代数 1

みかん猫[1,*]
[1] ある猫カフェ

姑且随便写点啥

I. 予備知識

A. 数と演算

Definition I.1. $S \neq \emptyset$ を集合とし、写像 $\oplus$

$$
\begin{aligned}
S \times S &\longrightarrow S \\
(x, y) &\mapsto x \oplus y
\end{aligned}
$$

を二項演算とよぶ

Definition I.2. $a, b \in \mathbb{Z}, b \neq 0$ とする、b が a を割り切る $\Longleftrightarrow \exists c \in \mathbb{Z}, s.t. a = bc$、$b|a$ で書く

Definition I.3. $a, b \in \mathbb{Z}$

1. $d \in \mathbb{Z}$ が a, b の公約数 $\Longleftrightarrow d|a$ かつ $d|b$
2. $0 \leq d \in \mathbb{Z}$ が a, b の最大公約数

$\Longleftrightarrow \forall a, b$ の公約数 d' に対して、$d'|d$ をみたすこと．$gcd\,(a, b) = d$ あるいは $(a, b) = d$ とかく．なお、$(a, b) = 1$ のとき a, b は互いに素とよぶ

Theorem I.4. ユークリッドの互除法
$a, b \in \mathbb{N}$、数列 $\{a_n\}_{n \geq 0}$ を次のように定める：

$$
\begin{aligned}
a_0 &= a \\
a_1 &= b \\
a_{i-1} &= a_i \cdot q_i + a_{i+1}\, (i \geq 1) \\
0 &\leq a_{i+1} < a_i
\end{aligned}
$$

このとき $\exists N \in \mathbb{N}, s.t. a_{N+1} = 0$ となり、$gcd\,(a, b) = a_N$

Proof. $(a_{i-1}, a_i) = (a_i, a_{i+1})$ をいう
$\because$ 左辺を d、右辺を d' とする．$d|a_{i-1}, a_i$ より、$d|a_{i+1} = a_{i-1} - a_i q_i$
よって d は a_i と a_{i+1} の公約数、$d|d'$．また、$d'|a_i$ かつ $d'|a_{i+1}, d'|a_{i-1} = a_i q_i + a_{i+1}$
よって d' は a_{i-1} と a_i の公約数、$d'|d$
以上より $d = d'$
$\{a_n\}$ は単調減少の非負数列より、$\exists a_{N+1} = 0$．$(a, b) = (a_0, a_1) = \cdots = (a_{N-1}, a_N) = (a_N, a_{N+1} = 0)$
よって $a_{N-1} = a_N q_N, (a, b) = (a_{N-1}, a_N) = a_N$ □

Proposition I.5. 拡張ユークリッドの互除法
$a, b \in \mathbb{Z}$ は 0 でないとする、$\exists u, v \in \mathbb{Z}, au + bv = (a, b)$. u, v の求め方

Proof.

$$
\begin{aligned}
\begin{pmatrix} x_{11} & x_{12} & \alpha \\ x_{21} & x_{22} & \beta \end{pmatrix}
\begin{matrix} ① \\ ② \end{matrix}
&\longrightarrow
\begin{pmatrix} ② \\ ① - q \times ② \end{pmatrix} \\
&= \begin{pmatrix} x_{21} & x_{22} & \beta \\ x_{11} - q x_{21} & x_{12} - q x_{22} & \alpha - q\beta \end{pmatrix}
\end{aligned}
$$

$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}$ から始めて次々に上の変形をすると、$(2, 3)$ 成分が 0 の行列が出る
これを $\begin{pmatrix} u & v & d \\ u' & v' & 0 \end{pmatrix}$ とおくと、$d = (a, b)\,, au + bv = (a, b)$ が成立（$au' + bv' = 0$ も成立） □

Example I.6. $135u + 48v = (135, 48)$ となる $u, v \in \mathbb{Z}$ を求める

Proof.

$$\begin{aligned}
\begin{pmatrix} 1 & 0 & 135 \\ 0 & 1 & 48 \end{pmatrix} &\longrightarrow \begin{pmatrix} 0 & 1 & 48 \\ 1 & -2 & 39 \end{pmatrix} \\
&\longrightarrow \begin{pmatrix} 1 & -2 & 39 \\ -1 & 3 & 9 \end{pmatrix} \\
&\longrightarrow \begin{pmatrix} -1 & 3 & 9 \\ 5 & -14 & 3 \end{pmatrix} \\
&\longrightarrow \begin{pmatrix} 5 & -14 & 3 \\ -16 & 45 & 0 \end{pmatrix} \\
135 \times 5 + 48 \times (-14) = 3
\end{aligned}$$

