– 応用代数ハンドアウト –

1章 群

by K. Asai

キーワード: 群，乗法群，加群，可換群，一般線形群，有限群，位数，対称群，部分群，
特殊線形群，交代群，同型，同型写像，正規部分群，剰余類，剰余群，単純群，指数，直交群，
ユニタリ群，直積，準同型写像，準同型定理，同型定理，巡回群，中心，中心化群，正規化群，
共役類，置換の型，類等式，自己同型群，内部自己同型群，外部自己同型群

0.（演算）本書では，特に断らない限り，演算といえば2項演算を指す．x, y に演算 $*$ を行った結果は $x * y$ のように表記される．集合 G がある演算 $*$ について閉じているとは，G の元たちにその演算を行った結果がまた G に属するということ，すなわち，

$$x, y \in G \ \Rightarrow \ x * y \in G \tag{1}$$

がなりたつことと定義する．たとえば整数全体の集合 $\mathbf{Z}$ は，加法，減法，乗法については閉じているが，除法については閉じていない．数学では種々の演算について閉じている集合を考え，その性質を研究することがよく行われる．

1.（群の定義）集合 G が，ある演算 $*$ について閉じていて，以下の公理をみたすとき，G を $*$ に関する **群** という．

$[G1]$	（結合律）	任意の $x, y, z \in G$ に対して，$(x * y) * z = x * (y * z)$.
$[G2]$	（単位元の存在）	ある $e \in G$ が存在し，任意の $x \in G$ に対して $x * e = e * x = x$ をみたす．この e を G の単位元という．
$[G3]$	（逆元の存在）	各 $x \in G$ に対して，$x * x^{-1} = x^{-1} * x = e$ をみたす元 $x^{-1} \in G$ が存在する．これを x の逆元という．

(ex1) 群は空集合ではないのはなぜか？

(ex2) (1) 群 G の単位元はただ1つであることを示せ． (2) $G = \{e\}$（すなわち G は単位元のみからなる）は群になることを示せ．この群を単位群という．

(ex3) (1) 各元 $x \in G$ に対して，その逆元はただ1つであることを示せ．

(2) $(x^{-1})^{-1} = x$ を示せ． (3) $(x * y)^{-1} = y^{-1} * x^{-1}$ を示せ．

(note) (1) 演算 $*$ に関する群を，$*$ を明示して，$(G, *)$ とかくこともある． (2) 群では結合律がみたされるので，演算の繰り返し $x_1 * x_2 * \cdots * x_n$ は括弧の付け方によらない．

（すなわち，括弧をどのように付けても相等しい.）（離散系論ハンドアウト 0 章参照）したがってこのような式では括弧は省略されることが多い.

G の演算 $*$ は乗法 $(\cdot)$ かまたは加法 $(+)$ であることが多い[1]．前者のとき，G は 乗法群 ，後者のとき，G は 加群 と呼ばれる．乗法群では演算の記号 $\cdot$ は省略されることが多い.

G が上の 3 つの公理 $[G1], [G2], [G3]$ の他に次をみたすとき，G は アーベル群 または 可換群 ，あるいは 可換である という.

$[G0]$ （交換律）　　任意の $x, y \in G$ に対して，$x * y = y * x$.

加群はつねに交換律をみたす ものとされる．加群においては，単位元を 0 で表して 0 元といい，また x の逆元を $-x$ で表して x の 反元 という．通常 $x + (-y) = x - y$ と略記する.

(note) 群の特定の元 a, b が $a * b = b * a$ をみたすとき，a と b は可換であるという.

(ex4) (1) $\mathbf{Z}$，$\mathbf{Q}$，$\mathbf{R}$，$\mathbf{C}$ でそれぞれ整数全体の集合，有理数全体の集合，実数全体の集合，複素数全体の集合を表す．これらはすべて加群になることを示せ.

(2) $\mathbf{Q}$，$\mathbf{R}$，$\mathbf{C}$ の記号の右肩に $^\times$ を付けることで，0 を除いた集合を表す．このとき，$\mathbf{Q}^\times$，$\mathbf{R}^\times$，$\mathbf{C}^\times$ はすべて可換な乗法群になることを示せ.

(ex5) 空間ベクトル全体の集合 V^3 に外積 $\times$ を定義できる．V^3 は $\times$ に関して群になるか？（線形代数ハンドアウト 3 章参照）

2.（群の例）成分が整数の n 項ベクトル全体の集合:

$$\mathbf{Z}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, \ldots, x_n \in \mathbf{Z} \right\} \tag{2}$$

は加法に関して群をなす，すなわち加群である．その 0 元は 0 ベクトルで，$\mathtt{x}$ の反元は $-\mathtt{x}$ である．このことは，成分が有理数や実数，複素数であっても同様である.

$K = \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ とする．ある固定された m, n に対して，K の元を成分とする (m, n) 型行列全体の集合 $M_{m,n}(K)$ は加群である．その 0 元は 0 行列 $O_{m,n}$ であり，A の反元は $-A$ である.

$K = \mathbf{Q}, \mathbf{R}, \mathbf{C}$ とする．固定された n に対して，K の元を成分とする，正則な n 次行列全体の集合を $GL(n, K)$ で表す．これは乗法群となり，一般線形群 と呼ばれる．$n \geq 2$ のとき，この群は可換ではない.

(ex6) (1) $GL(n, K)$ が乗法群になることを示せ．(2) $GL(n, K)$ は加法に関しては群をなさないことを示せ.

[1]乗法，加法に関する群（あるいは，それらについて閉じていること）を，それぞれ，積，和に関する群（あるいは，それらについて閉じている）ともいうことにする.

($\because$) (1) $GL(n,K)=G$ とおく．$X,Y\in G$ とすると，XY は n 次行列で，その成分は X,Y の成分の多項式，すなわち K の元になる．さらに正則な行列の積はまた正則になるので，XY は正則である．ゆえに G は積について閉じている．行列の演算法則より，G は結合律をみたす．n 次単位行列 $E_n\in G$ が存在し，任意の $X\in G$ に対して，

$$XE_n=E_nX=X \tag{3}$$

をみたすので，E_n は G の単位元である．最後に $X\in G$ に対して，X の逆行列 $X^{-1}=|X|^{-1}\tilde{X}$ ($\tilde{X}$ は X の余因子行列) は X の逆元であることを言う．まず

$$XX^{-1}=X^{-1}X=E_n \tag{4}$$

をみたす．次に $X^{-1}\in G$ を確認しておく．$(X^{-1})^{-1}=X$ なので，X^{-1} は正則な n 次行列である．また X^{-1} の成分は X の成分の有理式になるので，K の元となる． $\therefore X^{-1}\in G$． (q.e.d.)

有限個の元からなる群を 有限群 という．有限群 G の元の数を G の 位数 といい，$|G|$ で表す．有限群でない群を，無限群という．無限群 G の位数 $|G|$ は，厳密には G の集合としての濃度と考えるべきだが，ここでは簡潔に，G の位数は無限とし，$|G|=\infty$ とかくことにする．

n を固定するとき，n 文字の置換の集合 S_n は置換の積に関して群をなす．これを n 次対称群という．この群は有限群であり，$|S_n|=n!$ である．S_n の単位元は恒等置換 e であり，σ の逆元は σ の逆置換 σ^{-1} である．$n\geq 3$ のとき S_n は可換ではない.（線形代数ハンドアウト 7 章参照）

(ex7) S_3 の乗法表をかけ.（乗法表とは積の結果をかいた表である） ただし，

$$S_3=\{e,(1,2),(1,3),(2,3),\sigma,\tau\};\quad \sigma=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\tau=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}. \tag{5}$$

3.（部分群）G を群とする．G の部分集合 H が G と同じ演算に関して群であるとき，H を G の 部分群 という．G 自身や $\{e\}$ は必ず G の部分群になる．これらは自明な部分群と呼ばれる．G の部分群の部分群は，G の部分群である．G の部分群 H は G と共通の単位元を持つ.（(T1) の証明参照）

(T1) G を $*$ に関する群とする．H が G の部分群となるためには，H が G の空でない部分集合であって，$*$ および，逆元を求める演算 $x\longmapsto x^{-1}$ について閉じていることが必要十分である．

($\because$) H を G の部分群とする．H はもちろん G の空でない部分集合である．部分群 H が $*$ について閉じていることは明らか．H の単位元が G の単位元 e に等しいことを見ておく．H の単位元を a とすると，$a*a=a$ であり，この両辺に G における a の逆元 a^{-1} を掛けて，左辺 $=(a*a)*a^{-1}=a*(a*a^{-1})=a*e=a$．右辺 $=a*a^{-1}=e$． $\therefore a=e$．ゆえに，H の各元の逆元は G における逆元と同じになり，H は演算 $x\longmapsto x^{-1}$ について閉じていることがわかる．

逆に，H が G の空でない部分集合であって，$*$ および演算 $x \longmapsto x^{-1}$ について閉じているとする．

(i) G において結合律がなりたつので，その部分集合 H においても結合律がなりたつ．

(ii) H の任意の元 x を取れば，$x^{-1} \in H$ である．

(iii) (ii) より $x * x^{-1} = e \in H$ となる．

ゆえに，H は G の部分群である． (q.e.d.)

(T1) を言い換えた定理として次がある．これは実用上有用である．

(T1') H が G の部分群となるための必要十分条件は，$H \subset G$，$H \neq \emptyset$ であって，
$x, y \in H \Rightarrow x * y^{-1} \in H$ をみたすことである．

(note) $H \subset G$，$H \neq \emptyset$ の条件は明らかならば省略してよい．

(ex8) $\mathbf{Z}$ は $\mathbf{Q}$ の部分加群である．$\mathbf{Q}$ は $\mathbf{R}$ の部分加群である．$\mathbf{R}$ は $\mathbf{C}$ の部分加群である．

(ex9) $\mathbf{Q}^\times$ は $\mathbf{R}^\times$ の部分群である．$\mathbf{R}^\times$ は $\mathbf{C}^\times$ の部分群である．

(ex10) n 文字の置換のうちの，偶置換全体からなる集合を A_n とかく．これは S_n の部分群であり，n 次交代群と呼ばれる．ここで，符号が 1 の置換を偶置換，符号が -1 の置換を奇置換という．一般に，n 次対称群の部分群を n 次置換群という．

($\because$) （A_n が S_n の部分群であること）(T1') を用いる．$\sigma, \tau \in A_n$ とする．$\mathrm{sgn}(\sigma\tau^{-1}) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau^{-1}) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau) = 1 \cdot 1 = 1$． $\therefore$ $\sigma\tau^{-1} \in A_n$． (q.e.d.)

(note) $S_1 = A_1$ である以外は，$|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$ である．

(ex11) A_2, A_3, A_4 を求めよ．

(ex12) $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}$ とする．固定された n に対して，K の元を成分とし，行列式が 1 に等しい n 次行列全体の集合を $SL(n, K)$ で表す．これは $GL(n, K)$ の部分群になり，

特殊線形群

と呼ばれる．

($\because$) （$SL(n, K)$ が $GL(n, K)$ の部分群であること）(T1') を用いる．$SL(n, K)$ の各元は正則なので，$SL(n, K) \subset GL(n, K)$．次に $X, Y \in SL(n, K)$ とする．$GL(n, K)$ は群なので $XY^{-1} \in GL(n, K)$ は確かであり，$|XY^{-1}| = |X||Y^{-1}| = |X||Y|^{-1} = 1 \cdot 1^{-1} = 1$．
$\therefore$ $XY^{-1} \in SL(n, K)$． (q.e.d.)

(T2) G の部分群 H，H' に対して，$H \cap H'$ はまた G の部分群である．

($\because$) (T1') を用いる．$x, y \in H \cap H'$ を取る．$x, y \in H$ であり，H は部分群なので，$x * y^{-1} \in H$．同様に，$x, y \in H'$ であり，H' は部分群なので，$x * y^{-1} \in H'$．ゆえに，$x * y^{-1} \in H \cap H'$． (q.e.d.)

