群（主に有限群）

Ver. 0.10

Chap. 1 群

§1 群の定義

群

集合Gが次をみたすときGは群という.

・演算が定義されている

$$G \times G \longrightarrow G$$
$$(x, y) \longmapsto xy$$

・この演算が次をみたす.

結合則

$\forall x, y, z \in G \quad (xy)z = x(yz)$

単位元(eと書く)がある.

$\forall x \in G \quad xe = ex = x$

任意の元にその逆元(xに対しx^{-1}と書く)がある.

$\forall x \in G \quad \exists x^{-1} \in G$

$$xx^{-1} = x^{-1}x = e$$

演算はしばしば積とよばれる.

対称群 S_n

$X = \{1, 2, \dots, n\}$ のいれかえを考える.

たとえば $n = 3$ として

$$\begin{matrix} 1, & 2, & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix}$$

これを $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ と書く.

これらのすべてを集めたものを S_n と書く.

$n = 3$ の場合

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

S_3 には積がある.

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

結合則をみたす.

$$\left(\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right)\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

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

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\left(\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right)$$

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

同じ

単位元がある $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

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

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

逆元がある

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

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

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

S_n は群.

これを対称群(n次対称群)という.

一般に群の演算は可換ではない.

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

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

違う

演算がすべて可換な群を可換群

とかアーベル群という.

$\mathbb{Z}$ は $+$ に関して アーベル群

$x, y \in \mathbb{Z} \rightsquigarrow xy = x+y$

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto x+y \end{aligned}$$

xy

結合則 OK. $(x+y)+z = x+(y+z)$

単位元 0 $x+0 = 0+x = x$

逆元 $x \rightsquigarrow -x$ $x+(-x) = (-x)+x = 0$

アーベル群では 演算の記号に $+$ を使うことが多い

群の位数

群 G の濃度を G の位数といい $\#G$ と書く.

有限群のときは個数

$\# S_3 = 6$

$\# S_n = n!$

§2 部分群

部分群

Gの部分集合Hがeを含みGの演算で群となるときHをGの部分群という.

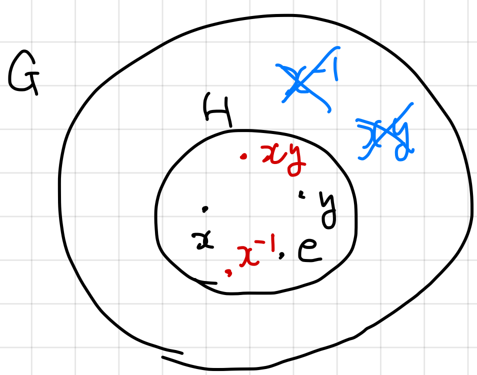
これはHが次をみたすとき．ということもできる.

$$\forall x, y \in H \Rightarrow xy \in H$$

$$\forall x \in H \Rightarrow x^{-1} \in H$$

このとき $e \in H$ は

$x, x^{-1} \in H$　$xx^{-1} \in H$ からいえる.



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

例　$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \subset S_3$

Prop.

$H \subset G$ が G の部分群

$\Leftrightarrow$ 「$x, y \in H \Rightarrow xy^{-1} \in H$」

(証)

$\Rightarrow$ は明らか

$\Leftarrow$

$x \in H$ に対して $xx^{-1} \in H$ だから $e \in H$

${}^\forall y \in H$ に対して $ey^{-1} = y^{-1} \in H$

${}^\forall x, y \in H$ に対して $y^{-1} \in H$ だから

$$xy = x(y^{-1})^{-1} \in H$$

┘

$\{e\}$, G も G の部分群.

$\langle S \rangle$

Sを群Gの部分集合とする.

$$x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \in G$$

$$x_1, \dots, x_n \in S$$

$$\varepsilon_1, \dots, \varepsilon_n = 1, -1$$

そのもの　逆元

となるxたちのすべてを集めるとGの部分群になる.

これを$\langle S \rangle$と書く.

生成元

$G = \langle S \rangle$のとき GはSで生成される, とか.

SはGの生成系などといい

Sの元をGの生成元という.

例

$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$ は S_3 の生成系

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

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

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

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

他の選び方もある. また, ムダがあってもよい.

