$ に対して，

$$g_1h = (g_1h_1)h_1^{-1}h = (g_2h_2)h_1^{-1}h = g_2\underbrace{(h_2h_1^{-1}h)}_{\in H} \in g_2H$$

である．ゆえに $g_1H \subset g_2H$ となる．同じく $g_2H \subset g_1H$ が成り立つ．したがって $g_1H = g_2H$ である．

(ii) $g \in G$ とする. 明らかに $g = g \cdot e \in gH$ であるので, g が左剰余類 gH に属する. (i) より G が左剰余類に分解される.

□

G がアーベル群のとき, $gH = Hg$ である.

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,

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

補題 2.2.3 Gを群とし，HをGの部分群とする．このとき，写像

$$G/H \longrightarrow {}_H\backslash G \qquad gH \longmapsto Hg^{-1}$$

は well-defined であり，全単射である．

証明： $g_1, g_2 \in G$とする．

$$\begin{aligned} g_1H = g_2H &\overset{\text{補題2.2.1}}{\iff} g_2 \in g_1H \\ &\iff g_2 = g_1 \cdot h \quad (h \in H) \\ &\iff g_2^{-1} = h' g_1^{-1} \quad (h' \in H) \\ &\iff g_2^{-1} \in Hg_1^{-1} \\ &\iff Hg_2^{-1} = Hg_1^{-1} \end{aligned}$$

以上より，写像 $gH \mapsto Hg^{-1}$ は well-defined であり，単射である．
明かに全射でもあるので，補題が従う． □

定義 2.2.4 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, $ghg^{-1} \in H$ が成り立つ.

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.

□

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 $f : G \to G'$ 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.

e': G' の単位元

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．

□

$H \subset G$ が正規部分群であるとき，次のように G/H に演算を定義することができる：$g_1, g_2 \in G$ に対して，

$$g_1H \cdot g_2H = g_1g_2H$$

と定義する．

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．

π は自然な射影とよばれる．

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. □

§2.3 準同型定理

定理 2.3.1 $f : G \to G'$ を群準同型とする. 写像

$$\tilde{f} : G/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$$
$$g\,\mathrm{Ker}(f) \longmapsto f(g)$$

は well-defined であり, 群同型 である

証明:

- まず, $\tilde{f}$ が well-defined であること を確認する. $H = \mathrm{Ker}(f)$ とおき, $gH = g'H$ とする. このとき, $g^{-1}g' \in H$ であるので, $f(g^{-1}g') = e$ である. 一方, $f(g^{-1}g') = f(g^{-1})f(g') = f(g)^{-1}f(g')$ より $f(g) = f(g')$ が成り立つ. 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: $g, g' \in G$ に対して
$\tilde{f}((gH)(g'H)) = \tilde{f}(gg'H) = f(gg') = f(g)f(g') = \tilde{f}(gH)\tilde{f}(g'H)$ 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. □

注意 2.3.2　$f : G \longrightarrow G'$　準同型.

・自然な写影 $G \longrightarrow G/\mathrm{Ker}(f)$ を π とおく.
$g \mapsto g\,\mathrm{Ker}(f)$

・自然な包含写像 $\mathrm{Im}(f) \hookrightarrow G'$ を ι とおく.
$x \longmapsto x$

f が以下のように分解できる:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ G/\mathrm{Ker}(f) & \xrightarrow[\tilde{f}]{} & \mathrm{Im}(f) \end{array}$$

すなわち $f = \iota \circ \tilde{f} \circ \pi$ が成り立つ.

注意 2.3.3　$f : G \to G'$ を群準同型とする.

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

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

例 2.3.4

(i) $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{R}) \;\middle|\; b = 0 \right\}$ とする. G は $GL(2,\mathbb{R})$ の部分群である. また,

$H = \left\{ \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \;\middle|\; x \in \mathbb{R} \right\}$ とおくと，H は G の正規部分群である．なぜならば，写像

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & \mathbb{R}^\times \times \mathbb{R}^\times \\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} & \longmapsto & (a, d) \end{array}$$

を考える．φ は群準同型であり，全射である．また，$H = \mathrm{Ker}(\varphi)$ であるので $H \triangleleft G$ であり，さらに $G/H \simeq \mathbb{R}^\times \times \mathbb{R}^\times$ である．

(ii) $f : \mathbb{R} \longrightarrow U = \{ z \in \mathbb{C} \mid |z| = 1 \}$, $x \longmapsto e^{2i\pi x}$

f は群準同型であり，$\mathrm{Ker}(f) = \mathbb{Z}$，$\mathrm{Im}(f) = U$ が成り立つ．

よって，$\mathbb{R}/\mathbb{Z} \simeq U$ である．

(iii) 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．

$\mathrm{Aut}(G)$ を G の自己同型群とする．$x \in G$ に対して，

$$\begin{array}{ccc} f_x : G & \longrightarrow & G \\ g & \longmapsto & xgx^{-1} \end{array}$$

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を **内部自己同型** という．

$$\begin{aligned} \varphi : G &\longrightarrow Aut(G) \\ x &\longmapsto f_x \end{aligned}$$

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）．

$Im(\varphi)$ は内部自己同型全体の部分群である．

$$\begin{aligned} Inn(G) &= \{ f \in Aut(G) \mid f \text{は内部自己同型} \} \\ &= Im(\varphi) \end{aligned}$$

とおく．

$$\begin{aligned} Ker(\varphi) &= \{ x \in G \mid f_x = id_G \} \\ &= \{ x \in G \mid \forall y \in G,\ xyx^{-1} = y \} \\ &= Z(G) \quad \text{が成り立つ．} \end{aligned}$$

よって，$G/Z(G) \simeq Inn(G)$ となる．

さらに，$Inn(G) \triangleleft Aut(G)$ が成り立つ．なぜならば，
$x \in G$, $\varphi \in Aut(G)$ とすると，

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

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．

第3章　群の位数

§3.1 定義

定義 3.1.1：Gを群とし，$g \in G$とする．

(i) **Gの位数**とは，Gの元の個数のことをいう．
(ii) **gの位数**とは，$\langle g \rangle$の元の個数のことをいう．gの位数を$\mathrm{ord}(g)$で表す．

$\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$が成り立つ．よって，写像

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow \langle g \rangle \\ n &\longmapsto g^n \end{aligned}$$

は全射である．また，明らかにφは準同型である．

$\mathrm{Ker}(\varphi) = \{ n \in \mathbb{Z} \mid g^n = e \}$　は

$\mathbb{Z}$の部分群であるので，$\mathrm{Ker}(\varphi) = m\mathbb{Z}$となる$m \geq 0$

が存在する．また，準同型定理より

$$\langle g \rangle \simeq \mathbb{Z}/\mathrm{Ker}(\varphi)$$

Case 1 : $m = 0$

このとき $\langle g \rangle \simeq \mathbb{Z}$ であり，g の位数は無限である．

また，$g^n = e$ をみたす $n \geq 1$ は存在しない．

Case 2 : $m \geq 1$

このとき $\mathrm{Ker}(\varphi) = m\mathbb{Z}$，$\langle g \rangle \simeq \mathbb{Z}/m\mathbb{Z}$ である．

よって，$\mathrm{ord}(g) = |\langle g \rangle| = |\mathbb{Z}/m\mathbb{Z}| = m$ である．

したがって，g の位数は $g^n = e$ をみたす自然数 n の中で最小のものである．

また，

$$g^n = e \iff n \text{ は } \mathrm{ord}(g) \text{ の倍数である．} \quad (*)$$

例 3.1.2 $G = GL(2, \mathbb{R})$ とし，$a = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$，$b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ とする．

$a^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ より a と b の位数はそれぞれ 2 である．

$b^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$a \cdot b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ であるので $(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ が成立つ.