3 つ以上の部分群についても (T2) と同様のことがなりたつ．あるいは無限個の部分群についても次のように一般化される．

(T2') G の部分群 H_λ $(\lambda \in \Lambda)$ に対して，$\bigcap_{\lambda \in \Lambda} H_\lambda$ はまた G の部分群である．

4.（同型）G, G' を 2 つの群とする．G から G' への写像 ϕ を

$$\phi : G \longrightarrow G' \tag{6}$$

で表す．ここに，G を ϕ の定義域（始域），G' を ϕ の終域という．また，

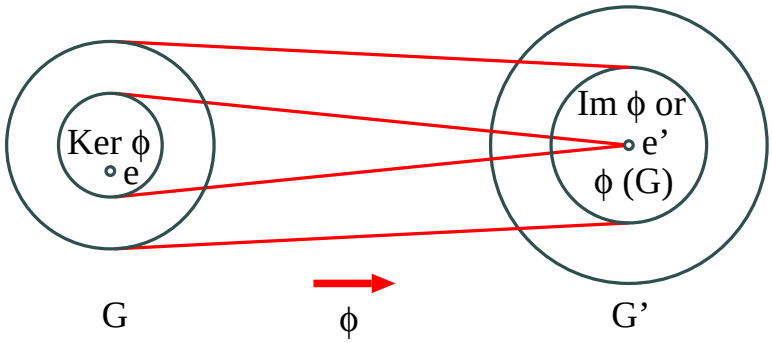
$$\mathrm{Im}\,\phi = \{\phi(x) \mid x \in G\} \tag{7}$$

を ϕ の像という．これは $\phi(G)$ ともかかれる．さらに，

$$\mathrm{Ker}\,\phi = \{x \in G \mid \phi(x) = e'\} \tag{8}$$

を ϕ の核という．ただし，e' は G' の単位元である．これは，$\phi^{-1}(e')$ ともかかれる．

写像 $\phi : G \longrightarrow G'$ に対して，$\mathrm{Im}\,\phi = G'$ のとき，すなわち任意の $x' \in G'$ に対してある $x \in G$ が存在して $\phi(x) = x'$ となるとき，ϕ を全射という．また，$x, y \in G$ のとき，$x \neq y \Rightarrow \phi(x) \neq \phi(y)$ をみたすとき，(あるいは，$\phi(x) = \phi(y) \Rightarrow x = y$ をみたすとき）ϕ を単射という．ϕ が全射かつ単射のとき，ϕ を全単射または 1 対 1 対応という．写像 $\phi : G \longrightarrow G$ が $\phi(x) = x$ $(x \in G)$ をみたすとき，ϕ を恒等写像と呼び，id_G，id，1_G，1 などで表す．これは 1 対 1 対応の最も簡単な例である．



G, G', G'', G''' を群とする．2 つの写像 $\phi : G \longrightarrow G'$，$\psi : G' \longrightarrow G''$ に対して合成 $\psi \circ \phi : G \longrightarrow G''$ を

$$\psi \circ \phi(x) = \psi(\phi(x)) \qquad (x \in G) \tag{9}$$

で定義する．さらに写像 $\omega : G'' \longrightarrow G'''$ があるとき，合成については次の結合律がなりたつ．

$$(\omega \circ \psi) \circ \phi = \omega \circ (\psi \circ \phi) \tag{10}$$

これにより，幾らかの写像の合成は括弧の付け方によらないので，括弧は省略できる．

写像 $\phi : G \longrightarrow G'$ に対し，次をみたすような写像 $\psi : G' \longrightarrow G$ を ϕ の逆写像といい，$\psi = \phi^{-1}$ で表す．

$$\begin{array}{lll} \psi \circ \phi = \mathrm{id} & (\psi \circ \phi(x) = x & (x \in G)) \\ \phi \circ \psi = \mathrm{id} & (\phi \circ \psi(x') = x' & (x' \in G')) \end{array} \tag{11}$$

このとき，ϕ もまた ψ の逆写像になっており，$(\phi^{-1})^{-1} = \phi$ がなりたつ．また，ϕ の逆写像は存在するとしてもただ 1 つである．次がなりたつ．

$$\phi \text{ が 1 対 1 対応} \iff \phi \text{ の逆写像が存在する} \tag{12}$$

(ex13) (1) 1 対 1 対応の合成はまた 1 対 1 対応になることを示せ．(2) $\phi : G \longrightarrow G'$ および $\psi : G' \longrightarrow G''$ が 1 対 1 対応のとき，$(\psi \circ \phi)^{-1} = \phi^{-1} \circ \psi^{-1}$ を示せ．(3) (12) を示せ．

2 つの群 $G = (G, *)$，$G' = (G', \star)$ に対して，G から G' への 1 対 1 対応 ϕ が存在して次をみたすとき，G と G' は 同型 であるといい，$G \simeq G'$ とかく．

$$\phi(x * y) = \phi(x) \star \phi(y) \qquad (x, y \in G) \tag{13}$$

この ϕ を G から G' への（G と G' の間の）同型写像 という．同型とは，群として全く同じ構造を持つことに他ならない．

(13) において，$x * y$ は G における演算であり，$\phi(x) \star \phi(y)$ は G' における演算であることに注意する．ϕ が 1 対 1 対応であることを仮定せず，単に (13) がなりたつとき，ϕ は準同型写像である，ϕ は演算を保存する（演算と両立する，演算と可換である）などという．

(note) (1) 2 つの群の間に同型写像が複数個存在することもある．(2) 同型写像を単に同型ともいう．

(ex14) 同型写像 ϕ に対して次を示せ．(1) $\phi(e) = e'$．(e' は G' の単位元) (2) $\phi(x^{-1}) = (\phi(x))^{-1}$．

(ex15) G から G' への同型写像 ϕ の逆写像 ϕ^{-1} は，G' から G への同型写像になることを示せ．

($\because$) ϕ は 1 対 1 対応なので，その逆写像 ϕ^{-1} が存在して 1 対 1 対応になる．また任意の $x', y' \in G'$ に対して，$x, y \in G$ が存在して $\phi(x) = x'$，$\phi(y) = y'$ となる．そこで (13) より，

$$\begin{aligned} \phi^{-1}(x' \star y') &= \phi^{-1}(\phi(x) \star \phi(y)) = \phi^{-1}(\phi(x * y)) \\ &= x * y = \phi^{-1}(x') * \phi^{-1}(y'). \qquad \text{(q.e.d.)} \end{aligned} \tag{14}$$

(note) 任意の群 G に対して明らかに $G \simeq G$ であり，また (ex15) より，$G \simeq G' \Rightarrow G' \simeq G$ がなりたつ．さらに，同型写像 $\phi : G \longrightarrow G'$，$\psi : G' \longrightarrow G''$ の合成 $\psi \circ \phi : G \longrightarrow G''$ はまた同型写像なので，$G \simeq G'$，$G' \simeq G'' \Rightarrow G \simeq G''$ がなりたつ．((T10–10') 参照)

(ex16) (1) K^+ で，K の正の元全体からなる集合を表す．$\mathbf{R}^+$ は乗法群である．$\mathbf{R}$ を加群と見るとき，$\mathbf{R} \simeq \mathbf{R}^+$ である．$\phi(x) = e^x$ が，$\mathbf{R}$ から $\mathbf{R}^+$ への同型写像を与える．実際，

$$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y) \qquad (x, y \in \mathbf{R}) \tag{15}$$

であり，またグラフより ϕ が 1 対 1 対応であることが確認できる．

(2) $\phi^{-1}(x) = \psi(x) = \log x$ は，$\mathbf{R}^+$ から $\mathbf{R}$ への同型写像になることを示せ．

5.（正規部分群，剰余類，剰余群）簡単のため，特に断らない限り，これ以後の節では群は乗法群として議論する．G を群，H をその部分群とする．G の元 g に対して，G の部分集合 gH を次で定める．

$$gH = \{gh \mid h \in H\} \tag{16}$$

これを H に関する（H を法とする）g の 左剰余類 という．g を明示しないときは，H に関する G の左剰余類ともいう．同様にして，

$$Hg = \{hg \mid h \in H\} \tag{17}$$

を H に関する（H を法とする）g の（G の）右剰余類 という．$g \in H$ ならば，$gH = Hg = H$ である．また，$g \in gH$，$g \in Hg$ である．剰余類には他に次のような性質がある．

.....

(T3) H を G の部分群，$g, g' \in G$ とするとき，

$$\begin{aligned} gH \cap g'H \neq \emptyset &\iff gH = g'H \iff g' \in gH, \\ Hg \cap Hg' \neq \emptyset &\iff Hg = Hg' \iff g' \in Hg. \end{aligned} \tag{18}$$

.....

($\because$) 同様なので，第 1 式を考える．まず左の $\iff$ を示す．

($\Rightarrow$) $gH \cap g'H \neq \emptyset$ とする．$k \in (gH \cap g'H)$ を取ると，$k = gh = g'h'$ $(h, h' \in H)$ とかける．$\therefore\ g = g'h'h^{-1}$．ゆえに，$gH$ の任意の元 gh_1 に対して，$gh_1 = g'h'h^{-1}h_1 = g'h_2 \in g'H$．したがって $gH \subset g'H$．同様にして，$gH \supset g'H$．それゆえ $gH = g'H$． (q.e.d.)

($\Leftarrow$) $g \in gH \neq \emptyset$ なので明らか． (q.e.d.)

($\because$) 次に第 1 式右の $\iff$ を示す．

($\Rightarrow$) $gH = g'H$ とすると，$g' \in g'H$ なので $g' \in gH$ を得る． (q.e.d.)

($\Leftarrow$) $g' \in gH$ とする．$g' \in g'H$ なので，$gH \cap g'H \neq \emptyset$ となる．ゆえに左の $\iff$ より，$gH = g'H$ を得る． (q.e.d.)

(ex17) (18) の第 2 式を示せ．

(T3) によれば，剰余類は少しでも重なれば一致してしまうことがわかる．そしていかなる元 $g \in G$ も，gH，Hg という剰余類に属している．そこで，左剰余類の集合[2]

$$G/H = \{gH \mid g \in G\} \tag{19}$$

を作れば，これは G の，互いに共通部分を持たない部分集合への分割になる．したがってまた，

$$G = \bigcup_{g \in G} gH \tag{20}$$

を得る．これを G の 左剰余類分解 という．同様に，右剰余類の集合

$$H\backslash G = \{Hg \mid g \in G\} \tag{21}$$

[2](19) において，$g \in G$ が動いても gH が同じ剰余類を重複して指していることは十分ありうる．剰余類の集合を作るとき，集合の定義より，重複した剰余類は 1 つの剰余類とみなす．(21) も同様．

もまた G のもう 1 つの分割を与え，したがって，G の 右剰余類分解

$$G = \bigcup_{g \in G} Hg \tag{22}$$

を得る．ここで，H が次の条件をみたすとする．

$$gH = Hg \qquad (g \in G) \tag{23}$$

このとき，H は G の 正規部分群 であるといい，記号で $H \triangleleft G$ または $G \triangleright H$ と表す．$H \triangleleft G$ ならば，(19) と (21) は全く同じ分割を表すことになるので[3]，その分割をあらためて G/H とかくことにする．このとき，G/H は左右の区別のない 剰余類 からなる．すなわち，

$$G/H = \{gH \mid g \in G\} = \{Hg \mid g \in G\}. \tag{24}$$

ここで，

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\} \tag{25}$$

と定義するとき，次がなりたつ．

(T4) 群 G の部分群 H に対して，以下の 4 つの命題は同値である．

$$\begin{array}{ll} \text{(i) } gH = Hg \quad (g \in G). & \text{(ii) } gHg^{-1} = H \quad (g \in G). \\ \text{(iii) } gHg^{-1} \subset H \quad (g \in G). & \text{(iv) } g \in G,\, h \in H \Rightarrow ghg^{-1} \in H. \end{array} \tag{26}$$

($\because$) (i) $\Longleftrightarrow$ (ii): 簡単なので略．

(ii) $\Longleftrightarrow$ (iii): $\Rightarrow$ は明らか．

($\Leftarrow$) (iii) がなりたつとする．任意の $g \in G$ を取るとき，$gHg^{-1} \subset H$．g の代わりに g^{-1} を代入してもなりたつので，$g^{-1}Hg \subset H$．　$\therefore\ H \subset gHg^{-1}$．　$\therefore\ gHg^{-1} = H$．

(iii) $\Longleftrightarrow$ (iv): $gHg^{-1} \subset H$ を言い替えると，$h \in H \Rightarrow ghg^{-1} \in H$ であることから明らか．(q.e.d.)

(note) (26) (i) – (iv) はすべて同値なので，これらのどれでも 1 つを $H \triangleleft G$ の定義としてよい．もちろん H が G の部分群であることは前提とする．

(ex18) (1) (26)(i) $\Longleftrightarrow$ (26)(ii) を示せ． (2) G，$\{e\}$ は G の正規部分群であることを示せ．(これらを自明な正規部分群ともいう) (3) 正規部分群の交わりはまた正規部分群になることを示せ． (4) $G = S_3, S_4$ のとき，G の適当な部分群 H に対して，G/H，$H\backslash G$ を求めよ． (5) 可換群の部分群は正規部分群であることを示せ．

($\because$) (3) $H_1, H_2 \triangleleft G$ とする．$H_1 \cap H_2 = N$ とおく．(T2) より，N は G の部分群である．次に，任意の $g \in G$ に対して $gNg^{-1} \subset N$ を示す．$N \subset H_1$，$H_1 \triangleleft G$ だから，$gNg^{-1} \subset gH_1g^{-1} = H_1$．同様に，$N \subset H_2$，$H_2 \triangleleft G$ だから，$gNg^{-1} \subset gH_2g^{-1} = H_2$．$\therefore\ gNg^{-1} \subset H_1 \cap H_2 = N$．　$\therefore\ N \triangleleft G$．(q.e.d.)

