

鈴木群論 解答

ゆじ

2021 年 8 月 21 日

第 1 章

基礎の概念

1.1 群の定義とその例

問題 1.1.1. G を結合法則を満たす積の定義された集合とする。ある元 $e \in G$ が存在し、次の二条件を満たしているとき、 G は群であることを示せ：


- (i) $\forall g \in G, ge = g.$
- (ii) $\forall g \in G, \exists h \in G, gh = e.$

Proof. $g \in G$ をとる。 $gh = e$ となる h をとり、 $hg' = e$ となる g' をとると、

$$hg = hge = hg(hg') = (h(gh))g' = (he)g' = hg' = e$$


となって $hg = e$ がわかる。また、 $hg = e$ より、

$$eg = (gh)g = g(hg) = ge = g$$

がわかる。よって e は両側単位元で h は g の両側逆元となる。以上で解答を完了する。 

問題 1.1.2. G を結合法則を満たす積の定義された集合とする。ある元 $e \in G$ が存在して、次の二条件を満たしているとき、 G は群であるか？：

- (i) $\forall g \in G, eg = g.$
- (ii) $\forall g \in G, \exists h \in G, gh = e.$

Proof. 群ではない。 H を群、 $a \stackrel{\text{def}}{=} H$ として、 $G \stackrel{\text{def}}{=} H \cup \{a\}$ に演算 $*$ を次で定める： $g_1, g_2 \in H$ なら H の演算で $g_1 * g_2 \stackrel{\text{def}}{=} g_1 g_2 \in H$ とする。 $g \in H$ と a に対しては $a * g = g * a \stackrel{\text{def}}{=} g$ とする。 $a * a = a$ とする。すると、 H の単位元を $e \in H \subset G$ とすることで、 G は群とはならないが与えられた二つの条件を満たす集合となる。以上で証明を完了する。 

注意. 結合法則を満たす積の定義された集合 G が次の二条件を満たしているとき群となる：

- (i) $\forall g \in G, eg = g$ となる元 $e \in G$ がただ一つ存在する。
- (ii) $\forall g \in G, \exists h \in G, gh = e.$

これを示す。

まず、元 $u \in G$ が $ue = e$ を満たすとする。このとき、任意の $g \in G$ に対して

$$ug = u(eg) = (ue)g = eg = g$$

となるので、 e の唯一性から $u = e$ が従う。

次に、 $g \in G$ を任意に取る。 $g' \stackrel{\text{def}}{=} ge$ において、 $g'h = e$ となる $h \in G$ をとり、さらに $hh' = e$ となる $h' \in G$ をとる。すると、

$$(hg)e = hghh' = hg(eh)h' = h((ge)h)h' = h(g'h)h' = heh' = hh' = e$$

が成り立つ。よって $hg = e$ となる。ここで

$$ge = gee = g'e = g'hg = eg = g$$

なので、 e は

$$\forall g \in G, ge = g$$

を満たす。よって、上の演習問題を使えば、 G は群であることが従う。

1.2 部分群

問題 1.2.1. 群 G の空でない部分集合 $H \subset G$ が部分群であるためには次が必要十分であることを示せ：

$$\forall g, h \in H, gh^{-1} \in H.$$

Proof. 必要性は、 $g, h \in H$ に対して $g, h^{-1} \in H$ であるので $gh^{-1} \in H$ となることから従う。

十分性を示す。 $g \in H$ をとる (H は空ではないので一つは元がある)。すると

$$e = gg^{-1} \in H$$

となる。よって $e \in H$ が成り立つ。次に $e \in H$ と任意の元 $g \in H$ に対して条件を使えば、

$$g^{-1} = eg^{-1} \in H$$

が成り立つ。さらに任意の $g, h \in H$ に対して、 $h^{-1} \in H$ なので、

$$gh = g(h^{-1})^{-1} \in H$$


が成り立つ。以上より H は部分群となる。



問題 1.2.2.


- (i) 有限群 G の空でない部分集合 $H \subset G$ が部分群であるためには、 $\forall g, h \in H, gh \in H$ であることだけで十分である。
- (ii) 群 G のすべての元の位数が有限であるとする。このとき、空でない部分集合 $H \subset G$ が部分群であるためには、 $\forall g, h \in H, gh \in H$ であることだけで十分である。
- (iii) 群 G の空でない部分集合 $H \subset G$ が部分群であるためには、一般には $\forall g, h \in H, gh \in H$ であることだけでは不十分である。例を挙げなさい。

Proof. 有限群ならすべての元の位数は有限なので (1) は (2) より従う。(2) を示す。 $g \in H$ と任意の $n > 0$ に対して、条件より帰納的に $g^n \in H$ が成り立つ。すべての元の位数が有限であることから、ある $n > 0$ に対して $g^n \in H$ が成り立ち、このとき $g^{-1} = g^{n-1} \in H$ が成り立つ。以上で H は部分群となる。

