群論 -代数的構造-

いろはの学習備忘録
https://168iroha.net

初回更新 2018 年 10 月 25 日
最終更新 2019 年 10 月 14 日

目次

第 1 章　基礎論 1

1.1　群の定義 1

1.2　変換作用の成す群 3

1.3　集合論的性質 5

1.4　群同型 10

1.5　生成系 15

第 1 章

基礎論

1.1　群の定義

定義 1.1

集合 S について，直積集合 S^n から集合 S' への写像 $f : S^n \to S'$ を与えたとき，f を S 上の n **項演算**という．特に，$S' \subseteq S$ ならば f という作用によって S は定まると考えることができ，このような S を**代数的構造**といい，集合と演算の組 (S, f) を**代数系**という．また，このような f を**閉じた演算**といい，一般に n 項演算は閉じた演算を指す場合が多い．特に，$n = 2$ であるとき $f : S \times S \to S$ であるが，このような 1 つの 2 項演算について閉じた代数的構造 S を**マグマ**という．

定理 1.1

代数系 (S, f) について，f が閉じた n 項演算とする．S の部分集合族 $\{T_k\}_{k\in\mathbb{N}}$ によるそれぞれの代数系 (T_k, f) が f について閉じているならば，$T = \bigcap_{k\in\mathbb{N}} T_k$ による代数系 (T, f) も f について閉じている．

Proof.

$f(T_k^n) \subseteq T_k$ かつ $T^n \subseteq T_k^n$ であるため，$f(T^n) \subseteq f(T_k^n) \subseteq T_k$ であり，$f(T^n) \subseteq \bigcap_{k\in\mathbb{N}} T_k = T$.

よって，命題は証明された．

□

集合 S の 2 項演算 f による代数系 (S, f) を与えたとして，任意の $a, b \in S$ により $f(a, b) \in S$ とあらわされるとき，2 項演算子 $*$ によって $a * b$ とあらわすとする．このとき，さらに任意の $c \in S$ を与えて

$$(a * b) * c = a * (b * c)$$

となるならば，S は f で**結合的**であるといい，S を**半群**という．このような演算法則を**結合法則**という．

ある $e \in S$ について

$$e * a = a * e = a$$

となるならば，f について e は S の**単位元**であるといい，これを満たす半群 S を**モノイド**という．さらに，a に対して

$$a * a' = e, \quad a'' * a = e$$

となる $a'' \in S$ が存在するとき，a' を a の**右逆元**といい a'' を a の**左逆元**という．特に，$a' = a''$ ならば a' を a の**逆元**といい，a^{-1} とあらわし，逆元が存在するような元を**可逆**もしくは**正則**という．

ここで，逆元について以下の定理を与える．

定理 1.2

モノイド S の元 $a \in S$ に右逆元と左逆元が存在するならばそれらは一致する．

Proof.

a の右逆元を a'，左逆元を a''，S の単位元を e とすれば

$$a' = ea' = (a''a)a' = a''(aa') = a''e = a''.$$

よって，命題は証明された．

□

また，

$$a * a = a$$

を満たすとき a を S の**冪等元**という．

ここで，以下の定義を与える．

定義 1.2

集合 G の 2 項演算 f による代数系 (G, f) について，$a, b \in G$ で $f(a, b) \in G$ を 2 項演算子 $*$ によって $a * b$ とあらわしたとき，任意の G の元について結合法則を満たし，単位元と逆元が存在するならば，G を**群**という．

これを論理式を用いてあらわすと以下のようになる．

1). マグマ

$$f : G \times G \to G$$

2). 結合法則

$$\forall a, b, c \in G \ s.t. \ (a * b) * c = a * (b * c)$$

3). 単位元の存在

$$\exists e \in G, \forall a \in G \ s.t. \ e * a = a * e = a$$

4). 逆元の存在

$$\exists e \in G, \forall a \in G, \exists a^{-1} \in G \ s.t. \ aa^{-1} = a^{-1}a = e$$

演算の順序が可換であるとき，f は**交換法則**を満たすといい，G を**可換群**もしくは**アーベル群**という．G がアーベル群で f が加法的な振る舞いをするとき代数系は $(G, +)$ とあらわし**加法群**もしくは**加群**といい，$a \in G$ の逆元は $-a$ とあらわす．

群論では基本的に乗法的記法をし，省略可能であれば省略するものとする．

ここで，群の演算における逆元に関する基本的な性質を示す．

補題 1.1　群 G の任意の $a, b \in G$ について

$$(ab)^{-1} = b^{-1}a^{-1}$$

が成り立つ．

Proof.

G の単位元を e とすれば

$$(b^{-1}a^{-1})ab = b^{-1}eb = b^{-1}b = e$$
$$ab(b^{-1}a^{-1}) = aea^{-1} = aa^{-1} = e$$

となり，$b^{-1}a^{-1}$ が ab の逆元となることから

$$(ab)^{-1} = b^{-1}a^{-1}$$

が成り立つ．

よって，命題は証明された．

□

以下では群の例を示す．

体 K 上のベクトル空間 V で $\dim V = n$ とすれば，線型写像 $f : V \to V$ 全体の集合は $GL_n(K)$ とあらわし，これは形式的には行列としてあらわすことができる．また，$\mathbb{C}$ 上の n 次正方行列全体を $M_n(\mathbb{C})$ とすれば，これは明らかに半群であり，逆行列の存在条件より

$$\{A \in M_n(\mathbb{C}) \,|\, \det A \neq 0\}$$

というように定義すれば，これは $GL_n(\mathbb{C})$ に等しいことがわかる．このとき，$GL_n(K)$ を K 上の積における n **次一般線型群**という．

また，$GL_n(\mathbb{C})$ の部分群として定義される

$$SL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \,|\, \det A = 1\} = \{A \in GL_n(\mathbb{C}) \,|\, \det A = 1\} \subset GL_n(\mathbb{C})$$