ゆえに ab の位数は無限である.

§3.2. ラグランジュの定理

定義 3.2.1 G を群とし, H を G の部分群とする.
G における H の**指数**とは, 集合 G/H の元の個数のことをいう.

G における H の指数を $[G:H]$ で表す. 補題 2.2.3 全単射 $G/H \longrightarrow {}_H\backslash G$ が存在するので

$$[G:H] = |G/H| = |{}_H\backslash G| \quad \text{が成り立つ.}$$

G の元の個数が有限であるとき, G を**有限群**という.

定理 3.2.2 G を有限群とし, H を G の部分群とする.

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

が成り立つ.

証明：補題 2.2.1(ii) より G は左剰余類に分割される．つまり，

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

とおくと，$G = \bigsqcup_{i=1}^{n} g_iH$ 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．

とくに，$|gH| = |H|$ 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 3.2.3. G を有限群とし，G の位数を n とおく．
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)．(*) より $g^m = e$ である．

定理 3.2.2 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

□

§3.3 巡回群

定義 3.3.1 G を群とする. G が1つの元で生成されるとき, 巡回群であるという. $G=\langle g\rangle$ をみたす元 g を生成元という.

定理 3.3.2 G を巡回群とする.

(i) G が無限ならば, $G \simeq \mathbb{Z}$ である.

(ii) G が有限ならば, $G \simeq \mathbb{Z}/m\mathbb{Z}$, $m=|G|$ である.

証明: $G=\langle g\rangle$ とする. 準同型 $\varphi: \mathbb{Z} \longrightarrow G$, $n \longmapsto g^n$ を考える. 準同型定理から従う. □

例 3.3.3 巡回群 $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ を考える.

整数 $k \in \mathbb{Z}$ に対して, 次が成り立つ

$$\gcd(k,n)=1 \iff \overline{k} \text{ が } \mathbb{Z}/n\mathbb{Z} \text{ を生成する.}$$

例 3.3.4 : p を素数とする. $\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}, \times\right)$ は位数 $p-1$ の巡回群である.

例えば, $p=7$ とする. $\left(\mathbb{Z}/7\mathbb{Z}\right)^{\times} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ である.

- $\bar{1}$ の位数は 1
- $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{8} = \bar{1}$ より $\bar{2}$ の位数は 3
- $\bar{3}^2 = \bar{9} = \bar{2}$, $\bar{3}^3 = \bar{2}\times\bar{3} = \bar{6} = -\bar{1}$, $\bar{3}^4 = -\bar{3} = \bar{4}$, $\bar{3}^5 = \bar{4}\times\bar{3} = \bar{5}$, $\bar{3}^6 = \bar{1}$ より $\bar{3}$ の位数は 6

したがって $\left(\mathbb{Z}/7\mathbb{Z}\right)^{\times} = \langle \bar{3} \rangle$

第4章　群作用

§4.1. 定義と例

G を群とし，X を集合とする．また，写像

$$f : G \times X \longrightarrow X$$

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．

定義 4.11.

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，

$$g \cdot (g' \cdot x) = (gg') \cdot x$$

が成り立つ．

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

$$\varphi_g : \begin{array}{ccc} X & \longrightarrow & X \\ x & \longmapsto & g \cdot x \end{array}$$

によって定義する．φ_g が全単射である．なぜならば，全ての $x \in X$ に対して，

$$\varphi_g \circ \varphi_{g^{-1}}(x) = \varphi_g\left(\varphi_{g^{-1}}(x)\right) = g \cdot (g^{-1} \cdot x) \overset{\text{定義4.11 (ii)}}{=} (gg^{-1}) \cdot x = e \cdot x \overset{\text{定義4.11 (i)}}{=} x$$

が成り立つ．よって $\varphi_g \circ \varphi_{g^{-1}} = id_X$．同様に $\varphi_{g^{-1}} \circ \varphi_g = id_X$ であり，φ_g は全単射である．

すなわち, $\varphi_g \in \mathcal{G}(X)$ である. また, 次が成り立つ:

(i) $\varphi_e = id_X$

(ii) $\varphi_{g^{-1}} = (\varphi_g)^{-1}$

(iii) $\varphi_{gg'} = \varphi_g \cdot \varphi_{g'}$

(iii) より, 写像

$$\begin{aligned} \varphi : G &\longrightarrow \mathcal{G}(X) \\ g &\longmapsto \varphi_g \end{aligned}$$

は群準同型である. ゆえに, 以下の対応が得られる.

$$\left\{ \begin{array}{l} f : G \times X \longrightarrow X \\ G \text{の} X \text{への作用} \end{array} \right\} \longrightarrow \left\{ \text{準同型 } G \longrightarrow \mathcal{G}(X) \right\}$$

$$f \longmapsto \varphi$$

補題 4.1.2 上の写像は全単射である. つまり, 群作用 $G \times X \xrightarrow{f} X$ と準同型 $G \to \mathcal{G}(X)$ は一対一で対応している.

証明: $\varphi : G \to \mathcal{G}(X)$ を準同型とする.

$g \in G$, $x \in X$ に対して

$g \cdot x = \varphi(g)(x)$ とおくことで，G の X への作用が得られる． □

例 4.1.3

(i) $X = G$ とする．

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

G の G への作用が得られる．この作用は**左移動**とよばれる．

(ii) $g \cdot h = ghg^{-1}$ と定義することで，G の自分自身への作用が定まり，

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 $\mathcal{P}(X)$ への作用が得られる．

§4.2. 軌道

定義 4.2.1. $x \in X$ に対して,

$$Gx = \{ g \cdot x \mid g \in G \}$$

と定義し, x の (G による) 軌道という.

注意 4.2.2 $x, x' \in X$ に対して

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

と定義することで, X 上の同値関係が定まる.

$\sim$ が同値関係であることを check

- $x = e \cdot x$ 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,
  $x'' = g' \cdot (g \cdot x) = (g'g) x$ 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) $GL(n,\mathbb{R})$ の $\mathbb{R}^n$ への自然な作用を考える．

ちょうど二つの軌道が存在する：

- $x \in \mathbb{R}^n \setminus \{0\}$ のとき $Gx = \mathbb{R}^n \setminus \{0\}$
- $x = 0$ のとき $Gx = \{0\}$

$\mathbb{R}^n$ は軌道に分割される：

$$\mathbb{R}^n = (\mathbb{R}^n \setminus \{0\}) \sqcup \{0\}$$

(ii) Gを群とする．Gが共役によって自分自身に作用する．

Gの元hの軌道 $\{ghg^{-1} \mid g \in G\}$ を hの共役類 という．

$G = \mathfrak{S}_n$ の場合を考える

$\sigma, \tau \in \mathfrak{S}_n$ に対して，以下が成り立つ．

σとτが共役である $\Longleftrightarrow$
$\sigma = c_1 \cdots c_r$ （c_i：互いに素な巡回置換）
$\tau = c_1' \cdots c_s'$ （c_i'：互いに素な巡回置換）
と書く．このとき，$r = s$ かつ 順番を除いて
$c_1, \cdots, c_r$ の長さ が $c_1', \cdots, c_r'$ の長さと一致する．

例：$n = 5$とし，$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$，$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$ とする．

$\sigma = \underset{\| c_1}{(12)}\underset{\| c_2}{(354)}$，$\tau = \underset{\| c_1'}{(145)}\underset{\| c_2'}{(23)}$ となる．

よって，σとτは共役である．

したがって，S_3 においてちょうど3つの共役類が存在する．

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

S_4 の共役類：

- $\{id\}$
- (ab)
- (abc)
- $(ab)(cd)$
- $(abcd)$

§4.3. 安定化部分群

定義 4.3.1 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 の安定化部分群（あるいは x の固定部分群）という．

G_x が部分群であることを check．

- $e \cdot x = x$ より $e \in G_x$ である．
- $g \in G_x$ ならば，$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g)x = e \cdot x = x$ よって $g^{-1} \in G_x$
- $g, g' \in G_x$ ならば，$(gg') \cdot x = g \cdot (g' \cdot x) = g \cdot x = x$ より $gg' \in G_x$．

補題 4.3.2. $x \in X, g \in G$ に対して,

$$G_{g\cdot x} = g G_x g^{-1}$$ である.