(3) の例はたとえば $\mathbb{N} \subset \mathbb{Z}$ など。以上で解答を完了する。 

問題 1.2.3. 加法に関する群 \mathbb{Q} は極大部分群を持たないことを示せ。

Proof. $A \subsetneq \mathbb{Q}$ を極大部分群とする。まず、 A と $\mathbb{Z} \subset \mathbb{Q}$ で生成される部分群が \mathbb{Q} となるとする。任意の $r \in \mathbb{Q}$ に対してある $a \in \mathbb{N}_{\geq 0}$ とある $n \in \mathbb{Z}, m \in A$ が存在して $r = -n + am$ が成り立つので、 $n + r \in A$ が成り立つ。とくに、 $k \in \mathbb{N}_{>0}$ に対して、ある $n \in \mathbb{Z}$ が存在して $n + 1/k \in A$ が成り立つ。よって $kn + 1 \in A$ が成り立つ。同様に、ある $n' \in \mathbb{Z}$ が存在して $n' + 1/(kn + 1) \in A$ が成り立つので、とくに $n'(kn + 1) + 1 \in A$ が成り立つ。ここで $n'(kn + 1) \in A$ なので、 $1 \in A$ が成り立つ。従って $\mathbb{Z} \subset A$ となって、 $A = \mathbb{Q}$ が従う。これは $A \neq \mathbb{Q}$ に反する。以上より、 A と \mathbb{Z} で生成される部分群は \mathbb{Q} とは異なる。 A の極大性より、 $\mathbb{Z} \subset A$ が従う。

次に、 $1/n \notin A$ となる最小の $n \in \mathbb{N}_{>0}$ をとる (任意の $k \in \mathbb{N}_{>0}$ に対して $1/k \in A$ となるとすると、任意の $m \in \mathbb{Z}, k \in \mathbb{N}_{>0}$ に対して $m/k \in A$ が成り立つことが従い、これは $A \neq \mathbb{Q}$ に反するので、このような n の存在がわかる)。このとき、 $1/n^2 \notin A$ となる。 A と $1/n$ で生成される部分群を A' とおく。 $1/n^2 \in A'$ と仮定すると、ある $a, b \in \mathbb{Z}, m \in A$ が存在して、 $1/n^2 = a/n + bm$ が成り立つ。よって $1/n = a + bmn \in \mathbb{Z} + A = A$ が成り立つ。これは $1/n \notin A$ に矛盾する。よって $1/n^2 \notin A'$ が従い、とくに $A' \neq \mathbb{Q}$ である。ここで $1/n \in A' \setminus A$ であるから、 $A \subsetneq A'$ である。これは A の極大性に反する。よって極大部分群 $A \subset \mathbb{Q}$ が存在しないことが示された。以上で解答を完了する。 


問題 1.2.4. G を群、 $X \subset G$ を $e \notin X$ となる部分集合とする。

$$\mathcal{H} \stackrel{\text{def}}{=} \{H \subset G \mid H \text{ は部分群で、} H \cap X = \emptyset\}$$


に包含関係で順序を入れるとき、 \mathcal{H} には極大元が存在することを示せ。また、 $H_0 \cap X = \emptyset$ となる H_0 を一つとって、

$$\mathcal{H}_0 \stackrel{\text{def}}{=} \{H \in \mathcal{H} \mid H_0 \subset H\}$$

とおくとき、 \mathcal{H}_0 にも極大元が存在する。


Proof. 前半は $H_0 = \{e\}$ とすることで後半より従うので、後半のみ示せば良い。 $\{H_i\}_{i \in I} \subset \mathcal{H}_0$ を全順序部分集合とする。 $H \stackrel{\text{def}}{=} \bigcup_{i \in I} H_i$ と定めると、これは群となる。さらに $H \cap X = \bigcup_{i \in I} (H_i \cap X) = \emptyset$ であるから、 $H \in \mathcal{H}_0$ である。従って Zorn の補題より主張が従う。以上で解答を完了する。 

問題 1.2.5. G を群、 $H \subsetneq G$ を真の部分群、 $S \subset G$ を有限集合とし、 $H, S = G$ と仮定する。このとき、 H を含む極大部分群が存在する。とくに、有限個の元で生成された群 G には極大部分群が存在する。


Proof. $H, T = G$ となる $T \subset S$ のうち元の数が最小のものを一つとる。 T の元の数の最小性から、 $H_0 \stackrel{\text{def}}{=} H, T \setminus \{t\} \neq G$ である。また、 $H_0, t = H, T = G$ であるから、 $t \notin H_0$ である。前問より、 H_0 を含み、 t を含まない部分群のうち極大なもの H' が存在する。 H' が極大部分群であることを示す。 $H' \subsetneq H_1 \subset G$ となる部分群 H_1 を任意にとる。このとき、 $H_0 \subset H' \subsetneq H_1$ と H' の極大性から、 $t \in H_1$ が成り立つ。よって $G = H_0, t \subset H_1$ が成り立ち、 $H_1 = G$ となるので、 H' は極大部分群である。以上で解答を完了する。 

1.3 剰余類

問題 1.3.1. $[\mathbb{Z} : k\mathbb{Z}] = k$ であり、 $0, 1, \dots, k-1$ は $k\mathbb{Z}$ に関する剰余類の代表系となる。

Proof. さすがに自明でいいよね。 

問題 1.3.2. 両側剰余類 HxK に入る K に関する右剰余類の数を求めよ。

Proof. $h_1xK = h_2xK \iff (h_2x)^{-1}h_1x = x^{-1}h_2^{-1}h_1x \in K \iff h_2^{-1}h_1 \in xKx^{-1}$ なのによって求める数は $[H : H \cap xKx^{-1}]$ である。 

問題 1.3.3.