[3]同様に，(20) と (22) は全く同じ分解を表す．

(note) $G \triangleright H$，$H \triangleright N$ であっても，$G \triangleright N$ とは限らない．たとえば，S_4 の部分集合:

$$V_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \tag{27}$$

は S_4 の正規部分群をなす.（これ (と同型な群) を Klein の 4 元群という.） さらにその部分群 $N = \{e, (1,2)(3,4)\}$ を取ると，$S_4 \triangleright V_4 \triangleright N$ であるが，$S_4 \not\triangleright N$ である．

一般に，G の部分集合 A, B が与えられたときに，これらの積 AB を次で定める．

$$AB = \{ab \mid a \in A,\, b \in B\} \tag{28}$$

これはまた G の部分集合となっている．このとき，

$$(AB)C = A(BC) \qquad \text{（結合律）} \tag{29}$$

がなりたつ．一応確認すると，

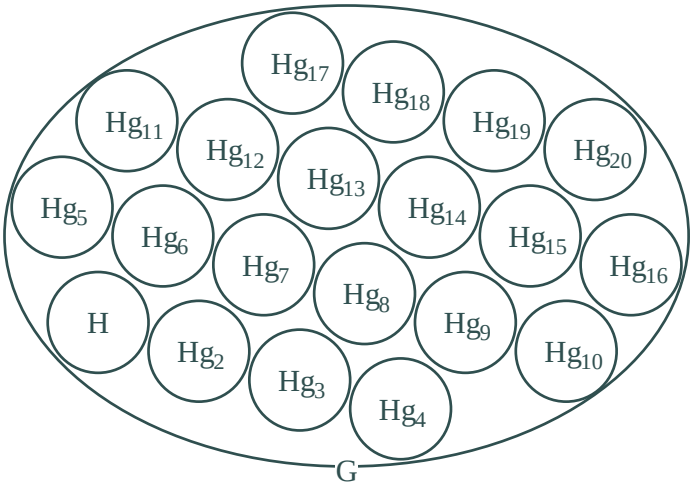
$$\begin{aligned} (AB)C &= \{xc \mid x \in AB,\, c \in C\} = \{(ab)c \mid a \in A,\, b \in B,\, c \in C\} \\ &= \{a(bc) \mid a \in A,\, b \in B,\, c \in C\} = \{ay \mid a \in A,\, y \in BC\} \\ &= A(BC). \end{aligned} \tag{30}$$

したがって，幾らかの部分集合の積 $A_1 A_2 \ldots A_s$ は括弧の付け方によらないので，括弧は省略できることがわかる．さて，$gH = \{g\}H$ のように考えれば，gH，Hg や gHg^{-1} などの定義は (28) による積の定義と一致する．したがって，幾らかの元や部分群が混ざった積も括弧の付け方によらないことになる．

ここで，$H \triangleleft G$ のとき，G/H に属する剰余類たちの間で積を考えるとどうなるか見てみよう．

$$(Hg)(Hg') = H(gH)g' = H(Hg)g' = (HH)(gg') = H(gg') \tag{31}$$

右辺 $H(gg')$ は gg' の剰余類なので，当然 G/H に属する．これで，G/H に対して積の演算が定義できた．



G/H

(T5) G を群，H を正規部分群とするとき，G/H は積に関して群をなす．特に G が可換群のとき，G/H は可換群になる．

($\because$) G/H が積について閉じていることは上で見た通りである．この演算が結合律をみたすことも (29) で見た．次に，$H \in G/H$ を取ると，

$$\begin{array}{l}(Hg)H = (Hg)(He) = H(ge) = Hg \\ H(Hg) = (He)(Hg) = H(eg) = Hg\end{array} \qquad (Hg \in G/H) \tag{32}$$

なので，H は G/H の単位元である．また，任意の $Hg \in G/H$ に対して，

$$\begin{array}{l}(Hg)(Hg^{-1}) = H(gg^{-1}) = He = H \\ (Hg^{-1})(Hg) = H(g^{-1}g) = He = H\end{array} \tag{33}$$

より，逆元 $(Hg)^{-1} = Hg^{-1} \in G/H$ が存在する．したがって G/H は群である．

次に G を可換群とする．任意の 2 元 $Hg, Hg' \in G/H$ に対して，

$$(Hg)(Hg') = H(gg') = H(g'g) = (Hg')(Hg) \tag{34}$$

となるので，G/H は可換群である． (q.e.d.)

G/H を G の H による 剰余群，あるいは H を法とする G の剰余群という．

G が自明でない正規部分群（すなわち，G，$\{e\}$ 以外の正規部分群）を持たないとき，G を 単純群 という．

(note) 一般に G の演算が $+$ や $*$ の場合でも，乗法群の場合と同様に剰余群が定義され，G/H で表される．加群では，左右の剰余類をそれぞれ $g + H$，$H + g$ とかくが，それらはつねに一致する．加群の剰余群 G/H では，演算は加法になるので，

$$(H + g) + (H + g') = H + (g + g') \tag{35}$$

のように計算する．

加群以外では，剰余類などは，(演算が乗法でなくても）gH，Hg，gHg^{-1} などとかくのが普通であり，剰余群においては，演算が $*$ ならば，

$$Hg * Hg' = H(g * g') \tag{36}$$

のような表記になる．

(ex19) 剰余群 G/H において，$(Hg_1)(Hg_2)\ldots(Hg_n) = H(g_1g_2\ldots g_n)$ がなりたつことを示せ．

(ex20) (1) $G/\{e\} \simeq G$ を示せ． (2) $G/G \simeq \{e\}$ を示せ．

(ex21) (1) 加群 $\mathbf{C}$ とその正規部分群 $\mathbf{R}$ に対して，$\mathbf{C}/\mathbf{R} \simeq \mathbf{R}$ を示せ．

($\because$) $\mathbf{C} = \{x + yi \mid x, y \in \mathbf{R}\}$ なので，

$$\mathbf{C}/\mathbf{R} = \{\mathbf{R} + yi \mid y \in \mathbf{R}\} \tag{37}$$

となる．ここで，

$$\begin{array}{rccc} \phi: & \mathbf{C}/\mathbf{R} & \longrightarrow & \mathbf{R} \\ & \mathbf{R}+yi & \longmapsto & y \end{array} \tag{38}$$

のように ϕ を定義すると，ϕ は $\mathbf{C}/\mathbf{R}$ から $\mathbf{R}$ への同型写像になる（示せ）ので，$\mathbf{C}/\mathbf{R} \simeq \mathbf{R}$. (q.e.d.)

(ex21) (2) 乗法群 $\mathbf{C}^\times$ とその正規部分群 $\mathbf{R}^+$ を取る．$\mathbf{C}$ 内の単位円 S^1 を次のように定める．

$$S^1 = \{z \in \mathbf{C} \mid |z| = 1\} \tag{39}$$

これは乗法群である．このとき，$\mathbf{C}^\times/\mathbf{R}^+ \simeq S^1$ を示せ．

($\because$) $\mathbf{C}^\times = \{re^{i\theta} \mid r \in \mathbf{R}^+, 0 \le \theta < 2\pi\}$ とかけるので，

$$\mathbf{C}^\times/\mathbf{R}^+ = \{\mathbf{R}^+ e^{i\theta} \mid 0 \le \theta < 2\pi\}. \tag{40}$$

そこで，

$$\begin{array}{rccc} \phi: & \mathbf{C}^\times/\mathbf{R}^+ & \longrightarrow & S^1 \\ & \mathbf{R}^+ e^{i\theta} & \longmapsto & e^{i\theta} \end{array} \tag{41}$$

のように ϕ を定義すると，ϕ は $\mathbf{C}^\times/\mathbf{R}^+$ から S^1 への同型写像になる（示せ）ので，$\mathbf{C}^\times/\mathbf{R}^+ \simeq S^1$. (q.e.d.)

6.（部分群の指数）G を群，H をその部分群とする．左剰余類の集合 G/H (19) および右剰余類の集合 $H\backslash G$ (21) を考える．G から G への 1 対 1 対応 $\phi(x) = x^{-1}$ により，左剰余類 gH は右剰余類 Hg^{-1} に移される[4]．なぜならば，gH の任意の元 gh に対して，$(gh)^{-1} = h^{-1}g^{-1} \in Hg^{-1}$ であり，Hg^{-1} の任意の元 hg^{-1} に対して，$gh^{-1} \in gH$ が存在して，$(gh^{-1})^{-1} = hg^{-1}$ となるからである．この写像 ϕ により，G/H から $H\backslash G$ への 1 対 1 対応が得られる．したがって，左または右の剰余類の個数が有限ならば，左剰余類の個数は右剰余類の個数に等しくなる．この数を H の（G に対する）**指数** といい，$(G:H)$ で表す．H が有限の指数を持たないときは，H の指数は無限であるといい，$(G:H) = \infty$ とかく．

特に G を有限群とし，H をその部分群とすると，任意の左右の剰余類 gH，Hg に対して，$|H| = |gH| = |Hg|$ がなりたつ．そこで，G の左剰余類分解

$$G = g_1H \cup g_2H \cup \cdots \cup g_sH \tag{42}$$

を考えると，$(G:H) = s = |G|/|H|$ となる．このことは，右剰余類分解

$$G = Hg_1' \cup Hg_2' \cup \ldots \cup Hg_s' \tag{43}$$

を用いても導かれる．これより，次を得る．

.....

(T6) 有限群 G の任意の部分群の位数は，G の位数の約数である．(Lagrange の定理) 特に，H が G の正規部分群ならば，$|G/H| = |G|/|H| = (G:H)$ がなりたつ．

.....

[4] $\phi(gH) = \{\phi(x) \mid x \in gH\} = Hg^{-1}$ を意味する．([8.] 参照)

(ex22) G を群とする．G から G への写像 $\phi(x) = x^{-1}$ は 1 対 1 対応であることを示せ．

(ex23) (1) 素数位数の群は自明な部分群しか持たないことを示せ． (2) 素数位数の群は単純群であることを示せ．

(ex24) $(S_n : A_n)$ を求めよ．

(ex25) 群 G の部分群 H の指数が 2 のとき，H は G の正規部分群となることを示せ．

($\because$) H の指数が 2 なので，G の左剰余類分解は $G = H \cup g_1 H$ となる．したがって，$g_1 H = G - H$ となる．ここで，$g \in H$ ならば $gH = H$ であり，$g \notin H$ ならば $gH \neq H$ なので，$gH = g_1 H = G - H$ となる．同様にして，$g \in H$ ならば $Hg = H$ であり，$g \notin H$ ならば $Hg = G - H$ が言える．こうして，任意の g に対して，$gH = Hg$ となる． (q.e.d.)

(ex26) A_n は S_n の正規部分群であることを示せ．

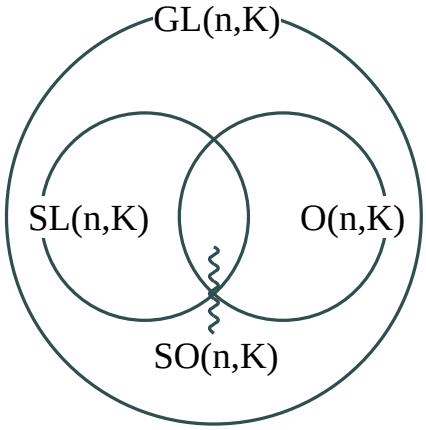
($\because$) A_n が S_n の部分群であることは (ex10) ですでに示した．次に，$\sigma \in S_n$，$\tau \in A_n$ とすると，$\mathrm{sgn}(\tau) = 1$ なので，$\mathrm{sgn}(\sigma\tau\sigma^{-1}) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma) = 1$．
$\therefore\ \sigma\tau\sigma^{-1} \in A_n$． $\therefore\ A_n \triangleleft S_n$． (q.e.d.)

($\because$) （別証） $(S_n : A_n)$ を既知として示す．$n = 1$ のとき，$S_1 = A_1$ なので $A_1 \triangleleft S_1$．
$n \geq 2$ のとき，$(S_n : A_n) = 2$ なので (ex25) より $A_n \triangleleft S_n$． (q.e.d.)

(ex27) $SL(n, K)$ は $GL(n, K)$ の正規部分群であることを示せ．

($\because$) $SL(n, K) = S$，$GL(n, K) = G$ とおく．S が G の部分群であることは (ex12) ですでに示した．次に，$X \in G$，$Y \in S$ とすると，$|XYX^{-1}| = |X||Y||X^{-1}| = |X| \cdot 1 \cdot |X|^{-1} = 1$．
$\therefore\ XYX^{-1} \in S$． $\therefore\ S \triangleleft G$． (q.e.d.)

$K = \mathbf{Q}, \mathbf{R}, \mathbf{C}$ とする．$T^t T = {}^t T T = E_n$（すなわち $T^{-1} = {}^t T$）をみたす n 次行列 T を n 次直交行列という．K の元を成分とする n 次直交行列全体の集合を $O(n, K)$ で表す．これは $GL(n, K)$ の部分群になり，直交群 と呼ばれる．$K = \mathbf{R}$ のときは，この群は $\mathbf{R}^n$ のベクトルの長さを変えない線形変換全体のなす群である．一般に，$O(n, K)$ の元は行列式が ± 1 の値を持つが，このうち行列式が 1 であるもの全体からなる集合を $SO(n, K)$ とかき，特殊直交群 と呼ぶ．$SO(n, K) = O(n, K) \cap SL(n, K)$ がなりたつ．$SO(n, K)$ は $O(n, K)$ の正規部分群であり，$(O(n, K) : SO(n, K)) = 2$ である．



(ex28) $T \in O(n, \mathbf{R})$ を取る．任意の $\mathtt{x} \in \mathbf{R}^n$ に対して，$||\mathtt{x}|| = ||T\mathtt{x}||$ を示せ．

(ex29) (1) $O(n, K)$ が $GL(n, K)$ の部分群であることを示せ． (2) $SO(n, K)$ が $O(n, K)$ の正規部分群であることを示せ．

($\because$) (1) (T1') を用いる．$O(n, K)$ の各元は正則なので，$O(n, K) \subset GL(n, K)$．次に $X, Y \in O(n, K)$ とする．明らかに XY^{-1} の成分は K の元であり，

$$\left(XY^{-1}\right)^{-1} = YX^{-1} = {}^t\left({}^tY\right){}^tX = {}^t\left(Y^{-1}\right){}^tX = {}^t\left(XY^{-1}\right) \tag{44}$$

$\therefore\ XY^{-1} \in O(n, K)$． (q.e.d.)

($\because$) (2) $O(n, K) = H$，$SO(n, K) = S$ とおく．$X, Y \in S$ とする．H 自体が群なので，$XY^{-1} \in H$ であり，

$$|XY^{-1}| = |X||Y^{-1}| = |X||Y|^{-1} = 1 \cdot 1^{-1} = 1. \tag{45}$$

$\therefore\ XY^{-1} \in S$．(T1') より，$S$ は H の部分群である．次に，$X \in H$，$Y \in S$ とすると，$|XYX^{-1}| = |X||Y||X^{-1}| = |X||Y||X|^{-1} = |X| \cdot 1 \cdot |X|^{-1} = 1$． $\therefore\ XYX^{-1} \in S$． $\therefore$ $S \triangleleft H$． (q.e.d.)

