数学演習 VII・VIII　5 月 30 日分解答[*1]

担当: 柳田伸太郎 (理学部 A 館 441 号室)
yanagida [at] math.nagoya-u.ac.jp
https://www.math.nagoya-u.ac.jp/~yanagida/2019S78.html

7　群論 2 (準同型定理)

7.1　部分群と商集合

問題 7.1. e を G の単位元とする.

(1) $H = H^{-1}$ について. H の任意の元 h' はある $h \in H$ を用いて $h' = h^{-1}$ と書ける. H は部分群なので $h^{-1} \in H$. つまり $h' \in H$. h' は任意だったので $H^{-1} \subset H$. 逆に任意の $h \in H$ に対し, H が部分群なので $h^{-1} \in H$ だが, $h = (h^{-1})^{-1}$ なので $h \in H^{-1}$. h は任意だったので $H \subset H^{-1}$.
$H = HH$ について. 上と同様にして, H が部分群であることから $HH \subset H$ が従う. また $e \in H$ より, 任意の $h \in H$ について $h = e \cdot h \in HH$. つまり $H \subset HH$.

(2) 部分群の 3 条件を確認すれば良い. $e \in H$ と $e \in K$ より $e \in H \cap K$. H と K が逆元を取る操作で閉じていることから, 任意の $h \in H \cap K$ について $h^{-1} \in H$ かつ $h^{-1} \in K$, つまり $h^{-1} \in H \cap K$. H と K が積を取る操作で閉じていることから, 任意の $h, k \in H \cap K$ について $hk \in H$ かつ $hk \in K$, つまり $hk \in H \cap K$.

問題 7.2. HK が部分群だと仮定する. 任意の $h \in H$ と $k \in K$ について, $hk \in HK$ の逆元は $(hk)^{-1} = kh \in KH$. 一方で HK が部分群であることから $(hk)^{-1} \in HK$. よって $kh \in HK$. h, k は任意だったから $KH \subset HK$. また以上の議論で h と k を交換して $HK \subset KH$ も示せる. よって $HK = KH$.

$HK = KH$ を仮定して, HK が積と逆元を取る操作で閉じていることを示す ($e \in H \cap K$ だから $e \in HK$ はこの仮定がなくても成立している). まず積について, 任意の $h_1k_1, h_2k_2 \in HK$ に対し $k_1h_2 \in KH = HK$ よりある $h \in H$, $k \in K$ があって $k_1h_2 = hk$. よって $(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(hk)k_2 = (h_1h)(kk_2) \in HK$. つまり HK は積で閉じている. 次に逆元について, 任意の $hk \in HK$ に対し $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$ なので, HK は逆元を取る操作で閉じている.

問題 7.3. まず $\{0\} = 0\mathbb{Z}$ と書けることに注意する. 部分群 $\{0\} \subsetneq G \subset \mathbb{Z}$ について, G に含まれる最小の正の整数を n とする.

G が部分群であることから $n\mathbb{Z} \subset G$ が言える. 実際, 演算で閉じていることから, 帰納法で $\{nm \mid m = 1, 2, \ldots\} \subset G$ が言える. また単位元 0 を含むことから $\{nm \mid m = 0, 1, \ldots\} \subset G$. 最後に逆元を取る操作で閉じていることから各 $m = 0, 1, \ldots$ に対し $-nm \in G$. 以上より $n\mathbb{Z} \subset G$.

次に $n\mathbb{Z} \subsetneq G$ と仮定して $m \in G \setminus n\mathbb{Z}$ を取る. G が逆元を取る操作で閉じていることから, $\pm m \in G$ なので, $m > 0$ と仮定して良い. m を n で割った余りを k とすると, $m = an + k$, $a \in \mathbb{Z}$ と書ける. $m \notin n\mathbb{Z}$ より $0 < k < n$. しかし $k = m - an \in G$ より n の取り方と矛盾する. 以上より $n\mathbb{Z} = G$.

問題 7.4. (1) 商集合 G/H への自然な射影を $\pi : G \to G/H$ と書く. G/H が G の類別を与える, つまり $G = \bigsqcup_{s \in G/H} \pi^{-1}(s)$ となることから $|G| = \sum_{s \in G/H} |\pi^{-1}(s)|$. 任意の $s \in G/H$ はある $x \in G$ を用いて $s = xH$ と書ける. また, どの $x \in G$ についても $|xH| = |H|$ となる. よって $|G| = \sum_{s \in G/H} |H| = [G : H] \cdot |H|$.

[*1] 2019/05/30 版, ver. 0.2.

(2) 問 (1) より, 任意の部分群 $H \subset G$ について, $|H|$ は $|G|$ の約数である. H として $g \in G$ の生成する G の部分群 $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$ をとれば結論が得られる.