(i) $H \subset G$ が有限部分群で $x \in G$ であれば、 HxH に含まれる H の左剰余類の数は HxH に含まれる H の右剰余類の数と等しい。これを示せ。

(ii) 群 G と部分群 $H \subset G$ を

$$G \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \mid r, s \in \mathbb{Q}, r \neq 0 \right\},$$

$$H \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \mid m \in \mathbb{Z} \right\} \subset G,$$

で定義する。自然数 $n \in \mathbb{N}$ に対し、

$$x \stackrel{\text{def}}{=} \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \in G$$

と定める。このとき、両側剰余類 HxH に含まれる H の左剰余類および右剰余類の数を求めよ。

Proof. (1) を示す。共役をとることで全単射 $H \cap x^{-1}Hx \xrightarrow{\sim} H \cap xHx^{-1}$ が得られるので、 $\#(H) < \infty$ であることから、

$$[H : H \cap x^{-1}Hx] = \#(H) / \#(H \cap x^{-1}Hx) = \#(H) / \#(H \cap xHx^{-1}) = [H : H \cap xHx^{-1}]$$


が従う。以上で (1) の解答を完了する。

(2) を示す。計算すれば、


$$HxH = \left\{ \begin{pmatrix} n & nm + m' \\ 0 & 1 \end{pmatrix} \mid m, m' \in \mathbb{Z} \right\},$$

$$Hx = \left\{ \begin{pmatrix} n & m \\ 0 & 1 \end{pmatrix} \mid m \in \mathbb{Z} \right\},$$

$$xH = \left\{ \begin{pmatrix} n & nm \\ 0 & 1 \end{pmatrix} \mid m \in \mathbb{Z} \right\},$$

となる。よって、左剰余類の数は 1 個、右剰余類の数は n 個である。 

問題 1.3.4. G を有限群、 $H \subsetneq G$ を真の部分群とすれば、 H のどの元とも共役ではない G の元が存在する。

Proof. H と共役な部分集合の数は $l \stackrel{\text{def}}{=} [G : N_G(H)]$ である。 H のある元と共役な G の元の集合は $S \stackrel{\text{def}}{=} \bigcup_{g \in N_G(H) \setminus G} g^{-1}Hg$ と表されるが、 $1 \in H \cap g^{-1}Hg \neq \emptyset$ であるから、 $\#(S) < \#(H)l \leq \#(G)$ となる。以上で証明を完了する。 

問題 1.3.5. 群 G の空でない部分集合 H が部分群であるための必要十分条件は $HH \subset H, H^{-1} \subset H$ が成り立つことである。これを示しなさい。また、このとき常に等号が成立することを示しなさい。

Proof. さすがに自明でいいと思う。 

問題 1.3.6. G を、平面の中に与えられた正 n 角形 R_n を保つ平面の合同返還のなす群 (=二面体群 D_{2n}) とする。 R_n の隣り合う頂点 $P, Q \in R_n$ を一つとり、頂点 $P \in R_n$ を通る内角の二等分線に関する対称変換を σ 、辺 PQ の垂直二等分線に関する対称変換を τ とする。 $S \stackrel{\text{def}}{=} \sigma, T \stackrel{\text{def}}{=} \tau$ とする。

(i) $\#(S) = \#(T) = 2$ を示せ。


(ii) もし n が奇数なら ST は部分群にならない。これを示せ。

(iii) 積 $\tau\sigma$ は R_n の中心周りの位数 n の回転であって、 P を Q に写す。これを示せ。

(iv) n が偶数でも ST は部分群にならない。これを示せ。

Proof. (1) は自明。(2) を示す。 $ST = \{1, \sigma, \tau, \tau\sigma\}$ なので ST は 4 元集合である。よってもし ST が G の部分群であれば、 $\#(G) = 2n$ は 4 で割り切れなければならない。しかし n は奇数なのでこれはあり得ない。

(3) を示す。まず $\tau(\sigma(P)) = \tau(P) = Q$ である。次に $\sigma(Q) \neq Q$ であるから $\tau(\sigma(Q)) \neq \tau(Q) = P$ である。これは回転しかあり得ない。 P, Q は隣り合っているので、 $\tau\sigma$ は位数 n である。

(4) を示す。 ST が部分群であれば、 $\tau\sigma$ は位数 2 でなければならないが、 $n \geq 3$ なのでこれは (3) に反する。以上で解答を完了する。 

問題 1.3.7. G を群、 $H, K \subset G$ を部分群として、 $G = HK$ であると仮定する。このとき、任意の $x, y \in G$ に対し $G = H^x K^y$ であり、さらにある $z \in G$ が存在して $H^x = H^z, K^y = K^z$ が成り立つことを示しなさい。

Proof. $x, y \in G$ を任意にとる。まず $x = hk$ となる $h \in H, k \in K$ をとると、


$$G = G^k = H^k K^k = H^{hk} K = H^x K$$

が成り立つ。次に $y^{-1} = h'k'$ となる $h' \in H^x, k' \in K$ をとると、 $y = k'^{-1}h'^{-1}$ となるので、

$$G = G^{h'^{-1}} = (H^x)^{h'^{-1}} K^{h'^{-1}} = H^x K^{h'^{-1}} = H^x K^y$$

が成り立つ。以上で一つ目の主張が示された。二つ目は、 $z \stackrel{\text{def}}{=} kh'^{-1}$ とおくと、 $h' \in H^x, x = kh, y = k'^{-1}h'^{-1}$ なので、

$$\begin{aligned} H^z &= H^{kh'^{-1}} = (H^k)^{h'^{-1}} = (H^x)^{h'^{-1}} = H^x, \\ K^z &= K^{kh'^{-1}} = K^{h'^{-1}} = K^y, \end{aligned}$$

が成り立つ。以上で解答を完了する。 

1.4 正規部分群、剰余群

問題 1.4.1.