□

Example I.7.

$$\begin{aligned}
6731 &= 4717 \cdot 1 + 2014 \\
4717 &= 2014 \cdot 2 + 689 \\
2014 &= 689 \cdot 2 + 636 \\
689 &= 636 \cdot 1 + 53 \\
636 &= 53 \cdot 12 + 0
\end{aligned}$$

$\gcd(6731, 4717) = 53$

Corollary I.8. $6717\mathbb{Z} + 4717\mathbb{Z} = 53\mathbb{Z}$
$\Longrightarrow x, y \in \mathbb{Z} : 6731x + 4717y = 53 \iff \begin{bmatrix} 1 & 0 & 6731 \\ 0 & 1 & 4717 \end{bmatrix}$

$$\begin{aligned}
\begin{bmatrix} 1 & 0 & 6731 \\ 0 & 1 & 4717 \end{bmatrix} &\longrightarrow \begin{bmatrix} 1 & -1 & 2014 \\ 0 & 1 & 4717 \end{bmatrix} \\
&\longrightarrow \begin{bmatrix} 1 & -1 & 2014 \\ -2 & 3 & 689 \end{bmatrix} \\
&\longrightarrow \begin{bmatrix} 5 & -7 & 636 \\ -2 & 3 & 689 \end{bmatrix} \\
&\longrightarrow \begin{bmatrix} 5 & -7 & 636 \\ -7 & 10 & 53 \end{bmatrix} \\
&\longrightarrow \begin{bmatrix} 77 & 127 & 0 \\ -7 & 10 & 53 \end{bmatrix} \\
-7 \cdot 6731 + 10 \cdot 4717 = 53
\end{aligned}$$

Remark I.9. $a, b \in \mathbb{Z}, d = (a, b), au + bv = d$ に対し、$u = u_0, v = v_0$ を整数解
このとき、任意の整数解は $u = u_0 + \dfrac{b}{d}k, v = v_0 - \dfrac{a}{d}k\ (k \in \mathbb{Z})$

II. 群の定義と例

Definition II.1. 群 $(G, \cdot)$ というのは、集合 G である二項演算 $\cdot$ を与えて、その二項演算 $\cdot$ は以下の条件を全てみたすこと

1. (閉) $\forall x, y \in G, x \cdot y \in G$
2. (結合律) $\forall x, y, z \in G, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
3. (単位元) $\exists e \in G, s.t. \forall x \in G, e \cdot x = x \cdot e = x$
4. (逆元) $\forall x \in G, \exists y \in G, s.t. x \cdot y = y \cdot x = e.$ このとき、$y = x^{-1}$ で表す

また、(1) $\sim$ (2) だけみたすと G は半群であり、(1) $\sim$ (3) だけみたすと G はモノイド（monoid）とよぶ

Definition II.2. 群 G の元の数を群の位数とよび、$|G|$ で表す．また、群の定義の閉より、$\forall x \in G, \exists n \in \mathbb{N}, s.t. x^n = e$、最も小さい n を群の元の位数とよび、$O(x)$ または $ord(x)$ で表す

Proposition II.3. G：群

1. $O(a) = O\left(a^{-1}\right)$
2. $\forall g \in G, O\left(gag^{-1}\right) = O(a)$
3. $O(a) = n$ なら、$O(a^r) = \dfrac{n}{(n,r)}$

Proof. G：群

1. $O(a) = n$ とすると、a^{-1} は逆元であるから $\left(a^{-1}\right)^n = (a^n)^{-1} = e^{-1} = e$．逆に、$O\left(a^{-1}\right) = m$ とすると、$(a^m)^{-1} = \left(a^{-1}\right)^m = e$ から、$O(a) \mid m$．（なぜなら $O(a)$ は $a^n = e$ をみたす最小の n）．よって、$m \mid n, n \mid m$ より、$O(a) = n = m = O\left(a^{-1}\right)$
2. $O\left(gag^{-1}\right) = n$ とすると、$\left(gag^{-1}\right)^n = ga\left(g^{-1}g\right)a\left(g^{-1}g\right)\cdots\left(g^{-1}g\right)ag^{-1} = ga^ng^{-1} = e$ から、$a^n = e$ で、$O(a) \mid n$. 逆に、$O(a) = m$ とすると、$a^m = e, ga^mg^{-1} = gg^{-1} = e, \cdots, g^ma^m\left(g^{-1}\right)^m = e$ から、$O\left(gag^{-1}\right) \mid m$．よって、$m \mid n, n \mid m$ より、$O\left(gag^{-1}\right) = n = m = O(a)$
3. $(n,r) = d, O(a^r) = k$ とする．$a^{\frac{r}{d}n} = e$ から、$k \left| \dfrac{n}{d} \right.$. $a^{rk} = e$ より、$n \mid rk$ から、$\dfrac{n}{d} \left| \dfrac{r}{d}k \right.$. また $d = (n,r)$ から、$\left(\dfrac{n}{d}, \dfrac{r}{d}\right) = 1$、よって $\dfrac{n}{d} \left| k \right.$ で、$k = \dfrac{n}{d}$