(note) $SO(n, K)$ が $O(n, K)$ の部分群であることは，次のようにしても示せる．$O(n, K)$ と $SL(n, K)$ が $GL(n, K)$ の部分群であり，$SO(n, K) = O(n, K) \cap SL(n, K)$ なので，(T2) より，$SO(n, K)$ は $GL(n, K)$ の部分群である．$SO(n, K) \subset O(n, K)$ なので，$SO(n, K)$ は $O(n, K)$ の部分群である．

正則な n 次複素行列 U であって，$UU^* = U^*U = E_n$（すなわち $U^{-1} = U^*$）をみたすものをユニタリ行列という．ここに，$U^* = \overline{{}^tU}$ である．n 次ユニタリ行列全体からなる集合を $U(n)$ で表す．これは $GL(n, \mathbf{C})$ の部分群になり，**ユニタリ群** と呼ばれる．n 次ユニタリ行列は行列式が絶対値 1 の複素数になるが，このうち行列式が 1 であるものの全体からなる集合を $SU(n)$ とかき，**特殊ユニタリ群** と呼ぶ．$SU(n)$ は $U(n)$ の正規部分群である．

(ex30) (1) $U(n)$ が $GL(n, \mathbf{C})$ の部分群であることを示せ． (2) $SU(n)$ が $U(n)$ の正規部分群であることを示せ． (3) $U(n) \cap O(n, \mathbf{C}) = O(n, \mathbf{R})$ であることを示せ．

7.（群の直積）G_1, G_2 を 2 つの群とするとき，G_1 と G_2 の直積 $G_1 \times G_2$ を

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1,\, g_2 \in G_2\} \tag{46}$$

で定義する．$G_1 \times G_2$ には，次のように演算が与えられる．

$$(g_1, g_2) * (g_1', g_2') = (g_1 g_1', g_2 g_2') \tag{47}$$

$G_1 \times G_2$ はこの演算に関して群になる．この群の単位元は (e_1, e_2) であり（e_1, e_2 はそれぞれ G_1, G_2 の単位元），$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$ である．

3 つ以上の群の直積 $G_1 \times G_2 \times \cdots \times G_n$ も同様に，

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_1 \in G_1,\, g_2 \in G_2, \ldots, g_n \in G_n\} \tag{48}$$

と定義され，次の演算に関して群になる．

$$(g_1, \ldots, g_n) * (g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n') \tag{49}$$

この群の単位元は $(e_1, e_2, \ldots, e_n)$ で，$(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$ である．

(ex31) $G_1 \times G_2$ が群になることを確認せよ．

($\because$) 明らかに $G_1 \times G_2$ は演算 $*$ について閉じている．次に結合律をみたすことを示す．$(g_1, g_2), (g_1', g_2'), (g_1'', g_2'') \in G_1 \times G_2$ とすると，

$$\begin{aligned} & ((g_1, g_2) * (g_1', g_2')) * (g_1'', g_2'') = (g_1 g_1', g_2 g_2') * (g_1'', g_2'') \\ = \;& ((g_1 g_1') g_1'', (g_2 g_2') g_2'') = (g_1 (g_1' g_1''), g_2 (g_2' g_2'')) \\ = \;& (g_1, g_2) * (g_1' g_1'', g_2' g_2'') = (g_1, g_2) * ((g_1', g_2') * (g_1'', g_2'')) . \end{aligned} \tag{50}$$

単位元が (e_1, e_2) で，$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$ であることは容易に確認できる．(q.e.d.)

.....

(T7) H_i が G_i の部分群のとき，$H_1 \times H_2$ は $G_1 \times G_2$ の部分群である．さらに，$H_i \triangleleft G_i$ ならば，$H_1 \times H_2 \triangleleft G_1 \times G_2$ である．3 つ以上の直積でも同様のことがなりたつ．

.....

($\because$) H_i を G_i の部分群とする．(T1') を用いて，$H_1 \times H_2$ が $G_1 \times G_2$ の部分群であることを示す．$(h_1, h_2), (h_1', h_2') \in H_1 \times H_2$ とする．

$$(h_1, h_2) * (h_1', h_2')^{-1} = (h_1, h_2) * (h_1'^{-1}, h_2'^{-1}) = (h_1 h_1'^{-1}, h_2 h_2'^{-1}) \in H_1 \times H_2 \tag{51}$$

よって示された．

次に $H_i \triangleleft G_i$ とする．$(g_1, g_2) \in G_1 \times G_2$，$(h_1, h_2) \in H_1 \times H_2$ を任意に取れば，

$$(g_1, g_2) * (h_1, h_2) * (g_1, g_2)^{-1} = (g_1 h_1 g_1^{-1}, g_2 h_2 g_2^{-1}) \in H_1 \times H_2. \tag{52}$$

$\therefore$ $H_1 \times H_2 \triangleleft G_1 \times G_2$．(q.e.d.)

$G_1 \triangleleft G_1$，$\{e_2\} \triangleleft G_2$ に (T7) を適用すると，$G_1 \times \{e_2\} \triangleleft G_1 \times G_2$ であり，また $G_1 \times \{e_2\} \simeq G_1$ となる．同様に，$G_2 \simeq \{e_1\} \times G_2 \triangleleft G_1 \times G_2$ である．ゆえに，$G_1 \times G_2$ は G_1 および G_2 と同型な正規部分群を持つことがわかる．3 つ以上の直積でも同様のことが言える．

(ex32) (1) $\underbrace{\mathbf{Z} \times \cdots \times \mathbf{Z}}_{n} \simeq \mathbf{Z}^n$ を示せ．(2) $\mathbf{Z}^m \times \mathbf{Z}^n \simeq \mathbf{Z}^{m+n}$ を示せ．

(ex33) 加群 $\mathbf{R}$ と $\mathbf{C}$ について，$\mathbf{R} \times \mathbf{R} \simeq \mathbf{C}$ を示せ．

(hint) $\phi : \mathbf{R} \times \mathbf{R} \longrightarrow \mathbf{C}$ として，$\phi(x, y) = x + iy$ を取る．ϕ が同型写像であることを言えばよい．

(ex34) 乗法群 $\mathbf{R}^+$，S^1，$\mathbf{C}^\times$ について，$\mathbf{R}^+ \times S^1 \simeq \mathbf{C}^\times$ を示せ．(S^1 の定義は (39) 参照)

(hint) $\phi : \mathbf{R}^+ \times S^1 \longrightarrow \mathbf{C}^\times$ として，$\phi(r, e^{i\theta}) = re^{i\theta}$ を取る．ϕ が同型写像であることを言えばよい．

8.（準同型定理）G, G' を 2 つの群とし，G から G' への写像 ϕ が (13) をみたすとき，ϕ を G から G' への 準同型写像 という．さらに，ϕ が全射であれば全準同型写像，ϕ が単射であれば単準同型写像，ϕ が 1 対 1 対応であれば同型写像という．簡単のため，写像は省略して，準同型，全準同型，単準同型，同型などの用語も用いる．

$\phi : G \longrightarrow G'$ を準同型（あるいは単に写像）とする．G の部分集合 A に対して，

$$\phi(A) = \{\phi(x) \mid x \in A\} \tag{53}$$

と定め，これを ϕ による A の像という．$\phi(A) = B$ のとき，ϕ により，A は B に移されるという．また，G' の部分集合 A' に対して，

$$\phi^{-1}(A') = \{x \in G \mid \phi(x) \in A'\} \tag{54}$$

と定め，これを ϕ による A' の逆像という．

(ex35) 準同型 $\phi : G \longrightarrow G'$ に対して次を示せ．(1) $\phi(e) = e'$．(2) $\phi(x^{-1}) = (\phi(x))^{-1}$．(3) $\phi(x_1 x_2 \dots x_s) = \phi(x_1)\phi(x_2)\dots\phi(x_s)$．

次がなりたつ．

.....

(T8) 準同型 $\phi : G \longrightarrow G'$ に対して，(i) $\mathrm{Ker}\,\phi$ は G の正規部分群であり，(ii) $\mathrm{Im}\,\phi$ は G' の部分群である．

.....

($\because$) (i) まず (T1') を用いて $\mathrm{Ker}\,\phi$ が G の部分群であることを示す．$x, y \in \mathrm{Ker}\,\phi$ とすると，

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)(\phi(y))^{-1} = e'e'^{-1} = e'e' = e'. \tag{55}$$

$\therefore\ xy^{-1} \in \mathrm{Ker}\,\phi$．よって示された．次に $g \in G$，$x \in \mathrm{Ker}\,\phi$ とすると，

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)e'(\phi(g))^{-1} = \phi(g)(\phi(g))^{-1} = e'. \tag{56}$$

$\therefore\ gxg^{-1} \in \mathrm{Ker}\,\phi$．　$\therefore\ \mathrm{Ker}\,\phi \triangleleft G$．(q.e.d.)

($\because$) (ii) (T1') を用いる．$x', y' \in \mathrm{Im}\,\phi$ とすると，$x, y \in G$ が存在して $x' = \phi(x)$，$y' = \phi(y)$．このとき，

$$x'y'^{-1} = \phi(x)(\phi(y))^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in \mathrm{Im}\,\phi. \tag{57}$$

ゆえに $\mathrm{Im}\,\phi$ は G' の部分群である．(q.e.d.)

.....

(T9) ϕ を準同型とするとき，ϕ が単準同型 $\iff \mathrm{Ker}\,\phi = \{e\}$．

.....

($\because$) ($\Rightarrow$) $\phi : G \longrightarrow G'$ を単準同型とする．G の元 x が $x \neq e$ をみたすとすると，$\phi(x) \neq \phi(e) = e'$．　$\therefore\ x \notin \mathrm{Ker}\,\phi$．　$\therefore\ \mathrm{Ker}\,\phi = \{e\}$．(q.e.d.)

($\because$) ($\Leftarrow$) $\phi : G \longrightarrow G'$ を準同型とし，$\mathrm{Ker}\,\phi = \{e\}$ とする．G の元 x, y が $x \neq y$ をみたすとすると，$xy^{-1} \neq e$ となる．　$\therefore\ xy^{-1} \notin \mathrm{Ker}\,\phi$．　$\therefore\ \phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)(\phi(y))^{-1} \neq e'$．　$\therefore\ \phi(x) \neq \phi(y)$．ゆえに ϕ は単準同型である．(q.e.d.)

(T10)（準同型の合成）$\phi : G \longrightarrow G'$，$\psi : G' \longrightarrow G''$ を群の間の（群から群への）2 つの準同型とするとき，合成 $\psi \circ \phi : G \longrightarrow G''$ もまた準同型である．

($\because$) G の任意の元 x, y に対して，

$$\begin{array}{rl} & \psi \circ \phi(xy) = \psi(\phi(xy)) = \psi(\phi(x)\phi(y)) \\ = & \psi(\phi(x))\,\psi(\phi(y)) = \psi \circ \phi(x)\ \psi \circ \phi(y). \qquad \text{(q.e.d.)} \end{array} \tag{58}$$

(T10') (i) 同型写像の合成は同型写像である．(ii) 全準同型の合成は全準同型である．(iii) 単準同型の合成は単準同型である．

($\because$) (i) これは，(T10) および，1 対 1 対応の合成がまた 1 対 1 対応になるということからわかる．(ii) (T10) および，全射の合成がまた全射になるということからわかる．(iii) (T10) および，単射の合成がまた単射になるということからわかる． (q.e.d.)

一般に写像の合成については結合律がなりたつので，同型や準同型の合成についても当然結合律 (10) がなりたつ．したがって，幾らかの (準) 同型の合成は括弧の付け方によらないので，括弧は省略できる．

G を群，H をその部分群とする．H から G への写像 m を

$$m(x) = x \qquad (x \in H) \tag{59}$$

で定めるとき，m を標準的単射という．これは単準同型である．次に，H を G の正規部分群とする．G から G/H への写像 p を

$$p(g) = Hg \qquad (g \in G) \tag{60}$$

で定めるとき，p を標準的全射という．これは全準同型である．

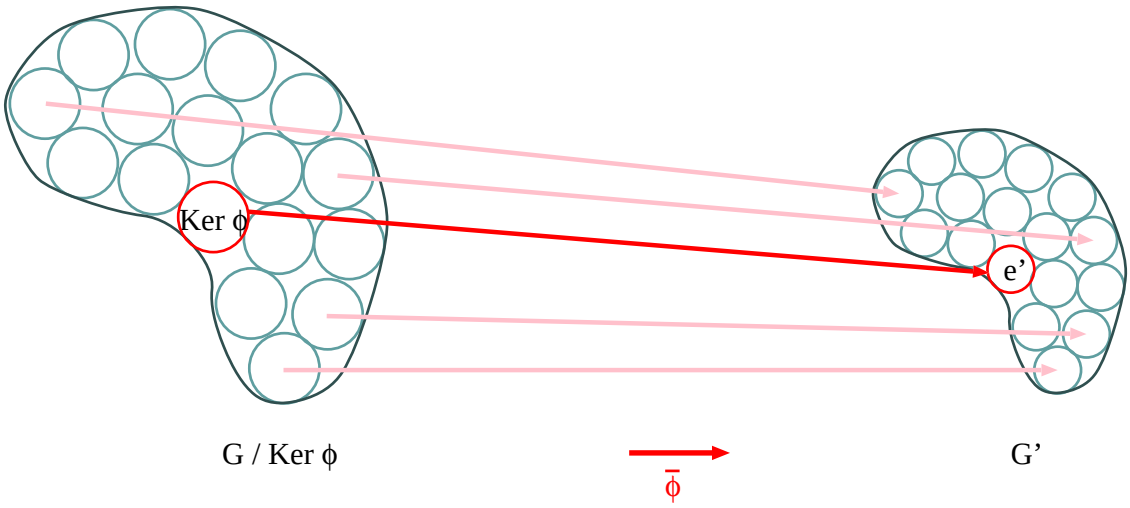
(ex36) (1) m が単準同型であることを示せ． (2) p が全準同型であることを示せ．