を n **次特殊線型群**といい，n 次単位行列を I_n としたときのユニタリ行列の集合

$$U_n = \{A \in M_n(\mathbb{C}) \,|\, A^*A = AA^* = I_n\} = \{A \in GL_n(\mathbb{C}) \,|\, A^*A = AA^* = I_n\} \subset GL_n(\mathbb{C})$$

を n **次ユニタリ群**という．同様にして $\mathbb{R}$ 上で考えれば

$$O_n = \left\{A \in M_n(\mathbb{R}) \,\middle|\, A^TA = AA^T = I_n\right\} = \left\{A \in GL_n(\mathbb{R}) \,\middle|\, A^TA = AA^T = I_n\right\} \subset GL_n(\mathbb{R})$$

という積における群を n **次直交群**という．

U_n と O_n で $SL_n(\mathbb{C})$ および $SL_n(\mathbb{R})$ のような特殊化を考えれば，

$$\begin{aligned} SU_n =& SL_n(\mathbb{C}) \cap U_n \\ SO_n =& SO_n(\mathbb{R}) \cap O_n \end{aligned}$$

と定義を与えることができ，それぞれを n **次特殊ユニタリ群**，n **次特殊直交群**という．

1.2　変換作用の成す群

自然数からなる集合 $\Omega = \{1, 2, \cdots, n\}$ を与え，全単射 $\sigma : \Omega \to \Omega$ を定義すれば，それは形式的にあらわしたグラフは

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

となり，$i_k = \sigma(k)$ とあらわすとすれば

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

とあらわすことができる．この σ のような操作を**置換**といい，置換の組み合わせは $n!$ だけ存在する．置換全体の集合を $\mathfrak{S}(\Omega)$ としたとき，置換演算について $\mathfrak{S}(\Omega)$ の任意の元は写像であり，それは全単射であることから結合法則を満たし，$\mathfrak{S}(\Omega)$ の任意の元には逆元が存在する．また，単位元は

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \in \mathfrak{S}(\Omega)$$

というように自明な恒等写像で与えられる．つまり，$\mathfrak{S}(\Omega)$ は置換演算について群であり，$\mathfrak{S}(\Omega)$ を n **次対称群**といい，$\mathfrak{S}_n$ もしくは $\mathrm{Sym}(n)$ とあらわすこともある．また，$\mathfrak{S}_n$ は置換の組み合わせの総数より $n!$ 個の元をもつ．

また，$k \in \Omega$ に対する置換で $i \leq n$ を用いて

$$\begin{pmatrix} k & \sigma(k) & \cdots & \sigma^i(k) \\ \sigma(k) & \sigma^2(k) & \cdots & k \end{pmatrix}$$

のように k は σ に対して巡回的になり，このような置換を長さ $i+1$ の**巡回置換**といい，$\sigma = (k\ \sigma(k)\ \sigma^2(k)\ \cdots\ \sigma^i(k))$ とあらわされ，$\{k, \sigma(k), \sigma^2(k), \cdots, \sigma^i(k)\}$ を**巡回域**という．特に，長さが 2 の巡回置換を**互換**といい，2 つの巡回置

換が共通の文字を含まないとき，2 つの巡回置換は**互いに素**であるという．

ここで，以下の補題を示す．

補題 1.2　互いに素な巡回置換は置換の積において可換である．

Proof.

対称群 $\mathfrak{S}_n$ の互いに素な巡回置換を $\sigma, \tau \in \mathfrak{S}_n$ とする．互いに素であることから，それぞれの巡回域全域の集合を A, B とすれば $A \cap B = \emptyset$ である．また，$\Omega = \{1, 2, \cdots, n\}$ を与えたとき，$\mathfrak{S}_n$ は Ω に対する対称群であるとする．

$k \in \Omega$ に対して $k \in A$ ならば $k \notin B$ であることから $\tau(k) = k$ であり，

$$\sigma(\tau(k)) = \sigma(k)$$

となる．また，$\sigma(k) \in A$ であるため $\sigma(k) \notin B$ となるため

$$\tau(\sigma(k)) = \sigma(k)$$

となる．つまり，$\sigma \circ \tau = \tau \circ \sigma$ となる．これは，$k \in B$ のときも $k \notin A$ となることから同様に示すことができる．

よって，命題は証明された．

□

ここで，置換の最も基本的である定理を示す．

定理 1.3

任意の置換は巡回置換の互いに素の場合を除き，一意に巡回置換の積に分解することが可能である．さらに，任意の巡回置換は互換の積に分解可能であり，その分解方法によらず分解数が偶数か奇数かは一意に決まる．また，偶数個の互換によって構成される置換を**偶置換**，奇数個の互換によって構成される置換を**奇置換**という．

Proof.

対称群 $\mathfrak{S}_n$ の任意の元 $\sigma \in \mathfrak{S}_n$ の n についての数学的帰納法により巡回置換への分解の証明を与える．

$n = 2$ のときは置換の組み合わせは

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

のみであるため成り立つ．次に，n で成り立つことを仮定して $n+1$ で成り立つことを示す．

$\sigma(n) = n$ であるときは $\sigma \in \mathfrak{S}_{n-1}$ とすることができるため成り立つ．$\sigma(n) \neq n$ のとき，巡回置換 $\tau = (\sigma(n)\ n)$ を定義することで $\tau(\sigma(n)) = n$ となり，$\tau \circ \sigma \in \mathfrak{S}_{n-1}$ とすることができるため成り立つ．

以上より，$\mathfrak{S}_n$ の任意の元は巡回置換へと分解することが可能である．

次に，巡回置換を互換へ分解することを考える．巡回置換を $\sigma = (i_1\ i_2\ \cdots\ i_n)$ とすれば，

$$\begin{aligned}(i_1\ i_2\ \cdots\ i_n) =& \begin{pmatrix} i_1 & i_n & i_2 & \cdots & i_{n-1} \\ i_n & i_1 & i_2 & \cdots & i_{n-1} \end{pmatrix} \begin{pmatrix} i_1 & i_2 & \cdots & i_{n-1} & i_n \\ i_2 & i_3 & \cdots & i_1 & i_n \end{pmatrix} \\ =& (i_1\ i_n)(i_1\ i_2\ \cdots\ i_{n-1})\end{aligned}$$