□

Example II.4.

1. $\mathbb{Z}$ は $+$ の計算で群になる
2. n 個の元からなる集合 G を $\{0, 1, \cdots, n-1\}$ で書き、二項演算を $\mod n$ での加法とすると、この群を C_n または $\mathbb{Z}/n\mathbb{Z}$ で表す
3. 集合の元を互換からなる置換 σ という二項演算で群になる
   (a) $\sigma' \circ \sigma$ も置換であるから、閉
   (b) 結合律はある数字を代入すればいい
   (c) $id \circ \sigma = \sigma \circ id = \sigma$ から、単位元は恒等写像
   (d) $\forall f$ は全射であるから、$\forall i \in K, \exists j \in K, s.t. f(j) = i$、また f は単射であるから、$f^{-1} : K \longrightarrow K$ は一々対応だから、f^{-1} は逆元である
4. $D_n = \langle \sigma, \tau : \sigma^n = \tau^2 = e, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$ は回すと鏡映操作からなる二面体群である
5. $GL(n) = \{A \in M(n) | \det(A) \neq 0\}$
6. $SL(n) = \{A \in M(n) | \det(A) = 1\}$
7. $O(n) = \left\{Q \in GL(n) \middle| QQ^T = Q^TQ = I\right\}$

Proposition II.5. 単位元と逆元は一意的に存在する

Proof.

1. $e, e' \in G$ はともに単位元であるとすると、$\forall g \in G, g \circ e' = e' \circ g = g = e \circ g = g \circ e$．すると $e' = e \circ e' = e' \circ e, e = e \circ e' = e' \circ e$．よって $e = e'$
2. $\forall g \in G$ に対し、逆元 γ, γ' が存在すると仮定すると $g \circ \gamma' = \gamma' \circ g = e = g \circ \gamma = \gamma \circ g$．すると

$$
\begin{aligned}
\gamma' &= \gamma' \circ e \\
&= \gamma' \circ (g \circ \gamma) \\
&= (\gamma' \circ g) \circ \gamma \\
&= e \circ \gamma \\
&= \gamma
\end{aligned}
$$

□

Corollary II.6. 左単位元と右単位元は必ず同じで、左逆元と右逆元も必ず同じである

Definition II.7. 集合 X 上の対称群は X から X への全単射からなる集合であり、S_X または $Sym(X)$ で表す

Definition II.8. $(G, \circ)$: 群
$\forall a, b \in G, a \circ b = b \circ a$ をみたすと、$(G, \circ)$ を交換群またはアーベル群とよぶ

III. 部分群と剰余類

Definition III.1. G 群、$H (\neq \emptyset) \subseteq G$
H が G の部分群であるとは G の演算で H も群になること. これは次の条件に同値

1. $e_G \in H$
2. $\forall x, y \in H \Longrightarrow xy \in H$
3. $\forall x \in H \Longrightarrow x^{-1} \in H$

Theorem III.2. G: 群、$H (\neq \emptyset) \subset G$

$$H \text{ は } G \text{ の部分群} \iff \forall x, y \in H, x^{-1}y \in H$$

Proof. $(\Longleftarrow)$

1. $\forall x, y \in H, x^{-1} \in H$、すると $xy = \left(x^{-1}\right)^{-1} y \in H$
2. $x \in H$ を任意に取り、$y = x$ とすると $e = y^{-1}x \in H$
3. $H \subset G$ より、H での結合律は成立する
4. $x \in G$ より、$x^{-1} \in G$ は必ず存在する. また、$x \in H, y = e \in H$ を取ると $x^{-1} = x^{-1}e = x^{-1}y \in H$