証明: $g' \in G$ に対して,

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

H, H' は部分群で, $H' = gHg^{-1}$ $(g \in G)$ のとき, H と H' が 共役部分群 であるという.

例 4.3.3 $G = GL(2,\mathbb{R})$ とし, G の $\mathbb{R}^2$ への自然な作用を考える. $x = \begin{pmatrix}1\\0\end{pmatrix}$ とする. x の安定化部分群は

$$\begin{aligned} G_x &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{R}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \;\middle|\; b \in \mathbb{R}, d \in \mathbb{R}^\times \right\} \end{aligned}$$

である.

例 4.3.4. G を群とし，G の自分自身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．$\left(\text{よって，} g \in G_x \iff gx = xg \right)$ この部分群を

x の **中心化群** といい，**$Cent_G(x)$** で表す．
明らかに $\langle x \rangle \subset Cent_G(x)$ が成り立つ．

例えば，$G = \mathfrak{S}_3$ とし，$\sigma = (1\ 2\ 3)$ とする．

$\tau \in \mathfrak{S}_3$ に対して $\tau\sigma\tau^{-1} = \left(\tau(1)\ \tau(2)\ \tau(3) \right)$ である．

よって $\left| Cent_{\mathfrak{S}_3}(\sigma) \right| \leq 3$ である．ゆえに

$$Cent_{\mathfrak{S}_3}(\sigma) = \{ id, \sigma, \sigma^2 \} = \langle \sigma \rangle$$

同様に，長さ n の巡回置換 σ に対して

$$Cent_{\mathfrak{S}_n}(\sigma) = \langle \sigma \rangle \quad \text{である．}$$

群 G が集合 X に作用しているとする.

補題 4.3.5 $x \in X$ とする. 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 であることを確認する. $gG_x = g'G_x$ 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: $g\cdot x = g'\cdot x$

$\Rightarrow g'^{-1}\cdot(g\cdot x) = g'^{-1}\cdot(g'\cdot x)$

$\Rightarrow (g'^{-1}g)\cdot x = (g'^{-1}g')\cdot x = e\cdot x = x$

$\Rightarrow g'^{-1}g \in G_x$

$\Rightarrow gG_x = g'G_x$

部分群 H に対して

$gH = g'H \Leftrightarrow g'^{-1}g \in H$

$\Leftrightarrow g^{-1}g' \in H$

φ が全射であることは明かである. したがって, φ は全単射である. □

定理 4.3.6　群 G が有限集合 X に作用しているとする．G による軌道を $C_1, C_2, \dots, C_r$ とおき，各軌道から一つずつ代表元 $x_1, x_2, \dots, x_r$ をとる．

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

が成り立つ．

証明：
注意 4.2.2 より，$X = C_1 \sqcup C_2 \sqcup \dots \sqcup C_r$

よって，$|X| = \sum_{i=1}^{r} |C_i|$ となる．補題 4.3.5 より 全単射 $G/G_{x_i} \longrightarrow C_i$ が存在するので，$|C_i| = [G : G_{x_i}]$ である．　□

§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. $x \in X$ とする. 任意の $g \in G$ に対して

$$g \cdot x = x$$

が成り立つとき, x を **固定点** という. X の固定点全体の集合を X^G で表す.

注意: x が固定点 $\iff$ $Gx = \{x\}$

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. 定理 4.3.6 より

$$|X| = \sum_{i=1}^{s} [G : G_{x_i}] \quad \text{である.}$$

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，$|X| \equiv \sum_{x_i \text{ 固定点}} 1 = |X^G| \pmod{p}$ □

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．$g \in G$ に対して，

$$\begin{aligned} g \text{ が固定点である} &\iff \forall h \in G,\ ghg^{-1} = h \\ &\iff \forall h \in G,\ gh = hg \\ &\iff g \in Z(G) \end{aligned}$$

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 は巡回群である．

$x \in G \setminus \{e\}$ 位数 $\mathrm{ord}(x)$ について，$\mathrm{ord}(x) \mid p$ かつ $\mathrm{ord}(x) \neq 1$ である．

よって $\mathrm{ord}(x) = p$，すなわち $\langle x \rangle = G$.

(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：$Z(G)=G$ を示せば良い．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．$Z(G)\neq G$ を仮定する．また，$x\notin Z(G)$ を満たす元 x とその中心化群 $Cent_G(x)$ を考える．明かに，

$$\langle x\rangle \subset Cent_G(x)$$
$$Z(G) \subset Cent_G(x) \quad \text{である．}$$

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． □

第5章 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 を有限群とする．G の位数が素数 p の倍数であるとき，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

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

$\mathbb{Z}/p\mathbb{Z}$ の X への作用を次のように定める．巡回置換 $(12\cdots p)$ をσとおき，

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

$$\bar{k}\cdot(x_1,\dots,x_p) = (x_{\sigma^k(1)}, x_{\sigma^k(2)}, \dots, x_{\sigma^k(p)}) \qquad \text{と定義する．}$$

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

この作用に関して，

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

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

$$\begin{aligned} G^{p-1} &\longrightarrow X \\ (x_1,\dots,x_{p-1}) &\longmapsto (x_1,\dots,x_{p-1},(x_1\cdots x_{p-1})^{-1}) \end{aligned}$$

は全単射である．ゆえに，$|X| = |G|^{p-1} \equiv 0 \pmod p$．
したがって，$(e,\dots,e)$ とは異なる固定点 $(g,\dots,g)$ が存在する．

とくに $g^p = e$ かつ $g \neq e$ であるので，g の位数は p である　□

§5.2. 正規化群

G を群とする．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 $g \in G$，部分群 $H \subset G$ に対して，

$$g\cdot H = gHg^{-1}$$

とおくことによって，GがGの部分群全体の集合への作用している．部分群 H の安定化部分群 Iは

$$N_G(H) = \{ g \in G \mid gHg^{-1} = H \}$$

であり，Hの正規化群という．

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 5.2.1　Gを群とし，H, KをGの部分群とする．

$HK = \{ hk \mid h \in H, k \in K \}$　と定義する．

$K \subset N_G(H)$ 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，

$$h_1 = k_1 h'^{-1} k_1^{-1} \in k_1 H k_1^{-1} = H$$

（$k_1 \in N_G(H)$）

である．

したがって，

$$xx'^{-1} = hk_1h'^{-1} = \underbrace{hh_1}_{\in H}\underbrace{k_1}_{\in K} \in HK.$$

よって，HKはGの部分群である．

最後に，$g \in HK$，$g = hk$　$(h \in H, k \in K)$ とする．

$g = k(k^{-1}hk) \in KH$. よって $HK \subset KH$ である.