となるため，

$$(i_1\ i_2\ \cdots\ i_n) = (i_1\ i_n)(i_1\ i_{n-1}) \cdots (i_1\ i_2)$$

というように互換に分解されることから巡回置換は互換の積に分解可能である．

互換の 2 乗は恒等写像となり，恒等写像は偶置換である．σ が偶置換であると仮定して他の表現 τ があるとすれば

$$\sigma = \tau \ \Rightarrow\ \tau^{-1} \circ \sigma = \mathrm{id}$$

となり，恒等写像は偶置換であることから τ も偶置換となる．これは奇置換の場合でも同様に示される．

よって，命題は証明された．

□

この定理より，任意の置換は偶置換か奇置換となる．これにより以下の定義を与えることができる．

定義 1.3

対称群 $\mathfrak{S}_n$ の任意の元 $\sigma \in \mathfrak{S}_n$ の偶置換もしくは奇置換かによって

$$\mathrm{sgn}\,(\sigma) = \begin{cases} 1 & (even\ permutation) \\ -1 & (odd\ permutation) \end{cases}$$

と定めたとき，これを σ の**符号**という．また，$\mathfrak{S}_n$ の全ての偶置換の集合は $\mathfrak{S}_n$ の部分群である．これを n **次交代群**といい，$\mathfrak{A}_n$ もしくは $\mathrm{Alt}(n)$ とあらわす．$\mathfrak{A}_n$ の要素数は $\mathfrak{S}_n$ の要素数の半分になることから $\frac{n!}{2}$ となる．

また，対称群は集合に作用する写像の集合であるが，より一般の作用を考えると，ある集合 X に対して任意の全単射 f, g が集合 G に属するとき，$f \circ g \in G$ で $f^{-1} \in G$ である G を考えることができる．このとき，G を**変換群**といい，対称群は変換群の特殊な場合として扱われる．例えば，体 K 上のベクトル空間 V に対して $\dim V = n$ ならば一般線型群 $GL_n(K)$ は V に作用する変換群であり，これを**行列群**という．これはベクトルの $V \to V$ となる線型変換のことである．

1.3　集合論的性質

群が集合論的性質によりどのように振る舞うのかを考える．そのため，まずはいくつかの定義を与える．

定義 1.4

群 G を与えたとき，$|G|$ を G の**位数**といい，位数が有限であるとき **有限群**，位数が無限大であるとき**無限群**という．空でない部分集合 $H \subseteq G$ が

$$\forall a, b \in H\ s.t.\ a^{-1} \in H\ \Rightarrow\ a^{-1}b \in H$$

を満たすとき，H は G の**部分群**という．これは仮定より閉じた演算で逆元が存在することと結合法則は自明であるが，単位元 e は $b = a$ とすることで $a^{-1}a = e \in H$ となるため H は群である．部分群で位数が最大であるのは G 自身であり，最小であるのは単位元のみから構成される群である．これらを**自明な部分群**といい，特に単位元から構成される部分群を**単位群**という．また，$H \subset G$ であるとき H を**真部分群**という．

群 $G_1, G_2, \cdots, G_n$ を与えたとき，これらの和集合は一般に群を形成しないことは自明である．しかし，直積集合においては $a, b \in G_1 \times G_2 \times \cdots \times G_n$ で $a = (a_1, a_2, \cdots, a_n)$ および $b = (b_1, b_2, \cdots, b_n)$ として

$$ab = (a_1b_1, a_2b_2, \cdots, a_nb_n)$$

とすることで $G_1 \times G_2 \times \cdots \times G_n$ は明らかに群である．これを**群の直積**もしくは**直積群**といい，

$$G_1 \otimes G_2 \otimes \cdots \otimes G_n$$

とあらわす．$G_1, G_2, \cdots, G_n$ が加法群であるならば

$$a + b = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)$$

とあらわし，これを直積の代わりに群の**直和**といい，

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n$$

とあらわされる．例えば $\mathbb{Z}$ は加法群であるが，$\mathbb{Z}^n$ も座標系の概念を用いることで加法群である．これは

$$\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n\ 個}$$

とあらわすことで群の直和として扱われる．

群 G とその部分群 $H \subseteq G$ を与えたとき，$g \in G$ のみからなる集合との積を

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

としたとき，以下の補題が与えられる．

補題 1.3　群 G とその部分群 $H \subseteq G$ を与えたとき，$a, b \in G$ に対して同値関係は

$$a \sim b \;\Leftrightarrow\; a^{-1}b \in H$$

と定めることができ，$g_1 \in G$ による g_1H は G の g_1 からなる同値類

$$G_1 = \{g \in G \,|\, g \sim g_1\}$$

と等しい．つまり，任意の $g \in G$ を与えれば，gH によって G は類別される．これは Hg でも同様に与えられる．

Proof.