(T11)（準同型定理）G から G' への全準同型 ϕ に対して，$\mathrm{Ker}\,\phi = N$ とおく．G から G/N への標準的全射を p とおく．このとき，G/N から G' への同型写像 $\overline{\phi}$ であって，$\overline{\phi} \circ p = \phi$ をみたすものがただ 1 つ存在する．これにより，

$$G/N \simeq G' \tag{61}$$

を得る．次の図は写像の関係を表す可換図式である．(可換図式とは，写像や写像の合成が，矢印のたどり方によらない図のことで，この場合は写像 $G \longrightarrow G'$ と写像の合成 $G \longrightarrow G/N \longrightarrow G'$ が同じ写像になることを示している．)

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ {\scriptstyle p}\downarrow & \overline{\phi}\nearrow & \\ G/N & & \end{array} \tag{62}$$



($\because$) G/N に属する剰余類 Ng を任意に取る．ϕ により，Ng の任意の元 ng は

$$\phi(ng) = \phi(n)\phi(g) = e'\phi(g) = \phi(g) \tag{63}$$

に移る．ここで写像 $\overline{\phi} : G/N \longrightarrow G'$ を

$$\overline{\phi}(Ng) = \phi(g) \tag{64}$$

で定めれば，$\overline{\phi}$ はきちんと定義される．また，任意の $g \in G$ に対して，

$$\overline{\phi} \circ p(g) = \overline{\phi}(p(g)) = \overline{\phi}(Ng) = \phi(g) \tag{65}$$

なので，$\overline{\phi} \circ p = \phi$ をみたす．この $\overline{\phi}$ 以外に $\overline{\phi} \circ p = \phi$ をみたすものはない．

そこで，$\overline{\phi}$ が同型写像であることを示す．G/N の任意の元 $Ng, N\tilde{g}$ に対して，

$$\overline{\phi}(Ng\,N\tilde{g}) = \overline{\phi}(N(g\tilde{g})) = \phi(g\tilde{g}) = \phi(g)\phi(\tilde{g}) = \overline{\phi}(Ng)\overline{\phi}(N\tilde{g}). \tag{66}$$

よって $\overline{\phi}$ は準同型である．次に $\overline{\phi}$ が 1 対 1 対応であることを示す．G' の任意の元 g' を取る．ϕ が全射なので，$\phi(g) = g'$ なる $g \in G$ がある．すると $Ng \in G/N$ に対して，$\overline{\phi}(Ng) = \phi(g) = g'$．ゆえに $\overline{\phi}$ は全射である．また $\overline{\phi}(Ng_1) = \overline{\phi}(Ng_2)$ とすると，$\phi(g_1) = \phi(g_2)$ となり，$\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2^{-1}) = \phi(g_1)(\phi(g_2))^{-1} = e'$．　$\therefore$ $g_1 g_2^{-1} = n \in N$．　$\therefore$ $g_1 = n g_2 \in N g_2$．ゆえに (T3) より $Ng_1 = Ng_2$．ゆえに $\overline{\phi}$ は単射である．以上より，$\overline{\phi}$ は 1 対 1 対応である．(q.e.d.)

準同型定理は，より一般的に次のように述べられる．

(T11')（準同型定理）G から G' への準同型 ϕ に対して，$\mathrm{Ker}\,\phi = N$ とおく．G から G/N への標準的全射を p とおく．このとき，G/N から $\mathrm{Im}\,\phi$ への同型写像 $\overline{\phi}$ であって，$\overline{\phi} \circ p = \phi$ をみたすものがただ 1 つ存在し，

$$G/N \simeq \mathrm{Im}\,\phi. \tag{67}$$

($\because$) ϕ は，G から $\mathrm{Im}\,\phi$ への全準同型なので，これに (T11) を適用すれば得られる．(q.e.d.)

(ex37) 写像 $\phi : \mathbf{C}^\times \longrightarrow \mathbf{R}^+$ を $\phi(z) = |z|$ で定義するとき，ϕ は全準同型であることを示せ．また，この写像に準同型定理を適用して，$\mathbf{C}^\times/S^1 \simeq \mathbf{R}^+$ を示せ．(S^1 の定義は (39) 参照)

9.（同型定理）準同型定理は，(全) 準同型があるとき，定義域を核で割って同型を誘導するという内容を持つ．これを幾らかの典型的な全準同型に適用すると，同型定理と呼ばれる定理を得る．少し準備をしたのち，同型定理を述べる．

(T12) G, G' を群，$\phi : G \longrightarrow G'$ を準同型とする．H を G の部分群，$N \triangleleft G$ とし，H' を G' の部分群，$N' \triangleleft G'$ とする．このとき，(i) $\phi(H)$ は $\mathrm{Im}\,\phi$ の部分群，$\phi(N) \triangleleft \mathrm{Im}\,\phi$ である．(ii) $\phi^{-1}(H')$ は G の部分群，$\phi^{-1}(N') \triangleleft G$ である．

($\because$) (i) まず (T1') を用いて $\phi(H)$ が $\mathrm{Im}\,\phi$ の部分群であることを言う．$x', y' \in \phi(H)$ とすると，$x, y \in H$ が存在して $\phi(x) = x'$，$\phi(y) = y'$．このとき，

$$x'y'^{-1} = \phi(x)(\phi(y))^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in \phi(H). \tag{68}$$

ゆえに，$\phi(H)$ は $\mathrm{Im}\,\phi$ の部分群である．

次に，$\phi(N) \triangleleft \mathrm{Im}\,\phi$ を言う．$\phi(N)$ が単に部分群であることは上と同様．$g' \in \mathrm{Im}\,\phi$，$n' \in \phi(N)$ $(n \in N)$ とすると，ある $g \in G$，$n \in N$ が存在して，$\phi(g) = g'$，$\phi(n) = n'$ となるので，

$$g'n'g'^{-1} = \phi(g)\phi(n)(\phi(g))^{-1} = \phi(g)\phi(n)\phi(g^{-1}) = \phi(gng^{-1}) \in \phi(N). \tag{69}$$

$\therefore$ $\phi(N) \triangleleft \mathrm{Im}\,\phi$. (q.e.d.)

($\because$) (ii) まず (T1') を用いて $\phi^{-1}(H')$ が G の部分群となることを言う．$x, y \in \phi^{-1}(H')$ とすると，

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)(\phi(y))^{-1} \in H'. \tag{70}$$

$\therefore$ $xy^{-1} \in \phi^{-1}(H')$．ゆえに，$\phi^{-1}(H')$ は G の部分群である．

次に，$\phi^{-1}(N') \triangleleft G$ を言う．$\phi^{-1}(N')$ が単に部分群であることは上と同様．$g \in G$，$n \in \phi^{-1}(N')$ とすると，

$$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)\phi(n)(\phi(g))^{-1} \in g'N'g'^{-1} = N'. \tag{71}$$

$\therefore$ $gng^{-1} \in \phi^{-1}(N')$. $\quad\therefore$ $\phi^{-1}(N') \triangleleft G$. (q.e.d.)

(T12') G, G' を群，$\phi : G \longrightarrow G'$ を準同型とする．$\mathrm{Ker}\,\phi$ を含む G の正規部分群全体の集合 $\mathbf{S}$ から，$\mathrm{Im}\,\phi$ の正規部分群全体の集合 $\mathbf{S}'$ への 1 対 1 対応 $\tilde{\phi}$ が，$\tilde{\phi}(N) = \phi(N)$ $(\tilde{\phi}^{-1}(N') = \phi^{-1}(N'))$ で得られる．この定理は，“正規部分群” を単に “部分群” に置き換えてもなりたつ．

($\because$)（同様なので正規部分群のときを示す）(T12) で見たように，ϕ により，G の正規部分群は，$\mathrm{Im}\,\phi$ の正規部分群に移される．ゆえに $\tilde{\phi}$ は $\mathbf{S}$ から $\mathbf{S}'$ への写像である．あとは $\tilde{\phi}$ が 1 対 1 対応であることを言う．$\mathbf{S}'$ の任意の元 N' を取る．$N = \phi^{-1}(N')$ とおくと，(T12) より $N \triangleleft G$ であり，$N' \ni e'$ より $N \supset \mathrm{Ker}\,\phi$ なので，$N \in \mathbf{S}$．また $N' \subset \mathrm{Im}\,\phi$

より $\phi(N) = N'$．ゆえに $\tilde{\phi}$ は全射である．次に，$\mathbf{S}$ の異なる 2 元 $N_1 \neq N_2$ を取る．仮に $\tilde{\phi}(N_1) = \tilde{\phi}(N_2) = N'$ とする．$x \in N_2 - N_1$ を取れるとしてよい．（取れないときは N_1, N_2 を入れ替える）そこで $\phi(x) = x' \in N'$ とおくとき，$y \in N_1$ が存在して，$\phi(y) = x'$ となる． $\therefore\ \phi(xy^{-1}) = \phi(x)(\phi(y))^{-1} = x'x'^{-1} = e'$． $\therefore\ xy^{-1} = n \in \mathrm{Ker}\,\phi$. $\therefore\ x = ny \in N_1$.（矛盾） ゆえに $\tilde{\phi}$ は単射である．以上より，$\tilde{\phi}$ は $\mathbf{S}$ から $\mathbf{S}'$ への 1 対 1 対応である． (q.e.d.)

. . . . . .

(T13) G を群，$N \triangleleft G$，とし，H を G の部分群とする．このとき，$HN = NH$ であり，これは G の部分群である．

. . . . . .

($\because$) $N \triangleleft G$ なので，$hN = Nh$ $(h \in H)$．ゆえに，$HN = NH$．次に HN が G の部分群であることを言う．$hn, h'n' \in HN$ とする．$hn(h'n')^{-1} = hnn'^{-1}h'^{-1} = hn''h''$．ここで，$Nh'' = h''N$ より，$hn''h'' = hh''n''' = h'''n''' \in HN$． (q.e.d.)

(ex38) G を群，N をその正規部分群，H を G の部分群で $H \supset N$ をみたすとする．このとき N は H の正規部分群にもなっており，H/N は G/N の部分群となることを示せ．

($\because$) （N が H の正規部分群となること） N が H の部分群であることは明らか．$N \triangleleft G$ なので，$gNg^{-1} = N$ $(g \in G)$ がなりたつ．ところが $H \subset G$ なので，$hNh^{-1} = N$ $(h \in H)$ がなりたつ． $\therefore\ N \triangleleft H$． (q.e.d.)

($\because$) （H/N が G/N の部分群となること） H/N の元 Nh は確かに G/N の元なので，$H/N \subset G/N$．H/N 自体が G/N と同じ演算に関する群であることは明らかなので，H/N は G/N の部分群である． (q.e.d.)

. . . . . .

(T14)（同型定理）

(i) G, G' を群，$\phi : G \longrightarrow G'$ を全準同型とし，$N' \triangleleft G'$ とする．$\phi^{-1}(N') = N$ とおくと，$N \triangleleft G$ となり，

$$G/N \simeq G'/N'. \tag{72}$$

(ii) G を群，$N \triangleleft G$，とし，H を G の部分群とする．このとき，

$$H/(H \cap N) \simeq (HN)/N. \tag{73}$$

(iii) G を群，$H, N \triangleleft G$，$H \supset N$ とするとき，

$$G/H \simeq (G/N)/(H/N). \tag{74}$$

. . . . . .

($\because$) (i) 全準同型の合成:

$$G \xrightarrow{\phi} G' \xrightarrow{p} G'/N' \tag{75}$$

（p は標準的全射）を考えると，$p \circ \phi : G \longrightarrow G'/N'$ を得るが，それは (T10') より全準同型になる．そして，

$$\mathrm{Ker}(p \circ \phi) = (p \circ \phi)^{-1}(N') = \phi^{-1}(p^{-1}(N')) = \phi^{-1}(N') = N \tag{76}$$

となる．そこで，$p \circ \phi$ に準同型定理を適用して，$G/N \simeq G'/N'$ を得る． (q.e.d.)

($\because$) (ii) 準同型の合成:

$$H \xrightarrow{m} HN \xrightarrow{p} HN/N \tag{77}$$

(m は標準的単射）を考えると，$p \circ m : H \longrightarrow HN/N$ を得るが，それは (T10) より準同型になる．さらに $p \circ m$ が全射であることを示す．HN/N の任意の元は $hnN = hN$ $(h \in H)$ の形で表され，その h に対して $p \circ m(h) = hN$ となるので，$p \circ m$ は全射である．こうして $p \circ m$ は全準同型だと言える．また，

$$\mathrm{Ker}(p \circ m) = (p \circ m)^{-1}(N) = m^{-1}(p^{-1}(N)) = m^{-1}(N) = H \cap N. \tag{78}$$

そこで，$p \circ m$ に準同型定理を適用して，$H/(H \cap N) \simeq HN/N$ を得る．(q.e.d.)

($\because$) (iii) $H, N \triangleleft G$，$H \supset N$ のとき，$H/N \triangleleft G/N$ を示す．まず H/N が G/N の部分群であることは (ex38) で見た．次に，$Ng \in G/N$，$Nh \in H/N$ とする．

$$(Ng)(Nh)(Ng)^{-1} = (Ng)(Nh)(Ng^{-1}) = Nghg^{-1} = Nh' \in H/N. \tag{79}$$

$\therefore$ $H/N \triangleleft G/N$．次に準同型の合成:

$$G \xrightarrow{p} G/N \xrightarrow{\tilde{p}} (G/N)/(H/N) \tag{80}$$

を考える．これは標準的全射の合成なので，(T10') より全準同型である．また，

$$\mathrm{Ker}(\tilde{p} \circ p) = (\tilde{p} \circ p)^{-1}(H/N) = p^{-1}(\tilde{p}^{-1}(H/N)) = p^{-1}(H/N) = H. \tag{81}$$

そこで，$\tilde{p} \circ p$ に準同型定理を適用して，$G/H \simeq (G/N)/(H/N)$ を得る．(q.e.d.)