$(\Longrightarrow)$
$\forall x, y \in H$、H が群であるから、H の閉性より、$x^{-1}y \in H$ □

Definition III.3. G: 群、$S \subset G$

$$\langle S \rangle = \{s_1^{e_1} \cdots s_n^{e_n} : n \in \mathbb{N}, s_i \in S, e_i = \pm 1\}$$

$G = \langle S \rangle$ であれば、S は G を生成するといい、S の元を生成元と呼ばれる. S が空集合であれば、$\langle S \rangle$ は自明群 $\{e\}$ である

Definition III.4. G: 群、$H \subset G$: 部分群
$\forall x \in G, xH := \{xh | h \in H\}$ は部分群 H が x に関する左剰余類である
同様に、$\forall x \in G, Hx := \{hx | h \in H\}$ は部分群 H が x に関する右剰余類である

左剰余類と右剰余類は対称性より区別できないから、以下説明がない場合は左剰余類しか考えない

Proposition III.5. H は群、$h \in H$ なら $hH = H$

Proof. 群の閉性より、$\forall h \in H, \forall h_0 \in H, hh_0 \in H$ から、$hH \subseteq H$. $h_0 \in H$ を任意にとると、逆元の存在性より、$\forall h \in H, \exists h^{-1} \in H$. また、閉であることより $h^{-1}h_0 \in H$ から、$h_0 = hh^{-1}h_0 \in hH$,i.e. $H \subseteq hH$. よって、$hH = H$ □

Definition III.6. G: 群、$H \subset G$
H が G での指数というのは G における左剰余類または右剰余類のかずであり、$|G : H|$ または $[G : H]$ または $(G : H)$ で表す

Example III.7.
1. $n\mathbb{Z}$ の k に関する左剰余類は $k + n\mathbb{Z}$ で表す. $n\mathbb{Z}$ の異なる左剰余類の数は n 個である
2. 剰余類は必ず部分群になることではない、例えば $1 + 6\mathbb{Z}$ は単位元が存在しない

Theorem III.8. 剰余類分解は同値関係

Proof.（左剰余類だけ証明する）
G: 群、$x, y \in G$、$H \subset G, y \in xH \iff x^{-1}y \in H$. 以下はこれを使って「$x \sim y \iff x, y$ は同じ左剰余類に属している」という関係は同値関係を証明する.

1. $\forall x \in G, e \in H$ から、$x = xe \in xH, x \sim x$
2. $x^{-1}y \in H$ とすると、H は群であるから $y^{-1}x = \left(x^{-1}y\right)^{-1} \in H$. i.e. $x \in yH, y \sim x$
3. $x^{-1}y \in H, y^{-1}z \in H$ とすると、H が閉であるから、$\left(x^{-1}y\right)\left(y^{-1}z\right) = x^{-1}z \in H, x \sim z$

□

Definition III.9. G: 群、$H \subset G$
$\forall x, y \in G, x, y$ が同じ左剰余類に属していると、x と y は法 H に関して合同という

Theorem III.10 (Lagrange の定理). G: 群、$H \subset G$ は部分群なら $\dfrac{|G|}{|H|} \in \mathbb{Z}$

Proof. $x \in G$ とする. xH の定義より、$|xH| \leq |H|$. また、群の演算の一意性より、$|xH| = |H|$. 左剰余類は互いに交わらないから、各 x は xH に属する. よって、$|G|$ は各左剰余類の濃度の和で、$|H|$ の倍数である □

左剰余類の間での演算は必ず閉ではないが、どの条件をみたせば閉になるのか? $x, y \in G$ とし、それらの左剰余類はそれぞれ xH, yH で、$xH = \{xh_1 | h_1 \in H\}, yH = \{yh_2 | h_2 \in H\}$ から、$xHyH := \{xh_1yh_2 | h_1, h_2 \in H\}$ とする. xh_1y と xh_2y は同じ左剰余類に属していると仮定すると、$(xh_1y)^{-1}(xh_2y) \in H, (xh_1y)^{-1} = y^{-1}h_1^{-1}x^{-1}$ から、$y^{-1}h_1^{-1}x^{-1}xh_2y \in H$、言い換えれば $y^{-1}h_1^{-1}h_2y \in H$. ここで $y \in G, h_1, h_2 \in H$ から、$\forall y \in G, y^{-1}Hy := \left\{y^{-1}h_iy \middle| h_i \in H\right\} \subseteq H$ が成立すれば、その演算が閉になる
群の演算の一意性より、$g^{-1}Hg \subseteq H$ から $\left|g^{-1}Hg\right| = |H|$ が得られるから、その必要な条件は $g^{-1}Hg = H, i.e. Hg = gH$、言い換えれば左剰余類は右剰余類となじである