(i) 群 G の部分群 H が正規部分群であるための必要十分条件は、任意の $x \in G$ に対して $x^{-1}Hx \subset H$ となることである。これを示せ。

- (ii) 群 G と部分群 H と元 $y \in G$ であって、 $y^{-1}Hy \subset H$ であるが $y \notin N_G(H)$ となる例を挙げよ。また、部分集合 $\{y \in G | y^{-1}Hy \subset H\}$ は群とは限らない。そのような例を挙げよ。

Proof. (1) は自明なので (2) を示す。問題 1.3.3 (ii) の G, H, x を考える。

$$y \stackrel{\text{def}}{=} x^{-1} = \begin{pmatrix} 1/n & 0 \\ 0 & 1 \end{pmatrix}$$

とする。


$$\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/n & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} n & mn \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/n & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & nm \\ 0 & 1 \end{pmatrix}$$

なので、 $H^y = y^{-1}Hy = xHx^{-1} \subsetneq H$ となる。とくに $H^y \neq H$ なので $y \notin N_G(H)$ となる。次に、 $g^{-1}Hg \subset H$ となるための $g \in G$ の条件を求める。任意の $m \in \mathbb{Z}$ に対して


$$\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1/r & -s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r & s+m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (s+m)/r - s \\ 0 & 1 \end{pmatrix} \in H$$

となると仮定して $r \in \mathbb{Q} \setminus \{0\}, s \in \mathbb{Q}$ を求める。つまり、 $\forall m \in \mathbb{Z}, (s+m)/r - s \in \mathbb{Z}$ と仮定する。さらに $s \neq 0$ と仮定する。 $m=0$ とすれば、 $k \stackrel{\text{def}}{=} s/r - s \in \mathbb{Z}$ となる。よって $r = (s+k)/s$ であり、任意の $m \in \mathbb{Z}$ に対して $(s+m)s/(s+k) - s = (m-k)s/(s+k) \in \mathbb{Z}$ が成り立つ。すなわち、任意の $m \in \mathbb{Z}$ に対して $ms/(s+k) \in \mathbb{Z}$ が成り立つ。違いに素な整数 $a, b \neq 0$ を用いて $s = a/b$ と表せば、任意の $m \in \mathbb{Z}$ に対して $ms/(s+k) = am/(a+kb) \in \mathbb{Z}$ が成り立つ。 a, b は違いに素であるから、 $m=1$ とすれば $a/(a+kb) \notin \mathbb{Z}$ となり、これは仮定に反する。よって $s=0$ である。するとこのとき $1/r \in \mathbb{Z}$ が成り立つ。逆に $s=0, 1/r \in \mathbb{Z}$ であれば任意の $m \in \mathbb{Z}$ に対して $(s+m)/r - s \in \mathbb{Z}$ が成り立つ。従って、

$$\{y \in G | y^{-1}Hy \subset H\} = \left\{ \begin{pmatrix} 1/n & 0 \\ 0 & 1 \end{pmatrix} \middle| n \in \mathbb{Z} \setminus \{0\} \right\}$$

となり、これは群ではない。以上で解答を完了する。 

問題 1.4.2. 部分集合 $S \subset G$ が正規であれば、 S は正規部分群である。これを示せ。

Proof. 本文の定理 2.19 より、任意の $g \in G$ に対して $S^g = S^g = S$ が成り立つので S は正規部分群である。以上で解答を完了する。 

問題 1.4.3.


- (i) 指数 2 の部分群は正規であることを示しなさい。
(ii) G を有限群とし、 $\#(G)$ を割り切る最小の素数を p とするとき、指数 p の部分群は正規であることを示しなさい。


Proof. (1) を示す。 $H \subset G$ が指数 2 の部分群であるとする。 $g \in G$ を任意にとる。 $gH = H \iff g \in H$ があるので、 $gH \neq H \iff g \notin H \iff Hg \neq H$ となるが、このとき $gH = G \setminus H = Hg$ となる。これは H が正規であることを示している。以上で (1) の証明を完了する。

(2) を示す。 p を $\#(G)$ を割り切る最小の素数とし、 $H \subset G$ を指数 p の部分群とする。ヒントに従って、 H が正規でないとは仮定する。すると、 H の共役であって H と異なる部分群 $K \subset G$ が存在する。 K は部分群なので、 $\#(K)$ は $\#(G)$ を割り切る。 p は $\#(G)$ を割り切る最小の素数なので、よって、 p は $\#(K)$ を割り切る