巡回群

唯一つの元で生成される群。すなわち、

$G = \langle g \rangle$ となる群を巡回群という。

$\langle \{g\} \rangle$　　$g \in G$　　$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$$A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

交代群

A_3 は S_3 の部分群で巡回群

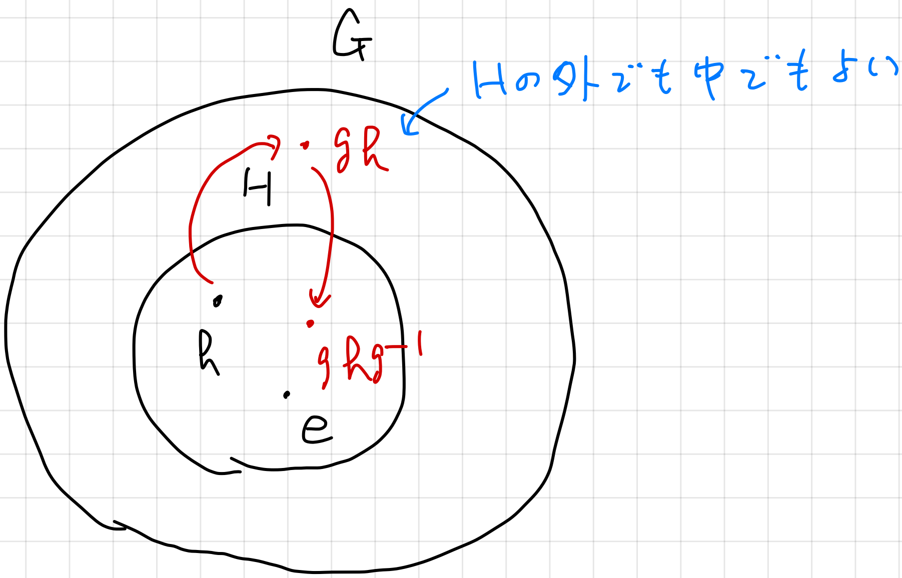
$$A_3 = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\rangle$$

$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \subset S_3$ も巡回群

正規部分群

Gの部分群Hが次をみたすとき正規部分群という

$$\forall g \in G \quad H = gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$



このとき $H \triangleleft G$ と書く.

アーベル群の部分群はすべて正規.

$$gHg^{-1} \rightsquigarrow g + H + (-g) = H$$

一般の場合は正規とは限らない.

注 $gHg^{-1} \subset H \quad \forall g \in G \Rightarrow gHg^{-1} = H$

(任意の g で $gHg^{-1} \subset H$ だから g^{-1} に対しては
$g^{-1}Hg \subset H \quad \therefore \quad H \subset gHg^{-1}$)

元の位数

$x \in G \quad x^n = e$ となるとき

n を x の位数という.

このような n がないとき x の位数は無限という.