まずは同値関係について確かめる．反射律は $b = a$ とすれば H は単位元をもつため成り立つ．対称律は

$$a^{-1}b \in H \;\Leftrightarrow\; b^{-1}a \in H$$

を満たせばいいが，補題 1.1 より $(a^{-1}b)^{-1} = b^{-1}a \in H$ であるため，これも成り立つ．推移律は $c \in G$ を与えたとき

$$a^{-1}b \in H, b^{-1}c \in H \;\Rightarrow\; a^{-1}c \in H$$

を満たせばいいが，H は演算について閉じているため

$$(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}c \in H$$

となり，これも成り立つ．よって，この同値関係の定義は well-defined である．

$g_1, g_2 \in G$ で $g_1 \not\sim g_2$ のとき $g_1H \cap g_2H \neq \emptyset$ であるとする．このとき，$c \in g_1H \cap g_2H$ が存在して

$$c = g_1h_1 = g_2h_2$$

となる $h_1, h_2 \in H$ が存在する．このとき，両辺に h_2^{-1} の積を取ることで

$$g_1h_1h_2^{-1} = g_2$$

が得られ，$h_1h_2^{-1} \in H$ より $g_2 \in g_1H$ となり，$g_1 \sim g_2$ となることから $g_1 \not\sim g_2$ に矛盾するため，$g_1H \cap g_2H = \emptyset$ となる．これは Hg_1 についても同様である．

よって，命題は証明された．

□

この補題より gH と Hg は G の同値類であり，それぞれを**左剰余類**および**右剰余類**といい，$gH = Hg$ となるときは単に**剰余類**という．また，g は左剰余類と右剰余類の代表元となり，それぞれにおける代表元から構築される G の商集合を**左代表系**および**右代表系**といい，$gH = Hg$ となるときは**完全代表系**という．左剰余類と右剰余類の商集合，つまりは左剰余類および右剰余類の集合を G/H および $H \setminus G$ とあらわし，$gH = Hg$ となるときは単に G/H とあらわす．また，集合論における完全代表系の性質より，集合 A が完全代表系であるとは，包含写像と商写像の合成 $A \hookrightarrow G \to G/H$ が全単射であるということである．

ここで，以下の補題を与える．

補題 1.4　有限群 G とその部分群 $H \subseteq G$ を与えたとき，T を左代表系とすれば T^{-1} は右代表系である．つまり，左代表系と右代表系，並びに完全代表系の元の間には 1 対 1 の対応が存在する．

Proof.

この命題は任意の左代表系の元の逆元が右代表系の元となることで十分である．$g \in G$ を左代表系の任意の元としたとき，$a \in G$ に対して左剰余類の同値関係の定義より

$$a \sim_L g \ \Leftrightarrow \ a^{-1}g \in H$$

となり，これが右剰余類の同値関係の定義より

$$a^{-1} \sim_R g^{-1} \ \Leftrightarrow \ a^{-1}g \in H$$

となればいい．左剰余類の同値関係の関係式を仮定したとき $a^{-1}g \in H$ であるため，左代表系の任意の元の逆元が右剰余類の同値関係を満たすことがわかる．これは右剰余類の同値関係の関係式を仮定したときも同様である．

よって，命題は証明された．

□

この補題より

$$|G/H| = |H \setminus G|$$

という関係式が得られ，これを G における H の**指数**といい，

$$[G : H] = |G/H| = |H \setminus G|$$

とあらわす．

ここで，以下の定理を示す．

定理 1.4　ラグランジュの定理

有限群 G とその部分群 $H \subseteq G$ を与え，さらに H の部分群 $K \subseteq H$ を与えたとする．このとき，指数について

$$[G : K] = [G : H][H : K]$$

が成り立つ．これを**ラグランジュの定理**という．

Proof.

G の左代表系の集合を T としたとき，G は

$$G = \bigcup_{g \in T} gH$$

と類別することができ，$|G| = |T||H|$ となることから $[G : H] = |T|$ である．同様にして，H の左代表系の集合を T' としたとき，H は

$$H = \bigcup_{h \in T'} hK$$

と類別することができ，$|G| = |T'||H|$ となることから $[G : H] = |T'|$ である．また，G の類別に対して H の類別を代入することで

$$G = \bigcup_{g \in T} g \bigcup_{h \in T'} hK = \bigcup_{g \in T} \bigcup_{h \in T'} ghK$$

となり，$|G| = |T||T'||K|$ となることから $[G : K] = |T||T'|$ となる．これに対して $|T|$ と $|T'|$ の式を代入することで

$$[G : K] = [G : H][H : K]$$

が得られる．

よって，命題は証明された．

□

これより，ただちに以下の系が得られる．

系 1.4-1　有限群 G の部分群の位数は $|G|$ の約数である．

Proof.

部分群 $H \subseteq G$ はラグランジュの定理の証明中より $n \in \mathbb{N}$ によって $|G| = n|H|$ という関係式が与えられ，これは $|H|$ は $|G|$ の約数であることを示している．

よって，命題は証明された．

□

この定理は有限群における著しい性質を与えている．

ここで，剰余類をより一般に扱うために以下の定義を与える．

定義 1.5

群 G の部分群 $S \subseteq G$ について，$g \in G$ を用いて

$$gSg^{-1}$$

の形であらわされる G の部分集合を**共役**という．左剰余類の同値関係と同様にして $a \in G$ に対して

$$g \sim a \ \Leftrightarrow \ g^{-1}a \in Sg^{-1}$$

という同値関係を与えれば，これは well-defined であり，gSg^{-1} は同値類になり，これで類別が可能である．この同値類を特に**共役類**といい，$S = gSg^{-1}$ が成り立つとき S を G の**正規部分群**もしくは**不変部分群**という．また，S が G の正規部分群であることは

$$S \lhd G, \quad G \rhd S$$

とあらわす．

定理 1.5

群 G の部分群 $S \subseteq G$ で S に対して可換な集合と S の任意の元に対して可換な集合

$$\begin{aligned} N_G(S) =& \{g \in G \,|\, gS = Sg\} \\ C_G(S) =& \{g \in G \,|\, \forall s \in S \ s.t. \ gs = sg\} \end{aligned}$$

はそれぞれ群となり，それぞれを**正規化群**，**中心化群**といい，

$$N_G(S) \rhd C_G(S)$$

となる．特に，$Z(G) = C_G(G)$ を G の**中心**という．

Proof.