最小の正の自然数である。 $H \neq K$ なので、 $K \neq H \cap K$ である。従って $\#(K)/\#(H \cap K) > 1$ であり、これは p 以上の素因子しか持たないので、とくに $\#(K)/\#(H \cap K) \geq p$ が成り立つ。ここで、

$$p \leq \#(K)/\#(H \cap K) = \#(HK)/\#(H) \leq \#(G)/\#(H) = p$$

となるので、 $\#(HK) = \#(G)$ が従い、よって $HK = G$ が従う。しかしこれは本文命題 (3.15) の系 2 に矛盾する。 H は正規である。以上で解答を完了する。 

(2) の別解答. G は G/H に左から作用する。これによって群準同型 $f: G \rightarrow S_p$ を得る。 $\text{Im}(f)$ は S_p の部分群であり、その位数は $p!$ と $\#(G)$ を割り切るが、 p は $\#(G)$ の最小の素因数であるので、 $\#(\text{Im}(f)) = p$ である。明らかに $H \subset \ker(f)$ であるので、以上より $H = \ker(f)$ が従う。これは H が正規であることを示している。 

問題 1.4.4.

$$Q \stackrel{\text{def}}{=} \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \pm \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} \right\} \subset M_2(\mathbb{C})$$

は行列の掛け算に関して群となる。 Q は位数 2 の部分群をただ一つしか持たず、 Q のすべての部分群は可換な正規部分群となるが、 Q は可換ではない。これを示せ。この Q を **四元数群** という。

Proof.

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


となるので位数 2 の元は単位行列に -1 をかけたものしかない。よって位数 2 の部分群は唯一である。他の真の部分群の位数は 4 であるが、これらは指数 2 であるからどれも正規部分群である。また、

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -\sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}$$


となるので、 Q は非可換群である。以上で解答を完了する。 

1.5 準同型、同型定理

問題 1.5.1. 巡回群の剰余群が巡回群であることを直接示せ。

Proof. G を巡回群とする。ある元 $g \in G$ が存在して、 $G = \{g^n | n \in \mathbb{Z}\}$ が成り立つ。 $N \triangleleft G$ を正規部分群とする。 $G/N = \{g^n N | n \in \mathbb{Z}\}$ であることを証明すれば良いが、 G/N の元はどれも $g' N, g' \in G$ の形で表され、 G の元はどれも g^n の形で表されるので、これは明らかである。 

問題 1.5.2. G を有限群、 $N \triangleleft G$ を正規部分群とする。このとき、 N を通る組成列が存在することを示せ。

Proof. G/N の組成列の一つとり、それを自然な全射 $G \rightarrow G/N$ で G に引き戻し、 N の組成列と繋げれば良い。 

問題 1.5.3. G を群、 $H \subset G$ を部分群とする。 G の部分群の列

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = H$$

であって、各 $i = 0, \dots, r-1$ について $G_i \supset G_{i+1}$ が極大正規部分群であるものが存在するとき、 H を組成部分群と言ひ、上の列を G と H の間の長さ r の組成列、 $\{G_0/G_1, \dots, G_{r-1}/G_r\}$ を組成剰余群列と言ふ。

- (i) H が組成部分群であれば、その組成剰余群列は単純群の集合で、それらの単純群の同型類は順序を除いて一意的であることを示せ。
- (ii) $H \subset G$ が組成部分群で $K \subset H$ が組成部分群であれば $K \subset G$ は組成部分群であることを示せ。
- (iii) $H \subset G$ が組成部分群であり、 $N \triangleleft G$ が極大正規部分群であるとき、 $H \subset N$ であるか、または $H \cap N \triangleleft H$ が極大正規部分群であることを示せ。後者の場合は $H/(H \cap N) \cong G/N$ が成り立つ。
- (iv) $H, K \subset G$ が組成部分群であるとき、 $H \cap K \subset K$ は組成部分群列であることを示せ。とくに $H \cap K \subset G$ は組成部分群列であり、 G と $H \subset K$ の間の組成剰余群列に含まれる単純群は、 G と H の間の組成剰余群列と G と K の間の組成剰余群列の和集合に含まれるある一つの単純群と同型であることを示せ。
- (v) $H, K \subset G$ を組成部分群であって、 $H \subset K$ であると仮定する。 $H \neq K$ なら、 G から K までの組成列の長さは G から H までの組成列の長さより短い。また、 $K \neq G$ なら、 K から H までの組成列の長さは G から H までの組成列の長さより短い。これを示せ。

Proof. (1) は Jordan-Hölder の定理と同様に証明すれば良い。(2) は H と K の間の組成列、 G と H の間の組成列を繋ぐことで従う。(3) を示す。 $H \not\subset N$ とする。組成列

$$H = G_r \triangleleft G_{r-1} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G$$

と一つとれば、組成列

$$H/(H \cap N) = G_r/(G_r \cap N) \triangleleft G_{r-1}/(G_{r-1} \cap N) \triangleleft \dots \triangleleft G_1/(G_1 \cap N) \triangleleft G_0/(G_0 \cap N) = G/N$$