Definition III.11. 以上の条件をみたす部分群は正規部分群とよび、H は G の正規部分群であることを $H \triangleleft G$ または $G \triangleright H$ で表す. もっと簡単にいうと、$H \triangleleft G \iff \forall h_i \in H, \forall g \in G, gh_ig^{-1} \in H$

上の説明よりこの演算は閉から、(2) ∼ (4) をチェックすればいい

1. $x, y, z \in G, \forall h_i \in H, (xh_1yh_2)zh_3 = xh_1(yh_2zh_3)$ から、$(xHyH)zH = xH(yHzH)$
2. $\forall h_i \in H, h_iH = Hh_i = H$（閉より）から、$H$ は単位元
3. $xHx^{-1}H = HH = H$

Definition III.12. これより、左剰余類の集合での演算があって、この演算と左剰余類の集合で群になる. この群を G が法 H に関して合同する商群であり、G/H で表す. Lagrange の定理より、$|G/H| = \dfrac{|G|}{|H|}$

Proposition III.13. G: 群、$N \triangleleft G, \forall g \in G, NgN = gN$

Proof. ここは剰余類の演算であるから、$\forall g \in G$、単位元 $e \in N$ を取れば $NgN = g = gN$ がある □

Definition III.14. G: 群、$S \subset G$
$C(S) := \{g \in G | \forall s \in S, gs = sg\}$ とする. これを S の G における中心化群という. なお、$C(G)$ を G の中心という

$\forall c \in C(G), \forall g \in G, cg = gc$ から、任意に $h \in G$ を取って、$hch^{-1}g = hh^{-1}cg = cg = gc = gchh^{-1} = ghch^{-1}$ がある、i.e.$hch^{-1} \in C(G)$. よって、$C(G) \triangleleft G$

Definition III.15. G: 群、$S \subset G$
H は S を包含する最小の部分群であると、$N(S) = \{n \in G | nH = Hn\}$ とし、$N(S) \triangleleft H$ がある. この $N(S)$ を S の正規化群という

IV. 共役と共役類

Definition IV.1. $d, f \in G, \exists g \in G, s.t. gdg^{-1} = f$ なら、d と f が共役といい、$d \sim f$ で表す

この共役関係は同値関係、なぜなら

1. $g = ggg^{-1}$ から $g \sim g$
2. $d \sim f$ とすると、$\exists g \in G, s.t. gdg^{-1} = f$ から、$d = g^{-1}fg = g^{-1}f\left(g^{-1}\right)^{-1}$、$f \sim d$
3. $d \sim f, f \sim h$ とすると、$\exists g_1, g_2 \in G, s.t. h = g_2fg_2^{-1} = g_2g_1dg_1^{-1}g_2^{-1} = g_2g_1d\left(g_2g_1\right)^{-1}$ から、$d \sim h$

Definition IV.2. $a \in G$ を包含する同値類 $Cl(a) = \left\{gag^{-1} \middle| g \in G\right\}$ を a の同値類といい、G での互いに共役な元からなる集合は G の共役類という

Corollary IV.3. 互いに共役な元の位数は同じ

Proof. $gdg^{-1} = f$ を考える．$Ord(f) = m$ とすると、$f^m = e$
すると $d^m = g^{-1}\left(gdg^{-1}\right)^m g = g^{-1}f^m g = g^{-1}eg = e$ □

V. 直積と半直積

Definition V.1. G, H: 群
$\forall (g_i, h_i) \in G \times H, (g_1, h_1)(g_2, h_2) := (g_1g_2, h_1h_2)$、この演算と集合 $G \times H$ は群になる、これを G と H の直積という

ここで、単位元は明らかに (e_G, e_H) である

Definition V.2. 任意個の群 $\{A_\lambda\}_{\lambda \in \Lambda}$ を考える
これらの直積は写像 $\{a : \Lambda \to \mathscr{A} | \forall \lambda \in \Lambda, a(\lambda) \in A_\lambda\} \subset Map(\Lambda, \mathscr{A})$（ただし、$\mathscr{A} := \bigcup_{\lambda \in \Lambda} A_\lambda$）