まずはそれぞれが G の部分群となることを示す．これは演算が閉じていて逆元がそれぞれの元に含まれることを示すことで十分である．$gS = Sg$ より $gs_1 = s_2g$ となる $s_1, s_2 \in S$ が存在する．つまり，$g_1, g_2 \in G$ に対して $s_1, s_2, s_3 \in S$ で

$$\begin{aligned} g_1s_1 = s_2g_1 \ &\Leftrightarrow \ g_1 = s_2g_1s_1^{-1} \\ g_2s_3 = s_1g_2 \ &\Leftrightarrow \ g_2 = s_1g_2s_3^{-1} \end{aligned}$$

という関係式を与えることができ，g_1 と g_2 の積は

$$\begin{aligned} g_1g_2 =& s_2g_1s_1^{-1}s_1g_2s_3^{-1} \\ =& s_2g_1g_2s_3^{-1} \\ g_1g_2s_3 =& s_2g_1g_2 \end{aligned}$$

となるため $gS = Sg$ を満たす．逆元は

$$g^{-1}s_1 = s_2g^{-1} \ \Leftrightarrow \ s_1g = gs_2$$

となることから $gS = Sg$ を満たすため，$N_g(S)$ は G の部分群である．また，$C_G(S)$ は $N_G(S)$ が G の部分群であるならば明らかに G の部分群となるため，それぞれが G の部分群になることが示された．

次に，$C_G(S)$ が $N_G(S)$ の正規部分群であることを示す．$s \in S$ で $gs = sg$ となる g の集合が $C_G(S)$ であるが，

$$g = sgs^{-1}$$

とあらわすことができるため，任意の $n \in N_G(S)$ を作用させて正規部分群の定義を満たすことを示せばいい．

$$\begin{aligned} ngn^{-1} =& nsgs^{-1}n^{-1} \\ =& (ns)g(ns)^{-1} \end{aligned}$$

このとき，$n \in G$ であるため $ns \in C_G(S)$ である．つまり，$g \in C_G(S)$ であることから $(ns)g(ns)^{-1} \in C_G(S)$ であり，$C_G(S) = nC_G(S)n^{-1}$ が得られる．以上より，正規部分群の定義を満たすため $N_G(S) \rhd C_G(S)$ である．

よって，命題は証明された．

□

これより，剰余類であるとは $gH = Hg$ であるため，$G \rhd H$ とならなければならないことがわかる．剰余類の同値類の定義より $g_1, g_2 \in G$ で

$$g_1 \sim g_2 \ \Leftrightarrow \ g_1^{-1}g_1, g_1g_2^{-1} \in H$$

であるが，任意の $x, x', y, y' \in G$ で $x \sim x'$ かつ $y \sim y'$ の同値関係が与えられたとき

$$\begin{array}{cccccc} y'^{-1}y \in H & \Leftrightarrow & y \in y'H & \Leftrightarrow & xy \in xy'H & \Leftrightarrow & xy \sim xy' \\ y'x^{-1} \in H & \Leftrightarrow & y' \in Hx & \Leftrightarrow & y'y' \in Hxy' & \Leftrightarrow & y'y' \sim xy' \\ x'y'^{-1} \in H & \Leftrightarrow & x' \in Hy' & \Leftrightarrow & x'y' \in Hy'y' & \Leftrightarrow & x'y' \sim y'y' \end{array}$$

となり，推移律より $xy \sim x'y'$ となる．

ここで，このような同値関係を一般化したものついての定義を与える．

定義 1.6

2 項演算による代数的構造 S 上で定義される同値関係 $\sim$ が任意の $x, x', y, y' \in S$ で $x \sim x'$ および $y \sim y'$ といった同値関係が与えられたとき

$$xy \sim x'y'$$

となるならば，このような同値関係を**合同関係**といい $x \equiv y$ とあらわす．

この定義より，剰余類は合同関係として考えることができる．

また，合同関係について以下の定理を与えられる．

定理 1.6

マグマ S 上で定義される合同関係 $\sim$ による商集合 $S/\sim$ は自然に定義される演算によりマグマを形成する．特に，S が半群であるならば $S/\sim$ は半群，モノイドであるならばモノイド，群であるならば群となる．

Proof.

$x \in S$ による同値類を $[x]$ とあらわすとする．$[x], [y] \in S/\sim$ に対して

$$[x][y] = [xy]$$

により $S/\sim$ 上に演算を定義することができ，これが同値類の代表元によらないならば $[x'], [y'] \in S/\sim$ で

$$[x] = [x'], [y] = [y'] \ \Rightarrow \ [xy] = [x'y']$$

となればいいが，これは S 上の合同関係の仮定により成り立つ．つまり，$S/\sim$ は演算について閉じておりマグマを形成する．

また，S が半群であるならば $x, y, z \in S$ に対する $[x], [y], [z] \in S/\sim$ で

$$([x][y])[z] = [xy][z] = [(xy)z] = [xyz]$$
$$[x]([y][z]) = [x][yz] = [x(yz)] = [xyz]$$

となるため，$S/\sim$ は結合法則を満たし半群となる．S がモノイドであるならば，S の単位元 $e \in S$ による同値類 $[e]$ が単位元となるため $S/\sim$ はモノイドとなる．S が群であるならば，$[x]$ の逆元は x の逆元 x^{-1} による同値類 $[x^{-1}]$ とすれば

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

となるため $S/\sim$ は群となる．

よって，命題は証明された．

□

この定理より，G の剰余類による商集合 G/H は自然に群を形成し，これを**剰余群**もしくは**商群**という．

1.4　群同型

群は集合の 1 つの形態であることから写像を定義することができる．群には単位元や逆元といった群の演算に付随する元が存在するため，そのような構造を保存するような写像を考えるべきである．

そこで，以下の定義を与える．

定義 1.7

2 項演算による代数的構造 G, G' における写像 $f : G \to G'$ が任意の $a, b \in G$ で

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

を満たすとき，f を**準同型写像**といい，ab といった G 上の演算が G' 上の演算 $f(a)f(b)$ に写されることを意味する．また，f が全射であるとき**上への準同型写像**といい，単射であるとき**中への同型写像**という．特に，f が全単射であるとき f を**上への同型写像**もしくは単に**同型写像**という．