($k \in K$, $k^{-1}hk \in k^{-1}Hk = H$)

同様に $kh = (khk^{-1})k \in HK$ より $KH \subset HK$ である. したがって $KH = HK$ となる □

命題 5.2.2 H, K を群 G の部分として, $K \subset N_G(H)$ 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 5.2.1. 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, $k \in K$, $x \in H \cap K$ に対して, $kxk^{-1} \in H \cap K$ 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 5.2.1. 参照) より, $x = kh$
($k \in K$, $h \in H$) と書ける. よって, $xH = khH = kH = f(k)$ 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. □

命題 5.2.2　H, K を群 G の部分として，$K \subset N_G(H)$ 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 5.2.1. 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，$k \in K$, $x \in H \cap K$ に対して，$kxk^{-1} \in H \cap K$ 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 5.2.1. 参照）より，$x = kh$
$(k \in K, h \in H)$ と書ける．よって，$xH = khH = kH = f(k)$ 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. G を有限群とし，その位数を n とおく．また，p を n の素因数とし，n を割り切る最大の p のべきを p^k とおく．部分群 H に対して，H の位数が p^k ならば，G の **pシロー部分群** という．

例えば，$G = \mathfrak{S}_4$ とすると $|G| = 4! = 24 = 2^3 \times 3$ である．

$H_2 = \langle (1\,2\,3\,4), (1\,3) \rangle$

$H_3 = \langle (1\,2\,3) \rangle$ と定義する．

$|H_2| = 8$，$H_3 = |3|$ が成り立つ（これは後で証明される）

よって，H_2 は $\mathfrak{S}_4$ の 2シロー部分群で，H_3 は $\mathfrak{S}_4$ の 3シロー部分群である．

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

証明：G の位数に関する帰納法によって証明する．

- Case 1：指数 $[G:H]$ が p で割り切れない部分群 $H \subsetneq G$ が存在するとき．

$|H| < |G|$ だから，帰納法の仮定より，H は p シロー部分群 K をもつ．

$|G| = |H| \times [G:H]$ である．
（$[G:H]$ は p と素である．）

よって，K は G の p シロー部分群である．

- Case 2：指数 $[G:H]$ が p で割り切れない部分群 $H \subsetneq G$ が存在しないとき．

このとき，任意の部分群 $H \subsetneq G$ に対して，$[G:H]$ が p で割り切れる　(*)

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と

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

が成り立つ．　($G_x = Cent_G(x)$ x の中心化群)

G の固定点全体の集合は，G の中心 $Z(G)$ である．よって，

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} [G : G_{x_i}]$$

この部分は p の倍数である．なぜならば，
$x_i \notin Z(G)$ だから $G_{x_i} \neq G$ である．
ゆえに (*) より $[G:G_{x_i}] \equiv 0 \pmod{p}$

したがって, $|Z(G)| \equiv |G| \equiv 0 \mod p$. とくに, $Z(G) \neq \{e\}$ である.

また, $|Z(G)|$ が p の倍数だから, コーシーの定理より
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. また,

$$G' = G/H \quad \text{とおき,}$$

自然な準同型 $\pi : G \to G'$ を考える. $|G'| < |G|$ だから,
帰納法の仮定より, G' は p シロー部分群 $K' \subset G'$ をもつ.

$$K = \pi^{-1}(K')$$

とおくと, K は G の p シロー部分群になることを示す. また, $H \subset K$ である.
π は準同型

$$\begin{aligned} \pi' : K &\longrightarrow K' \\ k &\longmapsto \pi(k) \end{aligned}$$

を誘導する. π が全射だから, π' も全射である. また,

$$\mathrm{Ker}(\pi') = K \cap \mathrm{Ker}(\pi) = K \cap H \overset{(*)}{=} H$$

$(*)$ $\because$ $H \subset K$ である

群同型定理より $K/H \simeq K'$ が得られる. ゆえに,

$$|K| = |H| \cdot |K'| = p \cdot |K'| \quad \text{である.}$$

同様に $\quad |G| = |H| \cdot |G'| = p\,|G'| \quad$ が成り立つ.

$|G| = p^m \cdot d$ $(\gcd(p,d)=1)$ ならば, $|G'| = p^{m-1} \cdot d$ である.

よって, $|K| = p \cdot |K'| = p \cdot p^{m-1} = p^m$ であり, K は G の

p シロー部分群である □

G の部分群 H に対して, H の位数が p のべキであるとき,
p 部分群という.

定理 5.3.3. (シロー) 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.

$$X = \{ xSx^{-1} \mid x \in G \} \quad \text{とおく.}$$

G は共役によって X に作用している.
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.

H は p 群なので，命題 4.4.2 より，

$$|X| \equiv |X^H| \mod p \quad \text{である.}$$

次に $|X|$ を求める．X は共役作用に関する S の軌道である．
この作用に関して，S の安定化部分群は

$$N_G(S) = \{ g \in G \mid gSg^{-1} = S \} \quad \text{である.}$$

補題 4.3.5 より 全単射 $G/N_G(S) \longrightarrow X$ が存在する．

よって，$|X| = [G : N_G(S)]$ である．

$S \subset N_G(S) \subset G$ より，$[G:S] = [G:N_G(S)] \cdot [N_G(S):S]$

（$[G:S]$ はこれは p と素である．（∵ S が p シロー））

よって，$[G:N_G(S)]$ も p と素である．ゆえに，$|X| = [G:N_G(S)]$ は p の倍数でない．$|X| \equiv |X^H| \mod p$ より，$X^H \neq \emptyset$ 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

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

$$|HS'| = \frac{|H| \cdot |S'|}{|H \cap S'|}$$

であり，ゆえに HS' は p 部分群である．（$\because$ H, S' 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．
（$\because$ $x \mapsto gxg^{-1}$ は G の自己同型である）

(iii) S を p シロー部分群とし，$X = \{gSg^{-1} \mid g \in G\}$ を考える．また，S の X への共役作用を考える．(i) の証明より，
$|X| \equiv |X^S| \pmod{p}$．また，$S' \in X^S$ とすると，$S \subset N_G(S')$ が成り立つ．また，⊗ より $S \subset S'$ となる

$|S| = |S'|$ より，$S = S'$ である．このことから，$X^S = \{S\}$ が成り立つ．したがって，

$$|X| \equiv |X^S| = 1 \pmod{p}$$ である　□

定理5.3.3. (シロー)　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．

$$X = \{ xSx^{-1} \mid x \in G \} \quad \text{とおく．}$$

Gは共役によってXに作用している．

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．

Hはp群なので，命題4.4.2より，

$$|X| \equiv |X^H| \mod p \quad \text{である．}$$

次に$|X|$を求める．Xは共役作用に関するSの軌道である．

この作用に関して，Sの安定化部分群は

$$N_G(S) = \{ g \in G \mid gSg^{-1} = S \} \quad \text{である．}$$

補題4.3.5より全単射 $G/N_G(S) \longrightarrow X$ が存在する．

よって，$|X| = [G : N_G(S)]$ である．

$S \subset N_G(S) \subset G$ より，$[G : S] = [G : N_G(S)] \cdot [N_G(S) : S]$

（$[G : S]$ はこれは p と素である．（∵ S が p シロー））

よって，$[G : N_G(S)]$ も p と素である．ゆえに，$|X| = [G : N_G(S)]$ は p の倍数でない．$|X| \equiv |X^H| \mod p$ より，$X^H \neq \emptyset$ 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

$$HS'/S' \simeq H/H \cap S'$$

が存在する．よって，

$$|HS'| = \frac{|H| \cdot |S'|}{|H \cap S'|}$$

であり，ゆえに HS' は p 部分群である．（∵ H, S' 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．以下が成り立つことを証明した．