を得る。ここで $H \not\subset N$ であるから、 $H/(H \cap N) \neq \{1\}$ であり、 G/N は単純群であるから、従って

$$H/(H \cap N) \xrightarrow{\sim} G_r/(G_r \cap N) \xrightarrow{\sim} \dots \xrightarrow{\sim} G_1/(G_1 \cap N) \xrightarrow{\sim} G/N$$

が成り立つ。 G/N は単純群であるから、とくに $H \cap N \triangleleft H$ は極大正規部分群である。以上で (3) の証明を完了する。

(4) を示す。 H の組成列

$$H = G_r \triangleleft G_{r-1} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G$$

を一つとる。 $K_i \stackrel{\text{def}}{=} K \cap G_i$ とおけば、(3) より $K_i = K_{i+1}$ であるか、または K_{i+1} は K_i の極大部分群であるかのどちらかが成り立つ。従って、

$$H \cap K = K_r \triangleleft K_{r-1} \triangleleft \dots \triangleleft K_1 \triangleleft K_0 = K$$

は (いくつか重複はあるが) 組成列である。よって $H \cap K$ は K の組成列である。さらに (3) より、 K_i/K_{i+1} は $\{1\}$ であるか、または $\cong G_i/G_{i+1}$ となるので後半も従う。以上で (4) の証明を完了する。

(4) より $H = H \cap K$ は K の組成部分群であるので (5) は明らかである。以上で解答を完了する。 ✍

1.6 自己同型

問題 1.6.1. 群 G が自明な中心を持つ ($Z(G) = \{1\}$) とき、 $C_{\text{Aut}(G)}(\text{Inn}(G)) = \{1\}$ であることを示せ。とくに $Z(\text{Aut}(G)) = \{1\}$ が成り立つ。

Proof. $\sigma \in C_{\text{Aut}(G)}(\text{Inn}(G))$ を任意に取る。このとき、任意の $g \in G$ に対して $\sigma \circ i_g = i_g \circ \sigma$ であるので、任意の $h \in G$ に対して $\sigma(g^{-1}hg) = g^{-1}\sigma(h)g$ が成り立つ。従って、任意の $g, h \in G$ に対して $\sigma(h)(\sigma(g)g^{-1})\sigma(h)^{-1} = \sigma(g)g^{-1}$ が成り立つ。 σ は自己同型であるから、任意の $g, h \in G$ に対して $h(\sigma(g)g^{-1})h^{-1} = \sigma(g)g^{-1}$ が成り立つ。よって任意の $g \in G$ に対して $\sigma(g)g^{-1} \in Z(G) = \{1\}$ が成り立ち、 $\sigma = \text{id}_G$ を得る。以上で解答を完了する。 \pencil

注意 (別解答). $\sigma : G \xrightarrow{\sim} G$ と $g \in G$ に対して $\sigma \circ i_g \circ \sigma = i_{\sigma(g)}$ であるが、左辺は $\text{Aut}(G)$ の群演算では $\sigma^{-1}i_g\sigma = i_{\sigma(i_g)}$ となるので、 $i_{\sigma(i_g)} = i_{\sigma(g)}$ が成り立つ。これは、以下の図式が可換であることを示している：

$$\begin{array}{ccc} G & \xrightarrow{g \mapsto i_g} & \text{Inn}(G) \\ \sigma \downarrow & & \downarrow i_{\sigma}|_{\text{Inn}(G)} \\ G & \xrightarrow{g \mapsto i_g} & \text{Inn}(G). \end{array}$$

もし $Z(G) = \{1\}$ であれば、 $G \xrightarrow{\sim} \text{Inn}(G)$ であるから、 $\text{Aut}(G) \rightarrow \text{Aut}(\text{Inn}(G)), \sigma \mapsto i_{\sigma}|_{\text{Inn}(G)}$ は全単射となる。これは $C_{\text{Aut}(G)}(\text{Inn}(G)) = \{\text{id}_{\text{Aut}(G)}\}$ を意味する。

問題 1.6.2. $Z(G) = \{1\}$ かつ $\text{Inn}(G) \subset \text{Aut}(G)$ が特性部分群であると仮定する。このとき $\text{Aut}(\text{Aut}(G)) = \text{Inn}(\text{Aut}(G))$ である。

Proof. はじめに、任意の $g \in G, \tau \in \text{Aut}(G)$ に対して $\tau \circ i_g = i_{\tau(g)} \circ \tau$ が成り立つことに注意しておく。

同型射 $\phi : \text{Aut}(G) \xrightarrow{\sim} \text{Aut}(G)$ を任意にとる。 $Z(G) = \{1\}$ なので $G \xrightarrow{\sim} \text{Inn}(G)$ である。また、 $\text{Inn}(G) \subset \text{Aut}(G)$ は特性部分群であるから、 ϕ は G の自己同型 $\alpha : G \xrightarrow{\sim} G$ を引き起こして、以下の図式を可換にする：

$$\begin{array}{ccc} G & \xrightarrow{g \mapsto i_g} & \text{Aut}(G) \\ \alpha \downarrow \cong & & \downarrow \cong \phi \\ G & \xrightarrow{g \mapsto i_g} & \text{Aut}(G). \end{array}$$

ここで、

$$\phi \circ i_g \circ \phi^{-1} = i_{\phi(i_g)} = i_{i_{\alpha(g)}} = i_{i_{\alpha}^{-1}(i_g)} = i_{\alpha}^{-1} \circ i_{i_g} \circ i_{\alpha}$$