(ex39) (1) 絶対値が正の有理数になる複素数全体からなる集合 Q は乗法群をなす．このとき，$\mathbf{C}^\times/Q \simeq \mathbf{R}^+/\mathbf{Q}^+$ を示せ.

(2) 乗法群についての同型: $\mathbf{R}^+/\mathbf{Q}^+ \simeq \mathbf{R}^\times/\mathbf{Q}^\times$ を示せ.

(3) 加群についての同型: $(\mathbf{C}/\mathbf{Q})/(\mathbf{R}/\mathbf{Q}) \simeq \mathbf{C}/\mathbf{R} \simeq \mathbf{R}$ を示せ.

(hint) (1) $\phi(z) = |z|$ を取れ．(2) $H = \mathbf{R}^+$，$N = \mathbf{Q}^\times$ とおくか，$\phi(x) = |x|$ を取れ．あるいは $K^\times/\{1, -1\} \simeq K^+$ $(K = \mathbf{R}, \mathbf{Q})$ を用いよ.

ここで，準同型定理の応用をもう少し述べておく.

(T15) 位数 n の有限群 G は，S_n のある部分群に同型である.

($\because$) $G = \{g_1, g_2, \ldots, g_n\}$ とする．$g \in G$ に対して $gG = G$ なので，

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix} \tag{82}$$

の 2 行は 1 行を並べ替えたものになっている．ゆえに，$gg_i = g_{\sigma(i)}$ $(i = 1, \ldots, n)$ をみたす $\sigma \in S_n$ が存在する．そこで写像 $\phi : G \longrightarrow S_n$ を

$$\phi(g) = \sigma \tag{83}$$

で定義する．このとき，ϕ が準同型であることを示す．$g, g' \in G$ とするとき，

$$\begin{array}{l} g_{\phi(gg')(i)} = (gg')g_i = g(g'g_i) = gg_{\phi(g')(i)} = g_{\phi(g)\phi(g')(i)}. \\ \therefore\ \phi(gg') = \phi(g)\phi(g'). \end{array} \tag{84}$$

また，$\phi(g) = e \iff gg_i = g_i \iff g = e$ より，$\mathrm{Ker}\,\phi = \{e\}$．ゆえに，準同型定理 (T11') より，$G \simeq G/\{e\} \simeq \mathrm{Im}\,\phi \subset S_n$． (q.e.d.)

.....

(T16) $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}$ とするとき，次がなりたつ．

$$\begin{array}{l} \text{(i) } GL(n,K)/SL(n,K) \simeq K^\times. \qquad \text{(ii) } O(n,K)/SO(n,K) \simeq \{1,-1\}. \\ \text{(iii) } U(n)/SU(n) \simeq S^1. \quad (S^1 \text{ の定義は (39) 参照}) \\ \text{(iv) } S_n/A_n \simeq \{1,-1\}. \qquad (n \geq 2) \end{array} \tag{85}$$

.....

($\because$) (i) 写像 $\phi : GL(n,K) \longrightarrow K^\times$ を次で定める．

$$\phi(X) = |X| \tag{86}$$

正則な行列の行列式は 0 でなく，K の元を成分とする行列の行列式は K の元なので，ϕ はきちんと定義されている．$X, Y \in GL(n,K)$ とするとき，

$$\phi(XY) = |XY| = |X||Y| = \phi(X)\phi(Y). \tag{87}$$

ゆえに ϕ は準同型である．また $K^\times$ の任意の元 k に対して $\phi(X) = k$ をみたす $X \in GL(n,K)$ が存在する．(なぜか?) ゆえに ϕ は全射である．ゆえに ϕ は全準同型である．そこで，$\mathrm{Ker}\,\phi$ を求める．$\phi(X) = |X| = 1 \iff X \in SL(n,K)$ より，$\mathrm{Ker}\,\phi = SL(n,K)$．したがって準同型定理より，$GL(n,K)/SL(n,K) \simeq K^\times$． (q.e.d.)

(ii),(iii) の証明も同様なので読者に委ねる．

($\because$) (iv) $n \geq 2$ とする．写像 $\phi : S_n \longrightarrow \{1,-1\}$ を次で定める．

$$\phi(\sigma) = \mathrm{sgn}(\sigma) \tag{88}$$

明らかに ϕ は全射であり，$\sigma, \tau \in S_n$ とするとき，

$$\phi(\sigma\tau) = \mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau) = \phi(\sigma)\phi(\tau) \tag{89}$$

なので，ϕ は全準同型である．そこで $\mathrm{Ker}\,\phi$ を求める．$\phi(\sigma) = \mathrm{sgn}(\sigma) = 1 \iff \sigma \in A_n$ より，$\mathrm{Ker}\,\phi = A_n$．ゆえに準同型定理より，$S_n/A_n \simeq \{1,-1\}$． (q.e.d.)

10.（元の位数と巡回群）群 G の元 a を取る．$aa = a^2$，$aaa = a^3, \ldots$ などと表記し，a の正のベキという．また，$a^0 = e$ と約束し，$a^{-n} = (a^{-1})^n$ によって a の負のベキを定める．このとき，$(a^n)^{-1} = a^{-n}$ となる．一般に，整数 m, n に対して，指数法則 $a^m a^n = a^{m+n}$，$(a^m)^n = a^{mn}$ がなりたつ．

$a^n = e$ をみたす最小の正の整数 n があればそれを a の 位数 といい，$\mathrm{ord}(a)$ で表す．どのような正の整数に対しても $a^n = e$ がなりたたないならば，a は無限位数を持つといい，$\mathrm{ord}(a) = \infty$ とかく．このときは，a のベキ

$$a^0 = e, a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, \ldots \tag{90}$$

はすべて異なる．なぜならば，仮に $a^m = a^n$ $(m > n)$ とすれば，両辺に a^{-n} をかけて，$a^{m-n} = e$ となるからである．

一般に G の元 a に対して，

$$\langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, \ldots\} \tag{91}$$

とおくと，これは G の部分群をなす．この部分群を a で生成される G の部分群という．

特に $\mathrm{ord}(a) = n$ のときは，(91) は

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\} \tag{92}$$

になる．ここで $e, a, a^2, \ldots, a^{n-1}$ はすべて異なるので，$|\langle a \rangle| = \mathrm{ord}(a)$ がなりたつ．

G が加群のときは，$a + a = 2a$，$a + a + a = 3a, \ldots$ などとかく．このとき，$\mathrm{ord}(a)$ は $na = 0$ となる最小の正の整数 n（なければ ∞）となり，(91)，(92) はそれぞれ，

$$\{0, \pm a, \pm 2a, \ldots\}, \qquad \{0, a, 2a, \ldots, (n-1)a\} \tag{93}$$

と表される．

(ex40) $\mathrm{ord}(a) = n$ のとき，(92) が G の部分群となることを示せ．

群 G が，G のある元 a によって $G = \langle a \rangle$ とかけるとき，G を 巡回群 あるいは巡回的であるといい，a を G の生成元という．巡回群は可換群である．位数が無限の巡回群を無限巡回群，位数が有限の巡回群を有限巡回群という．特に n 元からなる巡回群を総称的に C_n で表す．

正の整数 n に対して，$n\mathbf{Z}$ で n の倍数（0 と負の数を含めて）全体の集合:

$$n\mathbf{Z} = \{0, \pm n, \pm 2n, \ldots\} \tag{94}$$

を表す．$n\mathbf{Z}$ は $\mathbf{Z}$ の部分加群であり，正規部分群である．そこで，加群としての剰余群

$$\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z} \tag{95}$$

を考えることができる．これは，$n\mathbf{Z} + k$ $(0 \le k \le n-1)$ の形の剰余類からなっている．簡単のために $n\mathbf{Z} + k$ を $\overline{k}$ とかけば，

$$\mathbf{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\} \tag{96}$$

であり，$\mathbf{Z}_n$ においては，$\overline{k} + \overline{l} = \overline{k+l} = \overline{m}$（$m$ は $k + l$ を n で割った余り）と計算できる．$\mathbf{Z}_n$ は巡回群であり，その生成元は $1 \le x \le n$ かつ n と互いに素（最大公約数が 1）な x に対して $\overline{x}$ である．

(T17) 無限巡回群 G および有限巡回群 C_n について，(i) $G \simeq \mathbf{Z}$，(ii) $C_n \simeq \mathbf{Z}_n$.

($\because$) (i) 無限巡回群を $G = \{e, a^{\pm 1}, a^{\pm 2}, \ldots\}$ $(\mathrm{ord}(a) = \infty)$ とする．ここで，$\phi : G \longrightarrow \mathbf{Z}$ を，

$$\phi(a^m) = m \qquad (a^m \in G) \tag{97}$$

で定める．a のベキたちがすべて異なるので，ϕ をこのように定義できる．このとき明らかに ϕ は 1 対 1 対応である．任意の $a^m, a^n \in G$ に対して，

$$\phi(a^m a^n) = \phi(a^{m+n}) = m + n = \phi(a^m) + \phi(a^n). \tag{98}$$

ゆえに ϕ は同型写像である． $\therefore$ $G \simeq \mathbf{Z}$. (q.e.d.)

(ii) についても $\phi : C_n \longrightarrow \mathbf{Z}_n$ を，$\phi(a^m) = \overline{m}$ $(a^m \in C_n)$ とすれば同様に示せる．

(ex41) (1) 巡回群が可換群であることを示せ． (2) $\mathbf{Z} = \langle 1 \rangle$ を示せ． (3) $\mathbf{Q}^\times$ において $\langle 2 \rangle$ を求めよ． (4) $\mathbf{C}^\times$ において $\langle i \rangle$ を求めよ． (5) $\mathbf{Z}_6$ の加法表（和の結果をかいた表）をかけ． (6) $2 \leq n \leq 12$ に対して，$\mathbf{Z}_n$ の生成元をすべて求めよ．

(ex42) (1) $1 \leq n \leq 4$ に対して，S_n の各元の位数を求めよ．

(2) S_3 において，$\langle \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \rangle$ を求めよ． (3) (T17)(ii) を示せ．

(T18) 有限群 G の各元の位数は G の位数の約数である．

($\because$) 位数 n の有限群 G の任意の元 a を取ると，部分群 $\langle a \rangle$ が生じる．このとき，$|\langle a \rangle| = \mathrm{ord}(a)$．ところが (T6) より，位数 n の群の部分群の位数は n の約数なので，$\mathrm{ord}(a) \mid n$ を得る．ここに，$m \mid n$ で，m が n の約数であることを示す． (q.e.d.)

(T19) $a \in C_n$ とするとき， a が C_n の生成元 $\iff$ $\mathrm{ord}(a) = n$.

($\because$) ($\Rightarrow$) a を C_n の生成元とする．C_n は n 元からなるので，(92) の形になる．したがって，$\mathrm{ord}(a) = n$. (q.e.d.)

($\because$) ($\Leftarrow$) $\mathrm{ord}(a) = n$ とする．このとき $\langle a \rangle$ は (92) でかける．これは n 元からなる C_n の部分群なので，C_n に一致する． (q.e.d.)

(ex43) G を素数位数 p の群とする．(1) G の任意の元 $a \neq e$ の位数はいくらか？ (2) G が巡回群であることを示せ．

(ex44) $\mathrm{ord}(a) = n$ とする．(1) $\mathrm{ord}(a^{-1}) = n$ を示せ． (2) m を整数とするとき，$a^m = e \iff n \mid m$ を示せ． (3) $d \geq 1$，$d \mid n$ のとき，$\mathrm{ord}(a^d) = n/d$ を示せ．

(T20) $\mathrm{ord}(a) = n$，m を整数とするとき，$\mathrm{ord}(a^m) = n/(m, n)$．ここに，$(m, n)$ は m と n の最大公約数 $(\gcd(m, n))$ を意味する．

($\because$) a^m の位数は，$a^{mk}=e$ となるような最小の正の整数 k である．それは $n \mid mk$ をみたす最小の k である．ここで $(m,n)=d$ を取ると，

$$n \mid mk \iff \frac{n}{d} \mid \frac{m}{d}k \tag{99}$$

なので，(99) 右辺をみたす最小の k を求めればよいことがわかる．ここで，$\frac{n}{d}$ と $\frac{m}{d}$ は互いに素なので，$k=\frac{n}{d}$ となる． (q.e.d.)

(ex45) (1) 素数位数 p の元 a に対し，a^m の位数を求めよ．$(m=1,2,\ldots,p-1)$
(2) 1 の n 乗根全体からなる集合

$$Z_n=\{e^{\frac{2m}{n}\pi i} \mid m=0,1,\ldots,n-1\} \tag{100}$$

は巡回群であり，$Z_n \simeq C_n \simeq \mathbf{Z}_n$ がなりたつ．$1 \le n \le 12$ のとき，Z_n の各元の位数を求めよ．

(ex46) (1) 巡回群の部分群は巡回群になることを示せ． (2) S_n が巡回群 $\iff n=1,2$ を示せ．

($\because$) (1) $G=\langle a \rangle$ を巡回群とする．G の元は a のベキで表される．H を G の部分群とする．$a^m \in H$ をみたす最小の正の整数 m を取る．このとき H の任意の元は a^{mq} $(q \in \mathbf{Z})$ の形で表される．なぜならば，$a^n \in H$ とすると，n を m で割って $n=mq+r$ $(0 \le r < m)$． $\therefore\ a^n(a^{mq})^{-1}=a^{mq+r}a^{-mq}=a^r \in H$． $\therefore\ r=0$． $\therefore\ n=mq$．こうして，

$$H=\{e, a^{\pm m}, a^{\pm 2m}, a^{\pm 3m}, \ldots\}. \tag{101}$$

$\therefore\ H=\langle a^m \rangle$． (q.e.d.)