例 S_3

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ の位数は 2

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

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ の位数は 3

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

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

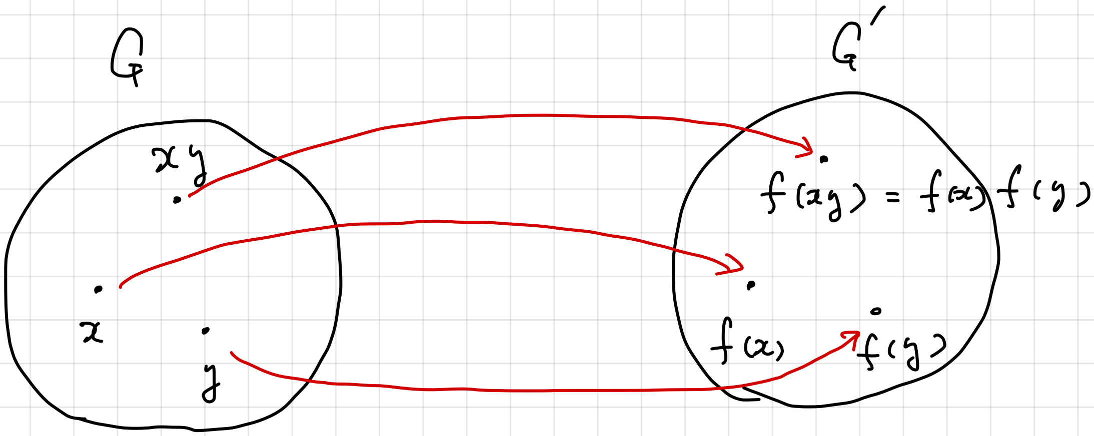
§3 準同型写像

準同型写像

群 G, G' に対し 写像 $f: G \to G'$ が

次をみたすとき f は G から G' への 準同型写像という

$$\forall x, y \in G \quad f(xy) = f(x)f(y)$$



f が 全単射のとき f を 同型写像という.

このとき G と G' は 同型といい $G \simeq G'$ と書く

Prop.

$f(x^{-1}) = f(x)^{-1} \qquad f(e) = e'$ ← G の単位元

(証)

$f(e^2) = f(e)f(e) = f(e)$

$f(e)^{-1}$ をかけると $f(e) = e'$

$f(xx^{-1}) = f(x)f(x^{-1}) = e'$

例

$$f : \mathbb{Z} \longrightarrow S_3$$

$$n \longmapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^n$$

$n=0$のときは$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$と考える.

$$f(n+m) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{n+m}$$

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

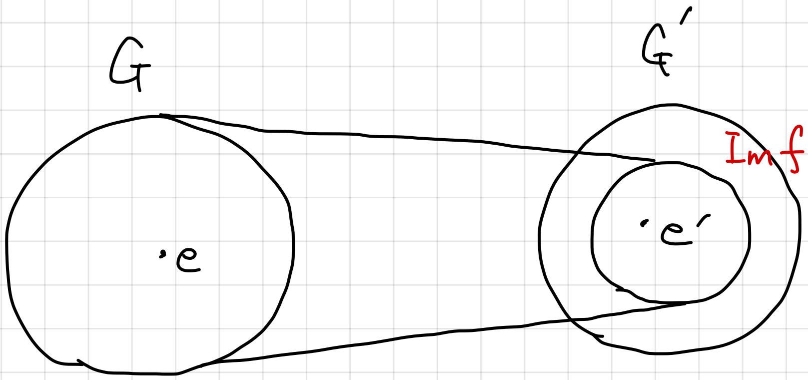
$$= f(n) f(m)$$

Im

$f : G \to G'$ に対し

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

を f の像という



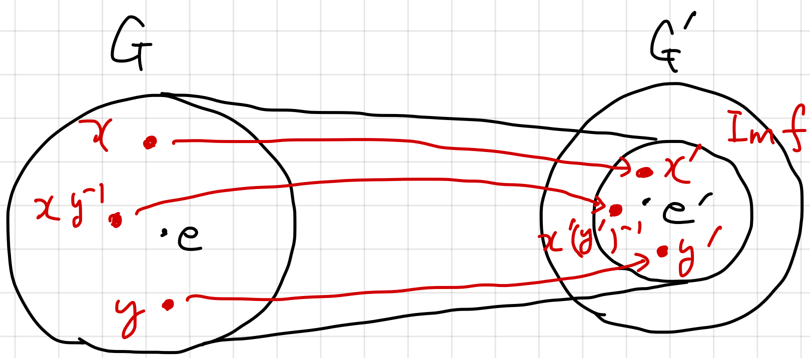
Im G は G' の部分群となる.

(証)