G, G' を群としてそれぞれの単位元を e, e' とすれば

$$f(e) = f(ee) = f(e)f(e) \ \Rightarrow \ f(e) = f(e)(f(e))^{-1} = e'$$

となり，さらに $g \in G$ で

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

となり，群の代数的構造を保存する写像となる．また，G と G' が同型写像によって関係づけられるとき，G と G' は**同型**であるといい $G \cong G'$ とあらわす．

群の準同型写像で e 以外にも e' に移される要素は存在し，それは構造を保存する写像の単射性の指標となる．このような e' に移される G の元の集合を**核**もしくは**カーネル**といい

$$\mathrm{Ker}\, f = \{g \in G \mid f(g) = e'\}$$

で与えられる．

ここで，同型に関する定理を与えるために以下の補題を示す．

補題 1.5　群 G, G' で準同型写像 $f : G \to G'$ を与えたとき，G の単位元を e として $\mathrm{Ker}\, f = \{e\}$ となることと f が単射であることは必要十分である．

Proof.

$\mathrm{Ker}\, f = \{e\}$ のとき，$a, b \in G$ で $f(a) = f(b)$ とすれば

$$f(ab^{-1}) = f(a)(f(b))^{-1} = f(e)$$

となるため $ab^{-1} \in \mathrm{Ker}\, f$ であり，$a = b$ となる．f が単射ならば，任意の $x \in \mathrm{Ker}\, f$ で

$$f(x) = f(e)$$

となるが，f の単射性より $x = e$ となる．

よって，命題は証明された．

□

補題 1.6　準同型写像の合成は準同型写像である．

Proof.

2 項演算による代数的構造を S, S', S'' として，準同型写像により $f : S \to S'$ および $f' : S' \to S''$ とあらわされるとする．任意の $a, b \in S$ を与えれば

$$f' \circ f(ab) = f'(f(a)f(b)) = f'(f(a))f'(f(b))$$

となるため，$f' \circ f$ は準同型写像である．

よって，命題は証明された．

□

補題 1.7　群 G, G' で準同型写像 $f : G \to G'$ を与えたとき，$\mathrm{Ker}\, f$ は G の正規部分群となる．

Proof.

G' の単位元を e' とすれば

$$\mathrm{Ker}\, f = \{g \in G \mid f(g) = e'\}$$

であり，G の任意の元 $a \in G$ に対して

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

となるため，$N = \mathrm{Ker}\, f$ として $N = aNa^{-1}$ を満たすため $\mathrm{Ker}\, f$ は G の正規部分群となる．

よって，命題は証明された．

□

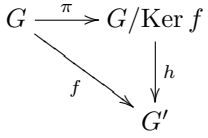
これより，以下の定理を与えることができる．

定理 1.7　群の準同型定理

群 G, G' で上への準同型写像 $f : G \to G'$ を与えたとき，$G/\mathrm{Ker}\, f \cong G'$ である．これを群の**準同型定理**という．

Proof.

商写像の普遍性より商写像 $\pi : G \to G/\mathrm{Ker}\, f$ を与えたとき，$f = h \circ \pi$ を満たす写像 h が存在する．



$x \in G$ の正規部分群における同値類を $[x]$ とすれば $[x], [y] \in G/\mathrm{Ker}\, f$ および G' の単位元 e' で

$$[x] = [y] \ \Leftrightarrow\ x^{-1}y \in \mathrm{Ker}\, f \ \Leftrightarrow\ e' = f(x^{-1}y) = (f(x))^{-1}f(y) \ \Leftrightarrow\ f(x) = f(y)$$

となり，h は単射であり，f は全射であることから h は全単射となる．これより，h が準同型写像であることを示せば十分である．

$$h([x][y]) = h([x][y]) = (h \circ \pi)(xy) = f(xy) = f(x)f(y) = h([x])h([y])$$

これは h が準同型写像であることを示すため，h は同型写像であり，$G/\mathrm{Ker}\, f \cong G'$ である．

よって，命題は証明された．

□

定理 1.8　第 1 同型定理

群 G, G' で上への準同型写像 $f : G \to G'$ を与えたとき，H' を G' の正規部分群とすれば逆像 $H = f^{-1}(H')$ は G の正規部分群であり，$G/H \cong G'/H'$ である．これを群の**第 1 同型定理**という．

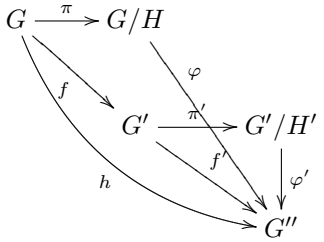
Proof.

$f^{-1}(H')$ は明らかに G の部分群であるため，任意の $h \in f^{-1}(H')$ および $g \in G$ を与えれば

$$f(ghg^{-1}) = f(g)f(h)(f(g))^{-1} \in H'$$

となり，$ghg^{-1} \in f^{-1}(H')$ となるため，$H = f^{-1}(H')$ は G の正規部分群である．

準同型写像 $f' : G' \to G$ を満たす群 G'' を与えたとき，$h = f' \circ f$ は準同型写像であり，商写像 π, π' を与えて準同型定理を満たすように以下の可換図式を与える．



このとき，φ と φ' は準同型定理より同型写像となるため，$G/H \cong G''$ および $G'/H' \cong G''$ となり，$G/H \cong G'/H'$ が得られる．

よって，命題は証明された．

□

定理 1.9　第 2 同型定理

群 G' の部分群 $N, H \in G$ で N が G の正規部分群であるとき，$H \cap N$ は H の正規部分群であり，$HN/N \cong H/(H \cap N)$ である．なお，

$$HN = \{hn \,|\, h \in H, n \in N\}$$
$$H^{-1} = \left\{h^{-1} \,\middle|\, h \in H\right\}$$

である．これを群の**第 2 同型定理**という．

Proof.