が成り立つので、よって $i_{\alpha} \circ \phi \in C \stackrel{\text{def}}{=} C_{\text{Aut}(\text{Aut}(G))}(\text{Inn}(\text{Inn}(G)))$ となる。

解答を完了するために、 $C = \{\text{id}_{\text{Aut}(G)}\}$ を示す。任意に $\psi \in C, \sigma \in \text{Aut}(G), g \in G$ をとる。すると

$$\begin{aligned} i_{\psi(\sigma) \circ i_g} &= i_{\psi(\sigma)} \circ i_{i_g} = \psi \circ i_{\sigma} \circ \psi^{-1} \circ i_{i_g} \stackrel{\star}{=} \psi \circ i_{\sigma} \circ i_{i_g} \circ \psi^{-1} \\ &= \psi \circ i_{\sigma \circ i_g} \circ \psi^{-1} = \psi \circ i_{i_{\sigma(g)} \circ \sigma} \circ \psi^{-1} = \psi \circ i_{i_{\sigma(g)}} \circ i_{\sigma} \circ \psi^{-1} \\ &\stackrel{\star}{=} i_{i_{\sigma(g)}} \circ \psi \circ i_{\sigma} \circ \psi^{-1} = i_{i_{\sigma(g)}} \circ i_{\psi(\sigma)} = i_{i_{\sigma(g)} \circ \psi(\sigma)} \end{aligned}$$

となる。ここで \star の箇所で $\psi \in C$ を使った。 $Z(G) = \{1\}$ と前問より $Z(\text{Aut}(G)) = \{\text{id}_G\}$ なので、内部自己同型をとる射 $\text{Aut}(G) \rightarrow \text{Aut}(\text{Aut}(G))$ は単射であり、よって任意の $g \in G$ に対して $\psi(\sigma) \circ i_g = i_{\sigma(g)} \circ \psi(\sigma)$ が成り立つ。従って、

$$i_{\psi(\sigma)(g)} \circ \psi(\sigma) = \psi(\sigma) \circ i_g = i_{\sigma(g)} \circ \psi(\sigma)$$

となる。右から $\psi(\sigma)^{-1}$ を合成して再び $Z(G) = \{1\}$ を用いることで、任意の $g \in G$ に対して $\psi(\sigma)(g) = \sigma(g)$ が成り立つ。これは $\psi(\sigma) = \sigma$ を示している。よって $\psi = \text{id}_{\text{Aut}(G)}$ となり、 $C = \{\text{id}_{\text{Aut}(G)}\}$ が従う。以上で解答を完了する。 \pencil

注意 (別解答). $A \stackrel{\text{def}}{=} \text{Aut}(\text{Aut}(G)), B \stackrel{\text{def}}{=} \text{Inn}(\text{Aut}(G)), I \stackrel{\text{def}}{=} \text{Inn}(\text{Inn}(G))$ とおく。 $Z(G) = \{1\}$ より $Z(\text{Aut}(G)) = \{\text{id}_G\}$ であり、前問より $A \xrightarrow{\sim} \text{Aut}(B), \text{Aut}(G) \cong B, I \cong G$ となる。すると

$$\begin{array}{ccccccc} 1 & \longrightarrow & C_A(I) & \longrightarrow & N_A(I) & \longrightarrow & [\text{Aut}(I) \cong \text{Aut}(G)] \\ & & \downarrow & & \downarrow & & \downarrow \sigma \mapsto i_\sigma \\ 1 & \longrightarrow & C_A(B) & \longrightarrow & A & \xrightarrow{\cong} & [\text{Aut}(B) \cong \text{Aut}(\text{Aut}(G))] \end{array}$$

という可換図式ができて、 $C_A(I) \subset C_A(B) = \{1\}$ が従う。これは上の証明の後半で示していることである。この部分の証明に $\text{Inn}(G) \subset \text{Aut}(G)$ が特性部分群であることは必要ない。

$\sigma \in \text{Aut}(G)$ と $g \in G$ に対して

$$i_\sigma(i_g) = \sigma^{-1} i_g \sigma = \sigma \circ i_g \circ \sigma^{-1} = i_{\sigma(g)}$$

であるから、 $i_\sigma^{-1} i_g i_\sigma = i_{i_\sigma(i_g)} = i_{i_{\sigma(g)}}$ となって $B = \text{Inn}(\text{Aut}(G)) \subset N_A(I)$ が従う。このことは $N_A(I) \rightarrow \text{Aut}(I)$ が全射であることを意味する。よって以下において \Leftarrow 側が成り立つことがわかる (\Rightarrow 側は上の図式の可換性より従う)：

$$N_A(I) = A \iff \text{Inn}(\text{Aut}(G)) = \text{Aut}(\text{Aut}(G)).$$

さらに、任意の $\phi \in A$ と $g \in G$ に対して $i_{\phi(i_g)} = \phi \circ i_g \circ \phi^{-1}$ であるから、以下が成り立つ：

$$\text{Inn}(G) \text{ char } \text{Aut}(G) \iff N_A(I) = A$$

結局、 $\text{Inn}(\text{Aut}(G)) = \text{Aut}(\text{Aut}(G))$ であることは $\text{Inn}(G) \subset \text{Aut}(G)$ が特性部分群であることと同値であることがわかる。