Corollary V.3. $\forall G, K$: 群、$H \triangleleft G, J \triangleleft K$ とすると、$(G \times K)/(H \times J) \simeq G/H \times K/J$

Definition V.4. G: 群、G は部分群 H と正規部分群 N が存在し、$G = NH$ をみたすかつ $N \cap H = \{e\}$ なら G は N と H の内半直積といい、$G = N \rtimes H$ で表す

VI. 群同型と群準同型

Definition VI.1. 群 G と K に対し、$\forall x, y \in G, f(x)f(y) = f(xy)$ をみたす全単射 $f : G \to K$ が存在するなら、これらの群が同型といい、この写像を同型写像という．また、群 G から自身への同型写像はこの群の自己同型写像とよび、$Aut(G)$ で表す

Definition VI.2. 群 G と K に対し、写像 $f : G \to K$ は $\forall x, y \in G, f(x)f(y) = f(xy)$ をみたすなら、G と K は準同型といい、この f を準同型写像という．

Proposition VI.3. 準同型写像 $\phi : G \to H$ とすると

1. $\phi(e_G) = e_H$
2. $\phi\left(g^{-1}\right) = \phi(g)^{-1}$

Proof.
1. $\phi(e_G) = \phi(e_Ge_G) = \phi(e_G)\phi(e_G)$
2. $\phi\left(g^{-1}\right)\phi(g) = \phi\left(g^{-1}g\right) = \phi(e_G)$、さらに (1) より $\phi\left(g^{-1}\right)\phi(g) = e_H$

□

Definition VI.4. 準同型写像 $f : G \to H$ に対して、f の核を $Ker(f) := \{u \in G | f(u) = e_H\}$ と定義し、また f の像を $Im(f) := \{f(u) | u \in G\}$ で定義する

$u \in Ker(f)$ とすれば、$\forall g \in G$

$$\begin{aligned} f\left(g^{-1}ug\right) &= f(g)^{-1} f(u) f(g) \\ &= f(g)^{-1} e_H f(g) \\ &= f(g)^{-1} f(g) \\ &= e_H \end{aligned}$$

があるから、$g^{-1}Ker(f)g = Ker(f)$ より、$Ker(f)$ は G の正規部分群である

Theorem VI.5. 準同型定理
$\phi : G \to H$ を群の準同型写像とすると、$Im\phi \simeq G/ker\phi$
($\simeq$ は二つの群が同型であることを表す)

Proof. $N = ker\phi$ とおく、$\psi : G/N \to Im\phi$ を $\psi(gN) = \phi(g)$ と定義する．$gN, g'N \in G/N$ は $gN = g'N$ となる元とする．これらの ψ での行き先が一致することを確認する．$\psi(gN)\psi(g'N)^{-1} = \psi\left(gg'^{-1}N\right)$ である．$gN = g'N$ より $gg'^{-1} \in N$ であるから、右辺は $\psi(N) = e_{Im\phi}$ となる．よって、$\psi(gN) = \psi(g'N)$ であり、ψ は写像になっている
$gN, g'N \in G/N$ を取る

$$\begin{aligned} \psi(gNg'N) &= \psi(gg'N) \\ &= \phi(gg') \\ &= \phi(g)\phi(g') \\ &= \psi(gN)\psi(g'N) \end{aligned}$$

よって、ψ は準同型である．
ψ の全射性は定義より明らかであり、$gN \in G/N$ は $gN \in Ker\psi$ をみたすものとし、$e_{Im\phi} = \psi(gN) = \phi(g)$ より、$g \in Ker\phi = N$ であるから、$gN = e_{G/N}$ で、ψ は単射である．よって、ψ は全単射である □

Theorem VI.6. 同型定理
G: 群、H: G の部分群．N を G の正規部分群とするとき、$(HN)/N \simeq H/(H \cap N)$ が成立する

Proof. $\phi : H \to (HN)/N$ を $h \mapsto hN$ と定義すると、これは準同型である．このとき $Ker\phi = H \cap N$ であるから、$(HN)/N \simeq H/(H \cap N)$ □

Theorem VI.7. G: 群、$H, K \triangleleft G, K \triangleleft H$ とすると、$(G/K)/(H/K) \simeq G/H$ が成立する

Proof. $\phi : G/K \to G/H$ を $\phi(gK) = gH$ と定めると、これは準同型になる．このとき $Ker\phi = H/K$ であるから、準同型定理より $(G/K)/(H/K) \simeq G/H$ □

---

* Electronic address: 306581756@qq.com