(note) この証明からわかるように，無限巡回群の部分群は無限巡回群である．有限巡回群の部分群が有限巡回群であることは言うまでもない．

.....

(T21) $\phi : G \longrightarrow G'$ を準同型，$a \in G$ とするとき，$\mathrm{ord}(\phi(a)) \mid \mathrm{ord}(a)$．特に ϕ が単準同型ならば，$\mathrm{ord}(a)=\mathrm{ord}(\phi(a))$．

.....

($\because$) $\mathrm{ord}(a)=n$ とする．$a^n=e$ より，$\phi(a^n)=(\phi(a))^n=\phi(e)=e'$． $\therefore\ \mathrm{ord}(\phi(a)) \mid n$．ここで ϕ が単準同型とすると，ϕ を $\phi : G \longrightarrow \mathrm{Im}\,\phi$ とみなせば同型写像になる．このとき逆写像 $\phi^{-1} : \mathrm{Im}\,\phi \longrightarrow G$ も同型写像なので，すでに示したことより，$n \mid \mathrm{ord}(\phi(a))$．$\mathrm{ord}(\phi(a)) \mid n$ と合わせて，$\mathrm{ord}(\phi(a))=n$． (q.e.d.)

一般に群 G の部分集合 S に対して，$\langle S \rangle$ によって，S を含むすべての部分群の共通部分を表す．これは (T2') より G の部分群となり，S で生成される G の部分群と呼ばれる．また，S を含む任意の部分群 H に対して，定義より $\langle S \rangle \subset H$ がなりたつので，$\langle S \rangle$ は S を含む最小の部分群であることがわかる．これを明示的にかけば，

$$\langle S \rangle = \{S \text{ の元たちおよびそれらの逆元たちからできる可能な積のすべて}\} \tag{102}$$

となる．特に $S=\{a\}$ のとき，$\langle S \rangle$ は $\langle a \rangle$ の定義と一致する．

$G=\langle S \rangle$ がなりたつとき，G は S で生成される，あるいは S は G の生成系であるという．また，S の元を G の生成元という．G が有限集合で生成されるとき，G を有限生成という．

正則な行列は，基本行列の積で表される.（線形代数ハンドアウト 5 章参照） したがって，K の元を成分とする n 次基本行列全体の集合を S とおけば，$GL(n,K)=\langle S\rangle$ である.

n 次対称群 S_n の各元は，互換の積で表される.（線形代数ハンドアウト 7 章参照） さらに，互換は $(i,i+1)$ $(i=1,\ldots,n-1)$ たちで表せることが示せる．これより，$S_n=\langle(1,2),(2,3),\ldots,(n-1,n)\rangle$ である.

11.（中心，中心化群，正規化群）G を群とする．G のすべての元と可換な元の集合，すなわち

$$Z=\{x\in G\mid xg=gx\quad(g\in G)\}\tag{103}$$

は G の正規部分群をなす．これを G の 中心 という．より一般に，G の部分集合 S を取るとき，

$$Z(S)=\{x\in G\mid xs=sx\quad(s\in S)\}\tag{104}$$

は G の部分群をなす．これを S の 中心化群 という．$Z=Z(G)$ である.

(note) G が可換群 $\iff$ $Z=G$ がなりたつ.

(ex47) (1) $Z(S)$ が G の部分群であることを示せ． (2) Z が G の正規部分群であることを示せ.

($\because$) (1) $x,y\in Z(S)$ とする．任意の $s\in S$ に対して，

$$(xy)s=x(ys)=x(sy)=(xs)y=(sx)y=s(xy).\tag{105}$$

$\therefore$ $xy\in Z(S)$．また，$xs=sx$ より，$sx^{-1}=x^{-1}s$ を得る． $\therefore$ $x^{-1}\in Z(S)$．ゆえに (T1) より，$Z(S)$ は G の部分群となる． (q.e.d.)

($\because$) (2) (1) より，Z が G の部分群であることは言えたので，$g\in G$，$x\in Z$ に対して，

$$gxg^{-1}=xgg^{-1}=xe=x\in Z.\tag{106}$$

$\therefore$ $Z\triangleleft G$． (q.e.d.)

G の部分集合 S と G の元 x に対して，

$$xSx^{-1}=\{xsx^{-1}\mid s\in S\}\tag{107}$$

を S と 共役な 部分集合という．S と xSx^{-1} は互いに共役になっている．特に H が G の部分群ならば，xHx^{-1} も G の部分群になる．xHx^{-1} を H と共役な部分群という．H が G の正規部分群ならば，H と共役な部分群は H のみである．ここで，再び S を単に部分集合とするとき，

$$N(S)=\{x\in G\mid xSx^{-1}=S\}\tag{108}$$

は G の部分群をなす．これを S の 正規化群 という.

(ex48) (1) $H\triangleleft G$ のとき，$N(H)=G$ を示せ． (2) G を可換群とするとき，G の任意の部分集合 S に対して $N(S)=G$ を示せ.

(ex49) (1) H が G の部分群のとき，xHx^{-1} も G の部分群になることを示せ．(2) $N(S)$ が G の部分群であることを示せ．

($\because$) (1) H を G の部分群とし，$g, g' \in xHx^{-1}$ とする．$g = xhx^{-1}$，$g' = xh'x^{-1}$ $(h, h' \in H)$ とかけるので，

$$gg'^{-1} = xhx^{-1}(xh'x^{-1})^{-1} = xhx^{-1}xh'^{-1}x^{-1} = xhh'^{-1}x^{-1} = xh''x^{-1} \in xHx^{-1}. \tag{109}$$

ゆえに，xHx^{-1} は G の部分群である．(q.e.d.)

($\because$) (2) $x, y \in N(S)$ とする．

$$(xy)S(xy)^{-1} = xySy^{-1}x^{-1} = xSx^{-1} = S \tag{110}$$

$\therefore$ $xy \in N(S)$．また，$xSx^{-1} = S$ より，$S = x^{-1}Sx$ を得る．$\therefore$ $x^{-1} \in N(S)$．ゆえに (T1) より，$N(S)$ は G の部分群となる．(q.e.d.)

(ex50) $n \leq 4$ のとき，S_n の適当な部分群 H について，$N(H)$ を求めてみよ．

(note) $S = \{a\}$ のとき，$Z(S) = Z(a)$，$N(S) = N(a)$ と略記する．

12.（共役類）群 G の元 x, y に対して，ある元 $g \in G$ が存在して，$y = gxg^{-1}$ となるとき，x と y は互いに共役であるという．共役であるという関係は G 上の同値関係，すなわち，反射的，対称的，推移的な関係である．(離散系論ハンドアウト 2 章参照) したがって，G は互いに共役な元全体からなる同値類によって類別される．この同値類のことを G の 共役類 という．より詳しく，x が含まれる共役類のことを x の共役類といい，$\mathrm{Cl}(x)$ で表す．すなわち，

$$\mathrm{Cl}(x) = \{gxg^{-1} \mid g \in G\}. \tag{111}$$

(ex51) 共役であるという関係が同値関係であることを示せ．

(note) (1) 単位元 e に対して，つねに $\mathrm{Cl}(e) = \{e\}$ である．(2) 可換群 G においては，すべての共役類がただ 1 つの元からなる．すなわち，$\mathrm{Cl}(x) = \{x\}$ $(x \in G)$.

(T22) 群 G において，互いに共役な元は等しい位数を持つ．

($\because$) $y = gxg^{-1}$ とすると，$x^n = e \iff y^n = gx^ng^{-1} = e$ がなりたつ．これより，$\mathrm{ord}(x) = \mathrm{ord}(y)$．(q.e.d.)

(T23) $\phi : G \longrightarrow G'$ を全準同型とするとき，G の各共役類 $\mathrm{Cl}(x)$ に対して，$\phi(\mathrm{Cl}(x)) = \mathrm{Cl}(\phi(x))$ がなりたつ．すなわち，共役類の ϕ による像はまた共役類である．

($\because$) G の元 x を任意に取る．$\mathrm{Cl}(x)$ の任意の元 gxg^{-1} $(g \in G)$ に対して，

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(x)(\phi(g))^{-1} \in \mathrm{Cl}(\phi(x)). \tag{112}$$

$\therefore$ $\phi(\mathrm{Cl}(x)) \subset \mathrm{Cl}(\phi(x))$．また，$\phi$ が全準同型なので，$\mathrm{Cl}(\phi(x))$ の任意の元 $g'\phi(x)g'^{-1}$ $(g' \in G')$ に対して，$\phi(g) = g'$ となる $g \in G$ があるので，

$$g'\phi(x)g'^{-1} = \phi(g)\phi(x)\phi(g^{-1}) = \phi(gxg^{-1}) \in \phi(\mathrm{Cl}(x)). \tag{113}$$

$\therefore$ $\mathrm{Cl}(\phi(x)) \subset \phi(\mathrm{Cl}(x))$．$\therefore$ $\phi(\mathrm{Cl}(x)) = \mathrm{Cl}(\phi(x))$．(q.e.d.)

(note) この証明からわかるように，ϕ が準同型のときは，$\phi(\mathrm{Cl}(x)) \subset \mathrm{Cl}(\phi(x))$ がなりたつ．

ここで，n 次対称群 S_n の共役類について考えよう．S_n の元のうち，以下のような文字の入れ替えを行うもの（他の文字は動かさない）のことを長さ s の巡回置換という．この置換を $(i_1 i_2 \dots i_s)$ で表す．

$$i_1 \longrightarrow i_2 \longrightarrow \cdots \longrightarrow i_s \longrightarrow i_1 \tag{114}$$

ただし，$(i_1 i_2 \dots i_s)$ の数字を順繰りに入れ替えた記号は同じ巡回置換を表す．たとえば $(235) = (352) = (523)$ である．

一般に S_n の元は互いに異なる文字を用いた巡回置換たちの積で表される．たとえば，

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 6 & 4 & 2 & 3 & 8 & 7 \end{pmatrix} = (152)(36)(78)(4) \tag{115}$$

のようにかける．このような分解を巡回置換分解（サイクル分解）という．巡回置換分解は，積の順序を除いて一意的である．置換を巡回置換分解したとき，各巡回置換の長さを大きい順に並べたものをその置換の型（巡回置換型）という．この例では $(3, 2, 2, 1)$ になる．

.....

(T24) S_n の 2 元が互いに共役であるための必要十分条件は，それらが同じ型を持つことである．すなわち，S_n の各共役類は，同じ型の置換全体からなる．

.....

($\because$) $\sigma \in S_n$ に対して，ある $\tau \in S_n$ によって $\tau\sigma\tau^{-1}$ を計算することは，σ の表示において 1 行と 2 行の数字を同じ仕方で入れ替えてしまうことである．したがって σ と $\tau\sigma\tau^{-1}$ の型は同じになる．すなわち，

$$\begin{aligned} &\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix} \quad \text{のとき,} \\ &\tau\sigma\tau^{-1} = \begin{pmatrix} j_1 & j_2 & \cdots & j_n \\ j_{i_1} & j_{i_2} & \cdots & j_{i_n} \end{pmatrix} \end{aligned} \tag{116}$$

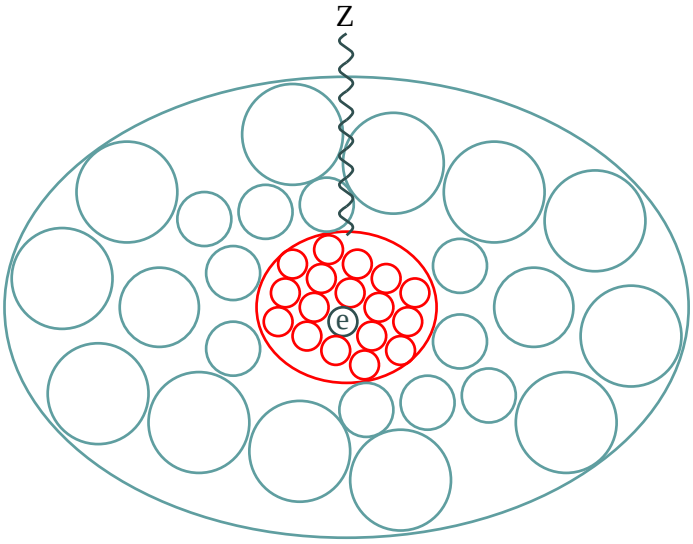
となるので，σ と $\tau\sigma\tau^{-1}$ の型は同じになる．たとえば $\sigma = (152)(36)(78)(4)$ ならば，$\tau\sigma\tau^{-1} = (j_1 j_5 j_2)(j_3 j_6)(j_7 j_8)(j_4)$ となる．

逆に，σ, ρ の型が同じであれば，数字の入れ替えを見て $\rho = \tau\sigma\tau^{-1}$ をみたす τ を見つけることができる． (q.e.d.)