注意. 上の注意の記号のもと、 $B = N_A(I)$ である。 $B \subset N_A(I)$ は任意の $\sigma \in \text{Aut}(G), g \in G$ に対して $i_\sigma(i_g) = i_{\sigma(g)}$ となることから明らかである。逆に $\phi \in N_A(I)$ とすると、任意の $g \in G$ に対して $i_{\phi(i_g)} = \phi \circ i_g \circ \phi^{-1} \in I$ となることから $\phi(i_g) \in \text{Inn}(G)$ が成り立つ。ここで $\phi(i_g) = i_{\sigma_\phi(g)}$ となる $\sigma_\phi(g) \in G$ をとれば、写像 $\sigma_\phi : G \rightarrow G$ は群準同型であり、群準同型 $N_A(I) \rightarrow B, \phi \mapsto \sigma_\phi$ を得る。この群準同型の核は $C_A(I)$ であるからこれは単射で、しかも包含射 $B \subset N_A(I)$ の左逆射となっているので、とくに $B = N_A(I)$ が従う。

問題 1.6.3. G を非可換単純群とする。このとき $\text{Aut}(G)$ のすべての自己同型は内部自己同型であることを示せ。

Proof. 前問より、 $\text{Inn}(G) \subset \text{Aut}(G)$ が特性部分群であることを示せば良い。 $\phi : \text{Aut}(G) \xrightarrow{\sim} \text{Aut}(G)$ を自己同型として、 $\phi(\text{Inn}(G)) \neq \text{Inn}(G)$ となると仮定する。 $\text{Inn}(G), \phi(\text{Inn}(G))$ は $\text{Aut}(G)$ の正規部分群であるから、 $N_{\text{Aut}(G)}(\text{Inn}(G)) = N_{\text{Aut}(G)}(\phi(\text{Inn}(G))) = \text{Aut}(G)$ となる。 G は非可換単純群なので、 $Z(G) = \{1\}$ である。従って $G \cong \text{Inn}(G)$ であり、 $\text{Inn}(G)$ は単純群となる。 $\phi(\text{Inn}(G)) \cap \text{Inn}(G) \triangleleft \text{Inn}(G)$ であり、 $\text{Inn}(G)$ は単純群なので、 $\phi(\text{Inn}(G)) \cap \text{Inn}(G) = \{1\}$ となる。以上より、

$$\phi(\text{Inn}(G)) \cap \text{Inn}(G) = \{1\}, \quad \text{Inn}(G) \subset N_{\text{Aut}(G)}(\phi(\text{Inn}(G))), \quad \phi(\text{Inn}(G)) \subset N_{\text{Aut}(G)}(\text{Inn}(G)),$$

が成り立つ。ここで本文補題 (3.16) を用いると、 $\text{Inn}(G)$ の任意の元と $\phi(\text{Inn}(G))$ の任意の元は交換可能、すなわち、 $G \cong \phi(\text{Inn}(G)) \subset C_{\text{Aut}(G)}(\text{Inn}(G))$ となることが従う。よって問題 1.6.1 より $G = \{1\}$ となって G

がアーベルでないことに反する。よって $\phi(\text{Inn}(G)) \cap \text{Inn}(G) = \text{Inn}(G)$ となり、 $\text{Inn}(G) \subset \text{Aut}(G)$ は特性部分群であることが従う。以上で解答を完了する。 

問題 1.6.4. σ を群 G の正規自己準同型として、 $H :=^{\text{def}} \sigma(G)$ とする。以下の問いに答えよ。

- (i) $g \in G$ とする。 $\sigma(g) :=^{\text{def}} z(g)^{-1}g$ となるように $z : G \rightarrow G$ を定義すると、 $\text{Im}(z) \subset C_G(H)$ が成り立つ。これを示せ。
- (ii) $H \triangleleft G$ であることを示せ。さらに $G = HC_G(H)$, $H \cap C_G(H) = Z(H) \subset Z(G)$ が成り立つことを示せ。
- (iii) $H, C_G(H)$ とともに σ 不変であることを示せ。さらに $\rho :=^{\text{def}} \sigma|_{C_G(H)} : C_G(H) \rightarrow C_G(H)$, $\zeta :=^{\text{def}} z|_H : H \rightarrow C_G(H)$ とおくと、 $\text{Im}(\rho) \subset Z(H)$ であり、そして任意の $h \in Z(H)$ に対して $h = \zeta(h)\rho(h)$ が成り立つことを示せ。
- (iv) 逆に $G = HC_G(H)$ となる群 G と正規部分群 $H \triangleleft G$ と準同型 $\zeta : H \rightarrow Z(H)$ と準同型 $\rho : C_G(H) \rightarrow Z(H)$ が与えられていて、任意の $h \in H$ に対して $h = \zeta(h)\rho(h)$ を満たしているとき、任意の元 $g = ch \in G, c \in C_G(H), h \in H$ に対して $\sigma(g) = \rho(c)\zeta(h)^{-1}h$ として $\sigma : G \rightarrow G$ を定義すれば、 σ は正規自己準同型であり、 $\text{Im}(\sigma) \subset H$ である。これを示せ。

Proof. 