$x', y' \in \mathrm{Im}\, G$ とすると

$\exists x, y \in G \quad f(x) = x', \ f(y) = y'$

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

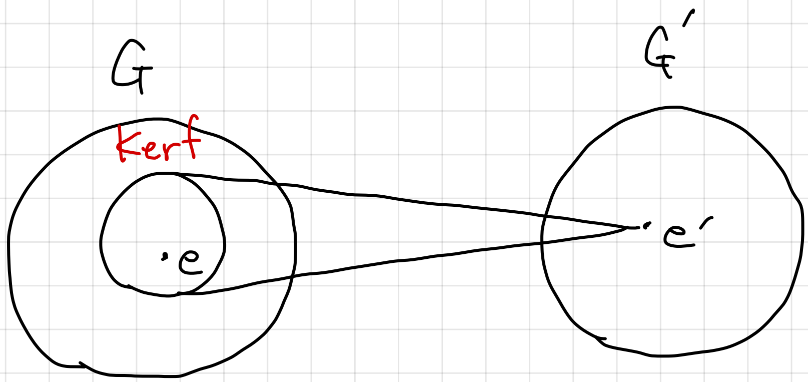


Ker

$f: G \to G'$ に対し

$\mathrm{Ker} f = f^{-1}(e') = \{x \in G \mid f(x) = e'\}$

を f の核という



Kerf は G の正規部分群になる.

(証)

$x, y \in \mathrm{Ker} f \quad f(xy^{-1}) = f(x) f(y)^{-1} = e'$

$\therefore$ Kerf は G の部分群

$x \in \mathrm{Ker} f$ とする.

$\forall g \in G \quad f(gxg^{-1}) = f(g) f(x) f(g^{-1})$

$= f(g) e' f(g^{-1}) = e'$

$\therefore \quad gxg^{-1} \in \mathrm{Ker} f$

例 $f : \mathbb{Z} \to S_3$

$$n \longmapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^n$$

$$f(0) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

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

$$f(2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$f(3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$\mathrm{Im} f = A_3$ ← S_3 の部分群

$\mathrm{Ker} f = 3\mathbb{Z}$ ← $\mathbb{Z}$ の(正規)部分群

§4 剰余群

剰余類

群 G とその部分群 H, $x \in G$ に対し

$$xH = \{xh \in G \mid h \in H\}$$

を x が定める H による左剰余類という

同値類の一種.

xH の任意の元を xH の代表現という.

$y \in xH$ のとき $\exists h$ $y = xh$ だから

$x = yh^{-1} \in yH$

よって $xH = yH$

$G/H = \{xH \mid x \in G\}$ と書く.

同様に. $Hx = \{hx \in G \mid h \in H\}$

を x が定める H による右剰余類といい

$H \backslash G = \{Hx \mid x \in G\}$ と書く

例

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

A_3

$$A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

$$S_3 / A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} A_3 , \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} A_3 \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} A_3 = A_3$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

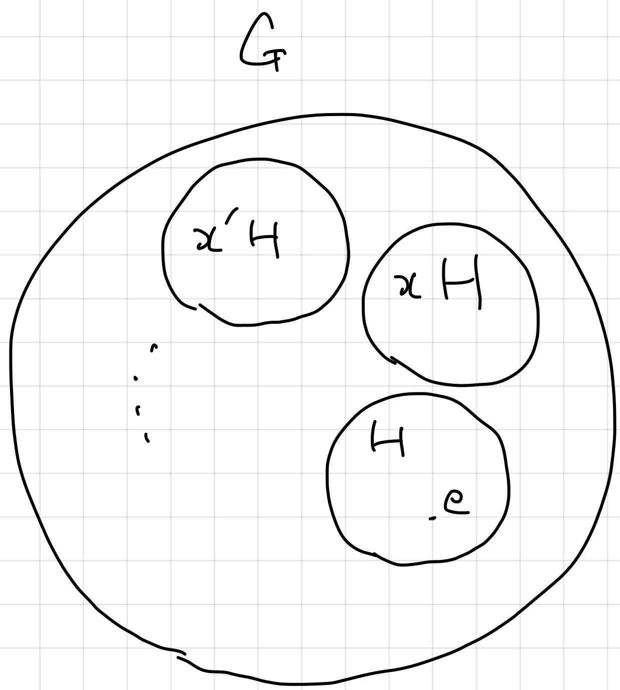
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} A_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} A_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} A_3$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} A_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} A_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} A_3$$

指数

G/H の濃度 ($= H\backslash G$ の濃度) を

H の G における指数といい. $(G:H)$ と書く.



ラグランジュの定理

$$\#G = (G:H)\#H$$

よって 有限群 G において 部分群の位数, 指数, 元の位数は G の位数の約数.

$\#S_3 = 6$ だから 位数 4 の部分群はない.

剰余群

$H \triangleleft G$ のとき

$$(xH)(yH) = xyH$$

によって G/H は群になる.