正の整数の列 $(\lambda_1, \lambda_2, \dots, \lambda_r)$ $(\lambda_1 + \lambda_2 + \cdots + \lambda_r = n;\ \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 1)$ を，n の分割という．n の分割の総数を n の分割数といい，$p(n)$ で表す．S_n の元の型は n の分割で表され，逆に n の分割は S_n のある元の型になっている．ゆえに，S_n における可能な型の数は，n の分割数 $p(n)$ に等しい．ここで，S_n の共役類は型の数だけあるから，その数は $p(n)$ に等しい．

次に，一般線形群 $GL(n, \mathbf{C})$ について考えよう．$GL(n, \mathbf{C})$ に属する行列 A, B が $B = P^{-1}AP$ の関係にあれば，これらは共役である．特に，A を対角化することは，A と共役な対角行列を見つけることに他ならない．A, B が対角化可能なとき，同じ対角行列（対角成分の順序は違ってよい）に対角化できれば，それらは共役な行列となるが，そうでなければ共役ではない．一般に，$A, B \in GL(n, \mathbf{C})$ が共役であるためには，A, B の

Jordan の標準形が（Jordan 細胞の順序を除いて）一致することが必要十分である．（線形代数ハンドアウト 12–14 章参照）



Z and conjugacy classes

一般に，群 G の中心 Z については，共役類の言葉で次のように記述できる．

(T25) 群 G の中心 Z はただ 1 つの元からなるすべての共役類たちの結びに等しい．

($\because$)

$$\begin{aligned} x \in Z \quad &\iff xg = gx \quad (g \in G) \iff gxg^{-1} = x \quad (g \in G) \\ &\iff \mathrm{Cl}(x) = \{x\}. \qquad \text{(q.e.d.)} \end{aligned} \tag{117}$$

(ex52) (1) S_3 を共役類に分解せよ． (2) S_4，S_5 はいくつの共役類に分解されるか．

(ex53) (1) S_n の中心を求めよ． (2) $GL(n, K)$ の中心を求めよ．（線形代数ハンドアウト 5 章参照） (3) $V_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ は S_4 の正規部分群であることを示せ．

G を有限群とする．G の 2 元以上からなる各共役類の大きさを d_i $(i = 1, \ldots, s)$ とおくとき，次がなりたつ．

$$|G| = |Z| + d_1 + \cdots + d_s \tag{118}$$

この等式を G の類等式という．これは G を共役類に分割し，大きさ 1 の共役類をまとめて中心 Z として元の数を数えれば簡単に得られる．ここで，各 d_i は $|G|$ の約数になることに注意する．より詳しく言うと次の通りである．

(T26) 有限群 G の共役類 $\mathrm{Cl}(x)$ に対して，$|\mathrm{Cl}(x)| = (G : N(x))$ であり，したがって $|\mathrm{Cl}(x)| \mid |G|$ である．

($\because$) $|\mathrm{Cl}(x)| = (G : N(x))$ を示せば後は明らか．$|\mathrm{Cl}(x)|$ を求めるために，gxg^{-1} $(g \in G)$ がどれだけ異なる値を持つかを考える．$H = N(x) = \{h \in G \mid hxh^{-1} = x\}$ とおく．$h \in H$ に対しては，$hxh^{-1} = x$．次に，左剰余類 gH に対して，$gh \in gH$ な

らば $(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = gxg^{-1}$．ここで，$gxg^{-1} = g'xg'^{-1}$ とすると，$g'^{-1}gxg^{-1}g' = (g'^{-1}g)x(g'^{-1}g)^{-1} = x$ なので，$g'^{-1}g \in H$． $\therefore\ g \in g'H$． $\therefore\ gH = g'H$．対偶を取ると，$gH \neq g'H \Rightarrow gxg^{-1} \neq g'xg'^{-1}$ を得る．ゆえに，gxg^{-1} は丁度左剰余類 gH の数だけ異なる値を持つ．その数はすなわち H の指数である． (q.e.d.)

この定理は形式的に次のように拡張される．S を G の部分集合とし，$\mathrm{Cl}(S)$ を S と共役な部分集合からなる共役類，すなわち

$$\mathrm{Cl}(S) = \{gSg^{-1} \mid g \in G\} \tag{119}$$

とおくとき，次がなりたつ．

(T26') 有限群 G の部分集合 S に対して，$|\mathrm{Cl}(S)| = (G : N(S))$，$|\mathrm{Cl}(S)| \mid |G|$．

($\because$) (T26) の証明で，x を S に置き換えればよい． (q.e.d.)

ここで，対称群の類等式を考えよう．n の分割全体の集合を $\mathscr{P}(n)$ で表す．$\lambda = (\lambda_1, \ldots, \lambda_r) \in \mathscr{P}(n)$ とするとき，λ の成分 $\lambda_1, \ldots, \lambda_r$ の中で i に等しいものの個数を m_i とかく．このとき，$\lambda = (1^{m_1}, 2^{m_2}, \ldots)$ のようにも表す．ここで，n 次対称群の共役類のうち，型が λ の置換からなるものを Cl_λ で表すことにする．$n \neq 2$ のとき $Z(S_n) = \{e\}$ であることに注意すると，S_n $(n \neq 2)$ の類等式は次のようになる．

$$n! = 1 + \sum_{\lambda \in \mathscr{P}(n),\, \lambda \neq (1^n)} |\mathrm{Cl}_\lambda| \tag{120}$$

さらに Cl_λ の大きさを考える．これは $\{1, 2, \ldots, n\}$ を，各細胞の大きさが λ_i になるように分割し，各細胞ごとに円順列を作る方法の数なので，

$$|\mathrm{Cl}_\lambda| = \frac{n!}{\lambda_1\lambda_2 \ldots \lambda_r \cdot m_1!m_2! \ldots m_{\lambda_1}!} \tag{121}$$

とかける．

(ex54) $n = 1, \ldots, 5$ とする．(1) S_n の類等式を求めよ． (2) A_n の類等式を求めよ．

(ex55) 位数が素数 p の正整数ベキである群を，p-群という．類等式を用いて，p-群の中心 Z について $Z \neq \{e\}$ であることを示せ．

13.（自己同型群）群 G から G への同型写像を G の 自己同型 (写像) という．G のすべての自己同型からなる集合は，自己同型の 合成 に関して群をなす．この群を G の 自己同型群 といい，$\mathrm{Aut}(G)$ で表す．以下，$\mathrm{Aut}(G)$ が群であることを示す．

(∵) (T10') より，自己同型の合成はまた自己同型になり，(10) でみたように，自己同型は合成に関して結合律をみたす．単位元は恒等写像 id であり，自己同型 ϕ の逆元は逆写像 ϕ^{-1} である． (q.e.d.)

特に，$g \in G$ に対して，

$$A_g(x) = gxg^{-1} \qquad (x \in G) \tag{122}$$

で定められる自己同型 A_g を G の 内部自己同型 という．内部自己同型でない自己同型を 外部自己同型 という．G の内部自己同型全体 $\mathrm{Inn}(G)$ は合成に関して $\mathrm{Aut}(G)$ の部分群をなす．これを G の 内部自己同型群 という．G の内部自己同型は，G の各共役類からそれ自身への 1 対 1 対応になっている．内部自己同型は次をみたす．

$$\begin{array}{l} A_g \circ A_{g'} = A_{gg'} \\ (A_g)^{-1} = A_{g^{-1}} \\ A_e = \mathrm{id} \end{array} \tag{123}$$

(ex56) (1) (123) を示せ． (2) A_g が自己同型であることを示せ． (3) $\mathrm{Inn}(G)$ が $\mathrm{Aut}(G)$ の部分群をなすことを示せ．

(∵) (1) 第 1 式を示す．

$$\begin{array}{l} A_g \circ A_{g'}(x) = g(g'xg'^{-1})g^{-1} = gg'x(gg')^{-1} = A_{gg'}(x). \qquad (x \in G) \\ \therefore\ A_g \circ A_{g'} = A_{gg'}. \qquad \text{(q.e.d.)} \end{array} \tag{124}$$

(∵) (2) 任意の $x, y \in G$ に対して，

$$A_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = A_g(x)A_g(y) \tag{125}$$

がなりたつので，A_g は G から G への準同型である．さらに任意の $x \in G$ に対して，$g^{-1}xg \in G$ を取ると，$A_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x$ となるので A_g は全射．また $A_g(x) = A_g(y)$ とすると，$gxg^{-1} = gyg^{-1}$． $\therefore\ x = y$．ゆえに A_g は単射．それゆえ A_g は 1 対 1 対応．よって A_g は自己同型である． (q.e.d.)

(∵) (3) (2) より，$\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$ である．$\mathrm{Inn}(G)$ の任意の元 A_g，$A_{g'}$ を取る．(123) より，

$$A_g \circ (A_{g'})^{-1} = A_g \circ A_{g'^{-1}} = A_{gg'^{-1}} \in \mathrm{Inn}(G). \tag{126}$$

ゆえに，$\mathrm{Inn}(G)$ は $\mathrm{Aut}(G)$ の部分群である． (q.e.d.)

(ex57) G から G への写像 L_g，R_g を

$$\begin{array}{ll} L_g(x) = gx & (x \in G) \\ R_g(x) = xg^{-1} & (x \in G) \end{array} \tag{127}$$

で定める．これらは 1 対 1 対応であるが，$g \neq e$ のとき自己同型ではないことを示せ．

(ex58) $n \geq 2$ のとき，L_g または R_g を用いて，$(S_n : A_n) = 2$ を示せ．（このこと自体は，(T16)(iv) よりすでに明らかである．）

($\because$) 互換 g を 1 つ取る．S_n の変換 L_g を考える．$S_n - A_n = O_n$ とおく．L_g によって，A_n は O_n に移り，O_n は A_n に移る．なぜならば，偶置換 σ に対して，$L_g(\sigma) = g\sigma$ は奇置換になり，奇置換 τ に対して，$L_g(\tau) = g\tau$ は偶置換になるから．そこで，$L_g : A_n \longrightarrow O_n$ を考えると，$L_g \circ L_g = \mathrm{id}$ となっているのでこれは 1 対 1 対応である． $\therefore\ |A_n| = |O_n|$. $\therefore\ (S_n : A_n) = 2$. (q.e.d.)

. . . . . .

(T27) (Goursat の補題) 群 G に対して，

$$\mathrm{Aut}(G) \triangleright \mathrm{Inn}(G). \tag{128}$$

. . . . . .

($\because$) $\mathrm{Inn}(G)$ が $\mathrm{Aut}(G)$ の部分群であることはすでに見た．$\phi \in \mathrm{Aut}(G)$，$A_g \in \mathrm{Inn}(G)$ とすると，

$$\begin{aligned} \phi \circ A_g \circ \phi^{-1}(x) &= \phi(g\phi^{-1}(x)g^{-1}) = \phi(g)\phi(\phi^{-1}(x))(\phi(g))^{-1} \\ &= \phi(g)x(\phi(g))^{-1} = A_{\phi(g)}(x). \qquad (x \in G) \\ \therefore\ \phi \circ A_g \circ \phi^{-1} &= A_{\phi(g)} \in \mathrm{Inn}(G). \end{aligned} \tag{129}$$

$\therefore\ \mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$. (q.e.d.)

この定理により，剰余群 $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ が得られる．これを 外部自己同型群 といい，$\mathrm{Out}(G)$ で表す．

(ex59) G が可換群ならば，$\mathrm{Inn}(G) = \{\mathrm{id}\}$，$\mathrm{Out}(G) \simeq \mathrm{Aut}(G)$ となることを示せ．

(ex60) (1) 加群 $\mathbf{Z}$ の自己同型群を求めよ．(2) 加群 $\mathbf{Q}$ に対して，$\mathrm{Out}(\mathbf{Q}) \simeq \mathrm{Aut}(\mathbf{Q}) \simeq \mathbf{Q}^\times$ を示せ．

(hint) 自己同型 ϕ で 1 が何に移るかを考えよ．

ここで，準同型定理を用いて $\mathrm{Inn}(G)$ の構造を調べると，次の定理を得る．

. . . . . .

(T28) Z を G の中心とするとき，

$$\mathrm{Inn}(G) \simeq G/Z. \tag{130}$$

. . . . . .

($\because$) G から $\mathrm{Inn}(G)$ への準同型 ϕ を，

$$\phi(g) = A_g \tag{131}$$

で定めることができる．実際，$g, g' \in G$ に対して，(123) より，

$$\phi(gg') = A_{gg'} = A_g \circ A_{g'} = \phi(g) \circ \phi(g'). \tag{132}$$

さらに ϕ は明らかに全準同型である．次に $\mathrm{Ker}\,\phi$ を求める．

$$\begin{aligned} \phi(g) = A_g = \mathrm{id} \quad &\Longleftrightarrow\ gxg^{-1} = x \quad (x \in G) \\ &\Longleftrightarrow\ gx = xg \quad (x \in G) \\ &\Longleftrightarrow\ g \in Z \end{aligned} \tag{133}$$

ゆえに，$\mathrm{Ker}\,\phi = Z$．そこで ϕ に準同型定理を適用して，$G/Z \simeq \mathrm{Inn}(G)$ を得る． (q.e.d.)

(ex61) $n \neq 2$ のとき，$\mathrm{Inn}(S_n) \simeq S_n$ を示せ．また，$\mathrm{Inn}(S_2) \simeq \{e\}$ を示せ．

(hint) Z を求めよ．

（参考）対称群の自己同型については興味深いことが知られている．$n \neq 6$ のとき，S_n には外部自己同型が存在せず，したがって，$\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$，$\mathrm{Out}(S_n) = \{e\}$ であるが，S_6 には外部自己同型が存在し，$\mathrm{Out}(S_6) \simeq C_2$ がなりたつ．これは，S_6 の自己同型の半分が内部自己同型，残り半分が外部自己同型であることを意味する．その外部自己同型の 1 つを ϕ とおけば，他の外部自己同型は $\phi \circ A_\sigma$（あるいは $A_\sigma \circ \phi$）$(\sigma \in S_6)$ の形で表される．S_n において，ある 1 つの数字 i を動かさない元の集合は S_{n-1} と同型な部分群になる．その部分群は全部で n 個あり，互いに共役で，内部自己同型で互いに移り合う．ところが S_6 にはそのような 6 個の共役な部分群からなる共役類以外に，それらとは共役でない S_5 と同型な 6 個の部分群が別の共役類をなしており，S_6 の外部自己同型はその 2 つの共役類の間の 1 対 1 対応を与える．