まずは $H \cap N$ が H の正規部分群となることを示す．任意の $h \in H$ により，

$$h(H \cap N)h^{-1} \subseteq (hHh^{-1}) \cap (hNh^{-1}) = H \cap (hNh^{-1})$$

であるが，N は G の正規部分群であるため $hNh^{-1} \subseteq N$ であり，

$$h(H \cap N)h^{-1} \subseteq H \cap N$$

となる．これは $H \cap N$ が H の正規部分群であることを示している．

次に，HN が G の部分群であり，その必要十分条件が $HN = NH$ であることを示す．H と N は G の部分群であるため

$$H = H^{-1}, \quad N = N^{-1}, \quad H = HH, \quad N = NN$$

を満たす．必要性は

$$HN = (HN)^{-1} = N^{-1}H^{-1} = NH$$

より明らかであり，十分性は $HN = NH$ を仮定することで

$$\begin{aligned}(HN)^{-1} =& N^{-1}H^{-1} = NH = HN \\ (HN)(HN) =& H(NH)N = H(HN)N = (HH)(NN) = HN\end{aligned}$$

となり，HN が G の部分群となる．以下のような写像

$$\begin{array}{ccc} H & \xrightarrow{f} & HN/N \\ \cup & & \cup \\ h & \longmapsto & hN \end{array}$$

を与えれば，f は上への準同型写像である．また，$\mathrm{Ker}\, f = H \cap N$ であるため，準同型定理より $HN/N \cong H/(H \cap N)$ である．

よって，命題は証明された．

□

定理 1.10　第 3 同型定理

群 G の正規部分群 $N, H \subseteq G$ で $N \subset H$ であるとき，$G/H \cong (G/N)/(H/N)$ である．これを群の**第 3 同型定理**という．

Proof.

準同型写像 $f : G \to G/N$ を与えたとする．H/N は G/N の正規部分群であり，これに対して $H \subseteq G$ であるため逆像で $f^{-1}(H/N) = H$ が成り立つ．これにより，第 1 同型定理より

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

が成り立つ．

よって，命題は証明された．

□

群 G で準同型写像 $f : G \to G$ が与えられれば f を G の**自己準同型**といい，f が同型写像であるならば**自己同型**という．また，自己同型は全単射であるため，その全体の集合は明らかに変換群を形成し，これを**自己同型群**といい $\mathrm{Aut}(G)$ とあらわす．

特に，任意の固定された $x \in G$ で

$$f_x : g \mapsto xgx^{-1}$$

と与えられる自己同型を**内部自己同型**といい，内部自己同型全体による集合は $\mathrm{Inn}(G)$ とあらわす．また，$f_x, f_y \in \mathrm{Inn}(G)$ で $g \in G$ に対して

$$(f_x \circ f_y)(g) = f_x(f_y(g)) = f_x(ygy^{-1}) = xygy^{-1}x^{-1} = (xy)g(xy)^{-1} = f_{xy}(g)$$

となり，逆写像は $f_x(x) = x$ となることを用いることで

$$\begin{aligned} f_x^{-1}(f_x(g)) =& f_x^{-1}(xgx^{-1}) \\ f_x^{-1}(x)f_x^{-1}(g)f_x^{-1}(x^{-1}) =& g \\ f_x^{-1}(x)f_x^{-1}(g)(f_x^{-1}(x))^{-1} =& g \\ xf_x^{-1}(g)x^{-1} =& g \\ f_x^{-1}(g) =& x^{-1}gx \\ f_x^{-1}(g) =& f_{x^{-1}}(g) \end{aligned}$$

となり，逆写像と演算が閉じているため $\mathrm{Inn}(G)$ は G に対する変換群を形成し，これを**内部自己同型群**という．

ここで，以下の定理が与えられる．

定理 1.11

群 G の内部自己同型群 $\mathrm{Inn}(G)$ は自己同型群 $\mathrm{Aut}(G)$ の正規部分群である．

Proof.

これは任意の $i \in \mathrm{Inn}(G)$ と $a \in \mathrm{Aut}(G)$ に対して

$$a \circ i \circ a^{-1} \in \mathrm{Inn}(G)$$

となることを示せばいい．任意の $g \in G$ と固定された $x \in G$ によって

$$i_x(g) = xgx^{-1}$$

であるとすれば

$$\begin{aligned} (a \circ i_x \circ a^{-1})(g) =& a(i_x(a^{-1}(g))) \\ =& a(xa^{-1}(g)x^{-1}) \\ =& a(x)(a \circ a^{-1})(g)a(x^{-1}) \\ =& a(x)g(a(x))^{-1} \\ =& i_{a(x)}(g) \end{aligned}$$

となり，$\mathrm{Inn}(G)$ は $\mathrm{Aut}(G)$ の正規部分群である．

よって，命題は証明された．

□

定理 1.12

群 G の内部自己同型群 $\mathrm{Inn}(G)$ と中心 $Z(G)$ について

$$\mathrm{Inn}(G) \cong G/Z(G)$$

が成り立つ．

Proof.