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，

A $H \subset gSg^{-1}$ を満たす $g \in G$ が存在する．

B $H \subset N_G(S)$ ならば $H \subset S$ である．

(ii) K, K' を p シロー部分群とする．**A** 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．

($\because$ $x \mapsto gxg^{-1}$ は G の自己同型である)

(iii) S を p シロー部分群とし，$X = \{gSg^{-1} \mid g \in G\}$ を考える．また，S の X への共役作用を考える．(i) の証明より，$|X| \equiv |X^S| \pmod{p}$．また，$S' \in X^S$ とすると，$S \subset N_G(S')$ が成り立つ．また，**B** より $S \subset S'$ となる

$|S| = |S'|$ より，$S = S'$ である．このことから，$X^S = \{S\}$ が成り立つ．したがって，

$$|X| \equiv |X^S| = 1 \pmod{p}$$ である　□

注意 5.3.4

(1) H を G の p シロー部分群とする．$H \triangleleft G$ ならば，H は G の唯一の p シロー部分群である．とくに，有限アーベル群は ただ一つの p シロー部分群 をもつ．

(2) 有限群 G の p シロー部分群の数 は $|G|$ の約数である．
なぜならば，S を p シロー部分群とすると，定理 5.3.3(ii) より G の p シロー 部分群全 体の集合は

$$\{ gSg^{-1} \mid g \in G \} \quad \text{である．}$$

よって，全単射 $G/N_G(S) \xrightarrow{\sim} \{ p \text{ シロー部分群} \}$ が存在し，p シロー部分群の数は $[G : N_G(S)]$ である．

例 5.3.5　G を位数が 15 の群とする．

$15 = 3 \times 5$ である．

n_3, n_5 をそれぞれ 3 シロー部分群，5 シロー部分群の数とする．

$$\begin{cases} n_3 \equiv 1 \mod 3 \quad \text{かつ} \quad n_3 \mid 15 \\ n_5 \equiv 1 \mod 5 \quad \text{かつ} \quad n_5 \mid 15 \end{cases}$$

よって $n_3 = n_5 = 1$ である．H_3, H_5 を G の 3 シロー部分群，5 シロー部分群とする．

$H_3 \triangleleft G$ ，$H_5 \triangleleft G$ が成り立つ．

$x \in H_3$, $y \in H_5$ とすると,

$$xyx^{-1}y^{-1} = \underbrace{(xyx^{-1})}_{\in H_5}\underbrace{y^{-1}}_{\in H_5} = \underbrace{x}_{\in H_3}\underbrace{(yx^{-1}y^{-1})}_{\in H_3}$$

よって, $xyx^{-1}y^{-1} \in H_3 \cap H_5 = \{e\}$.

したがって $xy = yx$ である. このことから,

$$\varphi : H_3 \times H_5 \longrightarrow G$$
$$(x, y) \longmapsto xy$$

は群準同型であることが分かる.

$$\mathrm{Ker}(\varphi) = \{ (x, x^{-1}) \mid x \in H_3 \cap H_5 \}$$
$$= \{ (e, e) \}$$

より, φ は単射である. $|H_3 \times H_5| = 15 = |G|$ より,

φ は群同型である.

以上より, $G \simeq H_3 \times H_5$

$$\simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$$

となり, G は巡回群である.

第6章　半直積

§6.1 定義

N, H を群とし，準同型

$$\varphi : H \longrightarrow Aut(N)$$

が与えられているとする．このとき，NとHの半直積 $N \rtimes_\varphi H$ を次のように定義する．

- 集合としては，$N \rtimes_\varphi H = N \times H$ である．
- 2つの元 (n_1, h_1), $(n_2, h_2) \in N \times H$ に対して

$$(n_1, h_1) * (n_2, h_2) = (n_1 \cdot \varphi(h_1)(n_2),\ h_1 h_2)$$

とおき，演算 $*$ を定める．

定理 6.1.1

(i) $G = N \times_\varphi H$ は $*$ に関して群をなす.

(ii) $N' = N \times \{e\}$ と $H' = \{e\} \times H$ は G の部分群であり, それぞれ N と H と同型である.

(iii) さらに $N' \triangleleft G$, $G/N' \simeq H$, $G = N'H'$, $N' \cap H' = \{(e,e)\}$ である.

証明:

(i) 結合性: $n_1, n_2, n_3 \in N$, $h_1, h_2, h_3 \in H$ とする

$$
\begin{aligned}
((n_1,h_1)*(n_2,h_2))*(n_3,h_3) &= (n_1\varphi(h_1)(n_2), h_1h_2)*(n_3,h_3) \\
&= (n_1\cdot\varphi(h_1)(n_2)\cdot\varphi(h_1h_2)(n_3),\ h_1h_2h_3) \\
&= (n_1\cdot\varphi(h_1)(n_2)\cdot\varphi(h_1)(\varphi(h_2)(n_3)),\ h_1h_2h_3) \\
&= (n_1\varphi(h_1)(n_2\varphi(h_2)(n_3)),\ h_1h_2h_3) \\
&= (n_1,h_1)*(n_2\varphi(h_2)(n_3),\ h_2h_3) \\
&= (n_1,h_1)*((n_2,h_2)*(n_3,h_3))
\end{aligned}
$$

単位元：

$$(e,e)*(n,h)=(e\varphi(e)(n),\ eh)=(n,h)$$

$$(n,h)*(e,e)=(n\varphi(h)(e),\ he)=(n,h)$$

より，(e,e) は G の単位元である．

逆元：$(n,h)\in G$ に対して

$$(n,h)*\left(\varphi(h^{-1})(n^{-1}),\ h^{-1}\right)=\left(n\varphi(h)\left(\varphi(h^{-1})(n^{-1})\right),\ hh^{-1}\right)$$

$$=(n\varphi(e)(n^{-1}),\ e)$$

$$=(nn^{-1},\ e)=(e,e)$$

$$\left(\varphi(h^{-1})(n^{-1}),h^{-1}\right)*(n,h)=\left(\varphi(h^{-1})(n^{-1})\varphi(h^{-1})(n),\ h^{-1}h\right)$$

$$=(\varphi(h^{-1})(n^{-1}n),\ e)$$

$$=(\varphi(h^{-1})(e),\ e)=(e,e)$$

よって，(n,h) は可逆元であり，その逆元は

$\left(\varphi(h^{-1})(n^{-1}),h^{-1}\right)$ である．

(ii) 写像 $N \xrightarrow{u} G$, $n \mapsto (n, e)$ と $H \xrightarrow{v} G$, $h \mapsto (e, h)$

は準同型である.

$$\left(\because \ (n_1, e) * (n_2, e) = (n_1 \varphi(e)(n_2), e) = (n_1 n_2, e) \right.$$
$$\left. (e, h_1) * (e, h_2) = (e \varphi(h_1)(e), h_1 h_2) = (e, h_1 h_2) \right)$$

よって, N' と H' は G の部分群である. また, u, v がそれぞれ同型写像 $N \xrightarrow{\sim} N'$, $H \xrightarrow{\sim} H'$ を誘導する.

(iii) 写像 $G \xrightarrow{w} H$, $(n, h) \mapsto h$ は準同型である.

$\mathrm{Ker}(w) = N'$ より, $N \lhd G$ であり, $G/N' \simeq H$ である.

$(n, e) * (e, h) = (n \varphi(e)(e), e h) = (n, h)$ より $G = N'H'$ である. 明らかに $N' \cap H' = \{(e, e)\}$ である.