これを剰余群という.

$$\left[\begin{array}{l} \begin{cases} xH = x'H \\ yH = y'H \end{cases} \Rightarrow \begin{cases} x' = xh \\ y' = yh' \end{cases} \\ \Rightarrow x'y' = xhyh' \\ \qquad = xy\underbrace{y^{-1}hy}_{\in H}\underset{\in H}{h'} = xyh'' \\ \Rightarrow xyH = x'y'H \end{array}\right.$$

$$\begin{aligned} p : G &\longrightarrow G/H \\ x &\longmapsto xH \end{aligned}$$

$\mathrm{Ker}\, p = H$

例

$3\mathbb{Z}$ は $\mathbb{Z}$ の（正規）部分群

$\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

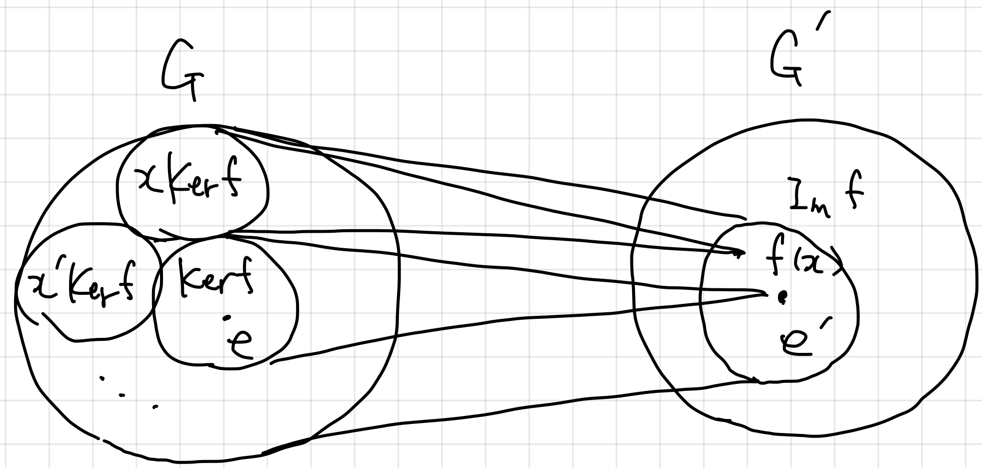
§5 準同型定理

準同型定理

$f: G \to G'$ 準同型写像のとき

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

は同型写像である.



(証)

・代表元のとり方によらないこと.

$x\,\mathrm{Ker}\, f = x'\,\mathrm{Ker}\, f$ のとき

${}^{\exists}k \in \mathrm{Ker}\, f \quad x = x'k$ だから

$$f(x) = f(x'k) = f(x')\underbrace{f(k)}_{e'} = f(x')$$

よって $\bar{f}(x\,\mathrm{Ker}\, f)$ が定まる.

・全射性

$x' \in \mathrm{Im} f$ のとき $\exists x \quad f(x) = x'$

$\bar{f}(x\mathrm{Ker} f) = f(x) = x'$ だから $\bar{f}$ は全射

・単射性

$\bar{f}(x\mathrm{Ker} f) = \bar{f}(x'\mathrm{Ker} f)$ とする.

$f(x) = \bar{f}(x') \qquad f(x)^{-1}\bar{f}(x') = e'$

$f(x^{-1}x') = e$

$\therefore x^{-1}x' \in \mathrm{Ker} f \qquad x' \in x\mathrm{Ker} f$

$\therefore x\mathrm{Ker} f = x'\mathrm{Ker} f$

・準同型性

$\bar{f}(x\mathrm{Ker} f\, x'\mathrm{Ker} f) = \bar{f}(xx'\mathrm{Ker} f)$

$= f(xx') = f(x)f(x') = \bar{f}(x\mathrm{Ker} f)\bar{f}(x'\mathrm{Ker} f)$

例 $f : \mathbb{Z} \to S_3$

$$n \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^n$$

$\mathrm{Im}\, f = A_3$

$\mathrm{Ker}\, f = 3\mathbb{Z}$

$A_3 \simeq \mathbb{Z}/\mathrm{Ker}\, f$