G は正規化群により $G = N_G(G)$ となるため $Z(G)$ は G の正規部分群である．$f : G \to \mathrm{Inn}(G)$ を与えれば，$x, g \in G$ と $i \in \mathrm{Inn}(G)$ によって

$$i_x(g) = xgx^{-1}$$

で $f : x \mapsto i_x$ という対応をとれば f は明らかに上への準同型写像となり，$\mathrm{Inn}(G) \cong G/Z(G)$ が得られる．

よって，命題は証明された．

□

また，群 G_1, G_2, G_3 が与えられたとき，直積群について，

$$(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$$

となることは $g_1 \in G_1, g_2 \in G_2, g_3 \in G_3$ を用いて写像 $f : ((g_1, g_2), g_3) \mapsto (g_1, (g_2, g_3))$ を与えたとき，これが明らかに同型写像になることからわかる．

1.5　生成系

まずは群の指数演算の定義を与える．

定義 1.8

群 G の任意の $g \in G$ の n 個の積を

$$g^n = \underbrace{gg\cdots g}_{n\text{ 個}}$$

とあらわす．また，$n = 0$ および n が負の整数 $-n$ とあらわされるとき G の単位元 e で，

$$\begin{aligned} g^0 &= e \\ g^{-n} &= (g^{-1})^n \end{aligned}$$

とあらわす．また，G が加法群であるならば，

$$ng = \underbrace{g + g + \cdots + g}_{n\text{ 個}}$$

のように定義される．

定理 1.13　群の指数法則

群 G の任意の $g \in G$ と $m, n \in \mathbb{Z}$ で

$$\begin{aligned} (g^m)^n &= g^{mn} \\ g^{m+n} &= g^m g^n \end{aligned}$$

が成り立つ．これを群の**指数法則**という．また，G が加法群であるならば，

$$\begin{aligned} n(mg) &= (nm)g \\ (m+n)g &= mg + ng \end{aligned}$$

とあらわされる．

Proof.

まずは第 1 式について示す．

$$(g^m)^n = (\underbrace{gg\cdots g}_{m\text{ 個}})^n = \underbrace{(\underbrace{gg\cdots g}_{m\text{ 個}})(\underbrace{gg\cdots g}_{m\text{ 個}})\cdots(\underbrace{gg\cdots g}_{m\text{ 個}})}_{n\text{ 個}} = \underbrace{gg\cdots g}_{mn\text{ 個}} = g^{mn}$$

同様にして第 2 式についても示す．

$$g^{m+n} = \underbrace{gg\cdots g}_{m+n\text{ 個}} = (\underbrace{gg\cdots g}_{m\text{ 個}})(\underbrace{gg\cdots g}_{n\text{ 個}}) = g^m g^n$$

よって，命題は証明された．

□

定義 1.9

群 G とその部分集合 S を与えたとき，S を含む G の全ての部分群の共通集合は定理 1.1 より G の部分群となる．これを S で生成される G の部分群といい，$\langle S\rangle$ とあらわす．$\langle S\rangle$ は G の S を含む最小の部分群であるとすることもでき，

$$\langle S\rangle = \{s_1^{n_1}s_2^{n_2}\cdots s_t^{n_t} \mid s_i \in S, n_1 \in \mathbb{Z}\}$$

とあらわすことができる．特に，$\langle S\rangle = G$ のとき S を G の**生成系**といい，S の元を G の**生成元**という．また，G が有限個の元からなる生成系をもつとき，G は**有限生成**であるという．

S が 1 つの元 $g \in G$ によって構成されるときは $\langle g\rangle$ とあらわすこともある．

群 G を与え，$g \in G$ の冪全体の集合は

$$\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$$

とあらわすことができ，指数法則により $\langle g\rangle$ は指数法則によって G の部分群となる．このような部分群は g によって生成される**巡回部分群**という．

加法群としての $\mathbb{Z}$ により写像 $f : \mathbb{Z} \to \langle g\rangle$ が $f : m \mapsto g^m$ とすればこれは明らかに上への準同型写像である．ある $n_g \in \mathbb{Z}$ で $n_g \geq 0$ を満たす整数の倍数全体による $\mathbb{Z}$ の部分群は $\mathrm{Ker}\, f$ に等しいものが存在し，G の単位元 e により

$$\mathrm{Ker}\, f = \left\{m \in \mathbb{Z} \,\middle|\, g^m = g^0 = e\right\} = \langle n_g\rangle$$

とあらわされ，準同型定理より

$$\langle g\rangle \cong \mathbb{Z}/\langle n_g\rangle$$

である．$\langle n_g\rangle$ は $\mathrm{Ker}\, f$ の定義より，$g^p = g^0$ を満たす 0 でない最小の $p \in \mathbb{N}$ が存在することにより，その倍数で生成される $\langle p\rangle$ に等しいことを示している．一般に $g^n = e$ となる $n \in \mathbb{N}$ が存在するとき，g は**位数有限**であるといい，このような最小の n を a の**位数**という．

また，g が位数有限であるとは

$$\exists p, q \in \mathbb{Z}(p \neq q)\ s.t.\ g^p = g^q$$
$$\exists p \in \mathbb{Z}\ s.t.\ |\langle g\rangle| = p$$

というようにあらわすこともできる．

特に，$G = \langle g\rangle$ となるとき G を**巡回群**といい，任意の巡回群は $\mathbb{Z}$ に準同型であり，巡回群が位数有限でないときは

$$\mathrm{Ker}\, f = \emptyset$$

であるため，$G \cong \mathbb{Z}$ となる．

また，有限群について以下の定理が与えられる．

定理 1.14

有限群 G の G の単位元を e としたとき，任意の元 $g \in G$ に対して

$$g^{|G|} = e.$$

Proof.

まずは $g^k = e$ を満たす $k \in \mathbb{N}$ が存在することを示す．G は有限群であるため，

$$g^a = g^b$$

のようになる $a, b \in \mathbb{N}(a < b)$ をとることが可能である．この両辺に対して g^{-1} を a 回乗ずることで，定理 1.13 を用いて

$$g^b(g^{-1})^a = e$$
$$g^{b-a} = e$$

となるため，$k = b - a$ とおけば $g^k = e$ となる k の存在が示される．

このとき，得られる k のうち最小の k で

$$H = \{g^1, g^2, \cdots, g^n\}$$

と与えられる H は巡回群かつ G の部分群である．ラグランジュの定理を用いることで

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

となるため，

$$g^{|G|} = g^{[G:H]|H|} = (g^{|H|})^{[G:H]} = e^{[G:H]} = e.$$

よって，命題は証明された．

□

この定理により，任意の有限群は巡回群となる部分群をもつ．