□

命題 6.1.2　以下の条件が互いに同値である.

(1) φ が自明な準同型である（すなわち，任意の $h \in H$ に対して $\varphi(h) = id_N$）

(2) $H' \triangleleft G$ である.

(3) $G = N \times H$（つまり $*$ が通常の直積の演算である.

証明：(1) $\Rightarrow$ (3) $\Rightarrow$ (2) は明らかである.

(2) を仮定する. $n \in N, h \in H$ に対して

$$(n^{-1}, e) * (e, h) * (n^{-1}, e)^{-1} = (n^{-1}, h) * (n, e)$$

$$= (n^{-1}\varphi(h)(n), h) \quad \text{である.}$$

$H' \triangleleft G$ より $(n^{-1}\varphi(h)(n), h) \in H'$ であり，ゆえに $n^{-1}\varphi(h)(n) = e$ となる. よって $\varphi(h)(n) = n$ すなわち $\varphi(h) = id_N$ が成り立つ.

□

§6.2 内部半直積

今，群 G とその部分群 N, H が与えられている
とする．また，N と H が以下の条件をみたすとする．

$$N \triangleleft G$$

$$G = NH$$

$$N \cap H = \{e\}$$

$h \in H, n \in N$ に対して

$$\varphi(h) = hnh^{-1}$$

とおくことで準同型 $\varphi : H \longrightarrow Aut(N)$ を定める．

定理 6.2.1

$$f : N \rtimes_\varphi H \longrightarrow G$$
$$(n, h) \longmapsto nh$$

は群同型である．

このとき，単に $G = N \rtimes H$ と表す

証明　f が準同型であることを示す.

$$
\begin{aligned}
&f((n_1, h_1) * (n_2, h_2)) \\
&\quad = f(n_1 \varphi(h_1)(n_2), h_1 h_2) \\
&\quad = f(n_1 h_1 n_2 h_1^{-1}, h_1 h_2) \\
&\quad = n_1 h_1 n_2 h_1^{-1} h_1 h_2 \\
&\quad = n_1 h_1 n_2 h_2 \quad = f((n_1, h_1)) f((n_2, h_2))
\end{aligned}
$$

仮定より f が全射である. また,

$$
\begin{aligned}
\mathrm{Ker}(f) &= \{(n, n^{-1}) \mid n \in H \cap H\} \\
&= \{(e, e)\} \quad \text{となる.}
\end{aligned}
$$

以上より f は群同型である. □

例 6.2.2

$G = \mathfrak{S}_3$ とし, $N = \langle (1\,2\,3) \rangle$, $H = \langle (1\,2) \rangle$
とすると $G = NH$, $H \cap N = \{id\}$, $N \lhd G$ である.

ゆえに $\mathfrak{S}_3 = N \rtimes H$ である.

逆に G を位数 6 の群とする. $6 = 2 \times 3$
n_2, n_3 : それぞれ 2 シロー部分群, 3 シロー部分群の数.

$$\begin{cases} n_2 \equiv 1 \mod 2 & \text{かつ } n_2 \mid 6 \\ n_3 \equiv 1 \mod 3 & \text{かつ } n_3 \mid 6 \end{cases}$$

よって $n_3 = 1$, $n_2 \in \{1, 3\}$ である. H_2, H_3 をそれぞれ
2 シロー部分群, 3 シロー部分群とする. 明らかに

$H_3 \lhd G$, $H_2 \cap H_3 = \{e\}$, $H_3 H_2 = G$ である. よって

$$G = H_3 \rtimes H_2$$

$H_2 \simeq \mathbb{Z}/2\mathbb{Z}$, $H_3 \simeq \mathbb{Z}/3\mathbb{Z}$ である. また,

$$Aut(\mathbb{Z}/3\mathbb{Z}) = \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$$

よって準同型 $\mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi} Aut(\mathbb{Z}/3\mathbb{Z})$ はちょうど 2 つ存在する.

- Y が自明ならば, $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$
- Y が非自明ならば $G \simeq G_3$ である.

ゆえに, 同型を除いて位数6の群がちょうど2つ存在する.

第7 自由群

これからアーベル群のみを考える. 演算を $+$ で表し, 単位元を 0 で表す.

§7.1. アーベル群の直和

$(A_i)_{i\in I}$ をアーベル群の族とする. $\prod_{i\in I} A_i$ を $(A_i)_{i\in I}$ の直積という. また,

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

は $\prod_{i\in I} A_i$ の部分群であり, $(A_i)_{i\in I}$ の直和という. とくに, I が有限ならば $\bigoplus_{i\in I} A_i = \prod_{i\in I} A_i$ が成り立つ.

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,

$$\prod_{i\in I} A_i = A^I \text{ と表し, } \bigoplus_{i\in I} A_i = A^{(I)} \text{ と表す.}$$

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

$$a = b + c \quad (b \in B,\ c \in C)$$

と表せるときに，$A = B \oplus C$ と書く．明かに，

$$A = B \oplus C \iff A = B + C \text{ かつ } B \cap C = 0.$$

定義 7.1.1 A をアーベル群とし，$\{x_i\}_{i \in I}$ を A の元の族とする．$\{x_i\}_{i \in I}$ が A の**基底**であるとは，任意の $x \in A$ が一意に

$$x = \sum_{i \in I} k_i x_i \qquad (k_i \in \mathbb{Z} \text{ であり，有限個を除いて } k_i = 0)$$

と表せることをいう．

A が基底をもつとき，A が**自由アーベル群**であるという．また，有限個の元からなる基底 $\{x_1, x_2, \dots, x_n\}$ が存在するとき，**有限生成自由アーベル群**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

$$\begin{aligned} \varphi : \mathbb{Z}^{(I)} &\longrightarrow A \\ (a_i)_{i \in I} &\longmapsto \sum_{i \in I} a_i x_i \end{aligned}$$

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，

$$e_j = (\delta_{ij})_{i \in I} \qquad \left(\text{ただし} \quad \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \right)$$

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

とくに $\mathbb{Z}^n$ $(n \geq 1)$ は有限生成自由アーベル群である．

補題 7.1.2 A を自由アーベル群とし，$\{x_i\}_{i \in I}$ を A の基底とする．また，B をアーベル群とし，$\{y_i\}_{i \in I}$ を B の元の族とする．このとき，$f(x_i) = y_i$ をみたす準同型

$$f : A \longrightarrow B$$

はただ一つ存在する．

証明：A の任意の元 x を一意的に $x = \sum_{i \in I} k_i x_i$ と表せる（但し，有限個を除いて $k_i = 0$）．f を $f(x) = \sum_{i \in I} k_i y_i$ によって定義できる．また，f の一意性は明らかである． □

命題 7.1.3　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 $f : \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ が存在すると仮定する．

$$2\mathbb{Z}^n = \{2x \mid x \in \mathbb{Z}^n\} \quad \text{を考える．}$$

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

$$\mathbb{Z}^n/2\mathbb{Z}^n \longrightarrow \mathbb{Z}^m/2\mathbb{Z}^m \qquad (*)$$

を誘導する．準同型

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{\pi} & (\mathbb{Z}/2\mathbb{Z})^n \\ (k_1, \cdots, k_n) & \longmapsto & (\bar{k}_1, \cdots, \bar{k}_n) \end{array}$$

は全射であり，その核は $2\mathbb{Z}^n$ であるので $\mathbb{Z}^n/2\mathbb{Z}^n \simeq (\mathbb{Z}/2\mathbb{Z})^n$ である．よって，$(*)$ の群の位数を比べれば，$2^n = 2^m$ となり，すなわち $n = m$．　□

系 7.1.4　A を有限生成自由アーベル群とし，$\{x_1, \cdots, x_n\}$ と $\{y_1, \cdots, y_m\}$ を A の基底とする．このとき，$n = m$ が成り立つ．

証明

$$\mathbb{Z}^n \xrightarrow{\sim} A \qquad \text{と} \qquad \mathbb{Z}^m \xrightarrow{\sim} A$$
$$(k_1,\dots,k_n) \longmapsto \sum_{i=1}^{n} k_i x_i \qquad (k_1,\dots,k_m) \longmapsto \sum_{i=1}^{m} k_i y_i$$

は同型写像である. 命題 7.1.3 より $n = m$ である. □

定義 7.1.5 Aの基底の元の個数を **Aの階数** といい, **$\mathrm{rank}(A)$** で表す.

例えば, $\mathbb{Z}^n$ の階数は n である.

§7.2 自由群の部分群.

補題 7.2.1 A をアーベル群とし, A' を自由アーベル群とする. また, $f : A \longrightarrow A'$ を全準同型とする. 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, $B \simeq A'$ である.

証明：$\{x_i'\}_{i\in I}$ を A' の基底とする．f が全射なので，$f(x_i)=x_i'$ をみたす $\{x_i\}_{i\in I}$ がとれる．補題 7.1.2 より，$g(x_i')=x_i$ をみたす準同型 $g: A' \longrightarrow A$ はただ一つ存在する．とくに，

$$(f\circ g)(x_i') = f(g(x_i')) = f(x_i) = x_i'$$

よって，$f\circ g = id_{A'}$ である．

$$B = \mathrm{Im}(g) = \{g(y) \mid y\in A'\}$$

と定義し，$A = B\oplus \mathrm{Ker}(f)$ を示す．

- $B\cap \mathrm{Ker}(f) = 0$ を示す．

  $x\in B\cap \mathrm{Ker}(f)$ とする．$x\in \mathrm{Im}(g)$ より $x=g(y)$ $(y\in A')$ と書ける．よって

  $$0 = f(x) = f(g(y)) = y$$ となり，ゆえに $x=0$ となる．

- $B+\mathrm{Ker}(f) = A$ を示す．

  $x\in A$ 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，
$c \in \mathrm{Ker}(f)$ である．また，$b \in B$ である．

したがって，$A = B + \mathrm{Ker}(f)$ が成り立つ．

以上より，$A = B \oplus \mathrm{Ker}(f)$ である．

最後に，$B \simeq A'$ を示す．f を B に制限すると，

準同型 $f' : B \longrightarrow A'$ が得られる．$A = B \oplus \mathrm{Ker}(f)$

より，f' は全単射である．　□

定理 7.2.2 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も有限生成自由アーベル群であり，さらに

$$\mathrm{rank}(B) \leq \mathrm{rank}(A)$$

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．

自然な射影 $f : A \longrightarrow \mathbb{Z}x_1$ を考える．

$$\sum_{i=1}^{n} k_i x_i \longmapsto k_1 x_1$$

$B_1 = \mathrm{Ker}(f) \cap B$ とおくと，$B_1 \subset \mathbb{Z}x_2 \oplus \dots \oplus \mathbb{Z}x_n$ である．
帰納法の仮定より B_1 は自由アーベル群であり，$\mathrm{rank}(B_1) \leq n-1$ である．

$B' = f(B)$とおくと，fは全準同型

$$B \xrightarrow{f'} B'$$

を誘導する．また，$\mathrm{Ker}(f') = B_1$である．補題 7.2.1 より

$$B = B_1 \oplus C \quad \text{かつ} \quad C \simeq B'$$

が成り立つ．$B' \subset \mathbb{Z}x_1$ より B'と C は自由アーベル群であり，$\mathrm{rank}(C) \leq 1$である．

したがって B も自由アーベル群であり,

$$\begin{aligned} \operatorname{rank}(B) &= \operatorname{rank}(B_1) + \operatorname{rank}(C) \\ &\leq n-1 \quad + 1 \quad = n. \end{aligned}$$

□

§7.3 ねじれ

定義 7.3.1. 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を A の**ねじれ部分群**といい, A_{tor} と書く.

A_{tor} が部分群であることを check

- 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,

$$nm(x-y) = nmx - nmy = 0 - 0 = 0 \text{ となる.}$$

よって, A_{tor} は A の部分群である.

$A_{tor} = \{0\}$ のとき, A を**ねじれのないアーベル群**という.

例 7.3.2 : $A = \mathbb{Z}^{(I)}$ ならば $A_{tor} = \{0\}$.

よって, 自由アーベル群はねじれのない群である.

定義 7.3.3 アーベル群 A に対して, $A = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$ となる $x_1, \ldots, x_n \in A$ が存在するとき, **有限生成アーベル群** という.

定理 7.3.4 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 は有限生成自由アーベル群である. つまり, $A \simeq \mathbb{Z}^n$ $(n \geq 1)$ である.

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

$$\lceil a_1x_1 + \cdots + a_nx_n = 0 \quad (a_1, \ldots, a_n \in \mathbb{Z}) \quad \text{ならば}, \quad a_1 = a_2 = \cdots = a_n = 0 \text{ である} \rfloor \qquad (*)$$

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

$\{x_1, \ldots, x_n\}$ 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, $x_1, \ldots, x_n$ は $(*)$ を満たすが, 任意の $y \in S \setminus \{x_1, \ldots, x_n\}$ に対して, $\{x_1, \ldots, x_n, y\}$ は $(*)$ を満たさない.

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

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

$y \in S \setminus \{x_1, \ldots, x_n\}$ とする. このとき, $my + a_1x_1 + \cdots + a_nx_n = 0$ となる $m, a_1, \ldots, a_n \in \mathbb{Z}$ $(m \neq 0)$ が存在する.

とくに, $my \in B$ となる. よって, $S = \{y_1, y_2, \ldots, y_N\}$ 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 $1 \leqslant i \leqslant N$ 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 6.1.3 参照）．主張が従う．

□

第8章　有限アーベル群

§8.1　アーベル p群

注意：

Ⅰ　A を有限アーベル群とし，$A_1 \subset A$ を部分群とする．$y \in A$ とし，$\overline{y} = y + A_1 \in A/A_1$ とする．このとき，任意の $x \in \overline{y}$ に対して

$$ord(\overline{y}) \mid ord(x)$$ が成り立つ．

（なぜならば，$nx = 0 \Rightarrow n\overline{y} = \overline{0} \Rightarrow ord(\overline{y}) \mid n$ である）．

Ⅱ　$x \in A$ とし，$ord(x) = n$ とおく．レポート1問4より，整数 $k \neq 0$ に対して

$$ord(kx) = \frac{n}{gcd(n,k)}$$ である．

補題 8.1.1. 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. $y \in A$ とし, $\bar{y} = y + A_1$ とする. このとき,

$$ord(\bar{y}) = ord(x)$$

を満たす $x \in \bar{y}$ 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^r $(r \geq 1)$ である.

$p^r \bar{y} = \bar{0}$ より $p^r y \in A_1$ である. よって $p^r y = n a_1$ と書ける. さらに, $0 \leq n < p^{r_1}$ を仮定して良い.

$$n = p^k n' \quad \text{かつ} \quad gcd(p, n') = 1$$

と書くことができる. Ⅰ より, $n a_1 = p^k n' a_1$ の位数は

$$ord(n a_1) = \frac{p^{r_1}}{gcd(n, p^{r_1})} = \frac{p^{r_1}}{p^k} = p^{r_1 - k}$$ である.

一方, $p^r y = n a_1$ より $ord(n a_1) = \dfrac{ord(y)}{gcd(p^r, ord(y))}$ である.

Ⅱ より $p^r = ord(\bar{y}) \mid ord(y)$ が成り立つ. よって

$ord(n a_1) = p^{r_1 - k} = \dfrac{ord(y)}{p^r}$ となり, すなわち

$$ord(y) = p^{r+r_1-k}$$

a_1 が最大位数の元だから, $r+r_1-k \leq r_1$ であり, ゆえに

$$\boxed{r \leq k}$$ である.

したがって,

$$p^r y = n a_1 = p^k n' a_1 = p^r \left(p^{k-r} n' a_1\right)$$ である

$x = y - p^{k-r} n' a_1$ と定める. 明らかに $x \in \overline{y}$

であり, $p^r x = 0$ である. (I) より

$ord(\overline{y}) = p^r \mid ord(x)$ であるので,

$$ord(x) = p^r = ord(\overline{y}) \qquad \square$$

定理8.1.2. 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.

証明

- **存在性**: A の位数に関する数学的帰納法 によって証明する.

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,

$$A/A_1 = \bar{A}_2 \oplus \bar{A}_3 \oplus \cdots \oplus \bar{A}_m \quad \text{かつ} \quad \begin{array}{l}\bar{A}_i \text{ の位数を } p^{r_i} \text{ とおくと} \\ p^{r_2} \geq p^{r_3} \geq \cdots \geq p^{r_m}\end{array} \quad (*)$$

を満たす 巡回部分群 $\bar{A}_2, \bar{A}_3, \ldots, \bar{A}_m \subset A/A_1$ が存在する.

$\bar{a}_i \in \bar{A}_i$ を $\bar{A}_i$ の生成元とする $(i = 2, \ldots, m)$. 補題 8.1.1 より,

$$a_i \in \bar{a}_i \quad \text{かつ} \quad \mathrm{ord}(\bar{a}_i) = \mathrm{ord}(a_i)$$

$A_i = \langle a_i \rangle$ $(2 \leq i \leq m)$ と定義し,

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_m$$

が成り立つことを示す. $x \in A$ に対して, $\bar{x} = x + A_1$ とおくと

$(*)$ より $\bar{x} = d_2 \bar{a}_2 + \cdots + d_m \bar{a}_m$ $(d_2, \ldots, d_m \in \mathbb{Z})$ と書ける.

よって, $x-(d_2a_2+\cdots+d_ma_m)\in A_1$ であり, ゆえに $x-(d_2a_2+\cdots+d_ma_m)=d_1a_1$ となる $d_1\in\mathbb{Z}$ が存在する. よって

$$x=d_1a_1+d_2a_2+\cdots+d_ma_m$$

したがって, $A=A_1+A_2+\cdots+A_m$ である.

また, (*) より A/A_1 の位数は $p^{r_1}\times\cdots\times p^{r_m}$ である. よって,

$$\begin{aligned}|A| &= |A_1|\times[A:A_1]\\ &= p^{r_2}\times p^{r_1}\times\cdots\times p^{r_m}=p^{r_1+\cdots+r_m}\end{aligned}$$

準同型 $\varphi:\ A_1\oplus\cdots\oplus A_m\longrightarrow A,\quad (x_1,\cdots,x_m)\longmapsto x_1+\cdots+x_m$ は

濃度が等しい集合の間の全射であるので, 全単射になる.

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

- **一意性**: 帰納法によって証明する. 以下のように, A が2つの表し方をもつと仮定する.

$$A=A_1\oplus\cdots\oplus A_m=A_1'\oplus\cdots\oplus A_{m'}'$$

但し, A_i の位数は p^{r_i}, A_i' の位数は $p^{r_i'}$ であり

$r_1\geq r_2\geq\cdots\geq r_m$ かつ $r_1'\geq r_2'\geq\cdots\geq r_{m'}'$ である.

よって, $pA=pA_1\oplus\cdots\oplus pA_m=pA_1'\oplus\cdots\oplus pA_{m'}'$ である. $A_i\simeq\mathbb{Z}/p^{r_i}\mathbb{Z}$ より

$pA_i\simeq p\mathbb{Z}/p^{r_i}\mathbb{Z}\simeq\mathbb{Z}/p^{r_i-1}\mathbb{Z}$ である. とくに $pA_i=0\Leftrightarrow r_i=1$.

$\begin{cases} r_i = 1 \text{ をみたす } i \text{ の数を } j \text{ とおく} \\ r_i' = 1 \quad \text{——————} \quad j' \text{ とおく.} \end{cases}$

したがって,

$$pA \simeq \mathbb{Z}/p^{r_1-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_{m-j}-1}\mathbb{Z}$$
$$\simeq \mathbb{Z}/p^{r_1'-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_{m'-j'}'-1}\mathbb{Z} \quad \text{となる.}$$

帰納法の仮定より,

$$\begin{cases} m-j = m'-j' \\ r_i - 1 = r_i' - 1 \quad (i = 1, \ldots, m-j) \end{cases} \qquad (**)$$

一方,

$$|A| = p^{r_1} \times \cdots \times p^{r_{m-j}} \times \underbrace{p \times \cdots \times p}_{j\text{コ}} = p^{r_1'} \times \cdots \times p^{r_{m'-j'}'} \times \underbrace{p \times \cdots \times p}_{j'\text{コ}}$$

$(**)$ より等しい

ゆえに, $j = j'$, $m = m'$ となり, 主張が従う. □

§8.2 有限アーベル群の構造定理

A を有限アーベル群とする．素数 p について

$$A(p) = \{ x \in A \mid x \text{ の位数が } p \text{ のべキ} \}$$

と定義する．$A(p)$ は明らかに A の部分群である．

補題 8.2.1 $A(p)$ は A の(唯一の) p シロー部分群である

証明 A はアーベル群だから，ただ一つの p シロー部分群をもつ．A の p シロー部分群を S とおくと，$S \subset A(p)$ が成り立つ ($\because$ $|S|$ が p のべキ)．逆に，$x \in A(p)$ とすると，$H = \langle x \rangle$ は p 部分群である．定理 5.3.3. (i) より，$H \subset S$ である．よって $A(p) = S$ □

定理 8.2.2. 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：準同型

$$\varphi : A(p_1) \oplus \dots \oplus A(p_r) \longrightarrow A \qquad \text{を考える.}$$
$$(x_1, \dots, x_r) \longmapsto x_1 + \dots + x_r$$

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

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

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

$$D^N x_1 = -(D^N x_1 + \dots + D^N x_r) = 0 \quad \text{となる.}$$

よって x_1 の位数は D^N の約数であり, p_1 のべきである.

D と p_1 が互いに素だから, $x_1 = 0$ となる. 同様に

$$x_2 = \dots = x_r = 0$$

を示すことができる. したがって, φ は単射である.

補題 8.2.1 より $A(p_i)$ は A の p_i-シロー部分群である. とくに

$$|A(p_i)| = p_i^{k_i}$$

が成り立つ. ゆえに, $A(p_1) \oplus \dots \oplus A(p_r)$ の位数は $p_1^{k_1} \cdots p_r^{k_r} = n$ である. よって, φ は全単射である

□

系 8.2.3. 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 8.1.2. と定理 8.2.2. から分かる. □

注意 定理 8.2.3 の $n_1, n_2, \ldots, n_k$ が一意に定まるとは限らない. 例えば $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$ である.