7.2 正規部分群

以下では対称群の元に関して, 次のような巡回置換の記号を使う.

$$(i,j) = \begin{pmatrix} \cdots & i & \cdots & j & \cdots \\ \cdots & j & \cdots & i & \cdots \end{pmatrix}, \quad (i,j,k) = \begin{pmatrix} \cdots & i & \cdots & j & \cdots & k & \cdots \\ \cdots & j & \cdots & k & \cdots & i & \cdots \end{pmatrix}.$$

問題 7.5. 答えは $\{e\}$, $\{e,(1,2,3),(1,3,2)\}$, S_3 自身の 3 つ.

定義より自明な部分群は正規. S_3 の自明でない部分群は位数 2 の $\{e,(1,2)\}$, $\{e,(1,3)\}$, $\{e,(2,3)\}$, 位数 3 の $\{e,(1,2,3),(1,3,2)\}$ の 4 つ. $\tau(i,j)\tau^{-1} = (\tau(i),\tau(j))$ に注意すると, 位数 2 のものはどれも正規ではないことが分かる. また位数 3 のものは同様の議論より (あるいは, 指数 2 なので問題 7.6 より) 正規だと分かる.

問題 7.6. $g \in H$ ならば, H が部分群であることから $gH = Hg$ が成立する. $g \notin H$ と仮定する. この時 $gH \neq H$ なので, 仮定から $G = H \sqcup gH$. 同様に左剰余類 $H\backslash G$ についても, $Hg \neq H$ と仮定から $G = H \sqcup Hg$. よって $Hg = gH$.

問題 7.7. 素数位数の巡回群.

問題 7.8. 問題 7.13 より $\mathrm{sgn} : S_n \to \{\pm 1\}$ は準同型で, $A_n = \mathrm{Ker}(\mathrm{sgn})$ だから, 問題 7.14 (1) よりこれは S_n の正規部分群. また隣接互換の符号が -1 だから sgn は全射なので, 準同型定理より $S_n/\mathrm{Ker}(\mathrm{sgn}) \simeq \{\pm 1\}$. よって指数は 2.

問題 7.9. V が A_4 の部分群であることは直接確認できる. 正規部分群であることを示すために, S_4 の元を巡回置換の元の積で表した時の型 (**cycle type**) で分類すると

$$\begin{aligned}
&e; \\
&(1,2),\ (1,3),\ (1,4),\ (2,3),\ (2,4),\ (3.4); \\
&(1,2,3),\ (1,3,2),\ (1,2,4),\ (1,4,2),\ (1,3,4),\ (1,4,3),\ (2,3,4),\ (2,4,3); \\
&(1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3); \\
&(1,2,3,4),\ (1,2,4,3),\ (1,3,2,4),\ (1,3,4,2),\ (1,4,2,3),\ (1,4,3,2).
\end{aligned}$$

任意の $\sigma, \tau \in S_4$ について, σ と $\tau\sigma\tau^{-1}$ の型が同じであることに注意する. V は 3 行目の型をもつものからなるので, 任意の $\tau \in S_4$ について $\tau V \tau^{-1} = V$ が分かる. よって V は S_4 の正規部分群.

問題 7.10. A_5 の元を cycle type で分類すると

$$e; \quad (i,j)(k,l) \text{ 型が 15 個}; \quad (i,j,k) \text{ 型が 20 個}; \quad (i,j,k,l,m) \text{ 型が 24 個}.$$

A_5 の正規部分群 N は cycle type で類別される. つまり $N = \{e\} \sqcup C_1 \sqcup \cdots$ と互いに素な部分集合に分解できる. 特に $|N| = 1 + |C_1| + \cdots$. 一方 N は部分群だから $|N|$ は $|A_5| = 60$ を割り切る. しかし 1, $1+15$, $1+20$, $1+24$, $1+15+20$, $1+15+24$, $1+20+24$, $1+15+20+24$ のうち 60 の約数は 1 と $1+15+20+24$ だけ. つまり正規部分群の分解として可能なものは $\{e\}$ と A_5 のみ.

7.3　商群

問題 7.11. $g_1N = g_1'N$ なら $(g_1g_2)N = (g_1'g_2)N$ を示す．$g_1N = g_1'N$ より $h := g_1^{-1}g_1' \in N$ なので $g_1'g_2 = g_1g_1^{-1}g_1'g_2 = g_1hg_2$. N が正規部分群であることから $hg_2 = g_2h'$ となる $h' \in N$ がある．よって

$$g_1'g_2N = g_1hg_2N = g_1g_2h'N = (g_1g_2)N.$$

同様にして $g_2N = g_2'N$ なら $(g_1g_2)N = (g_1g_2')N$ が示せる．よって well-defined.

G/N の結合則は, $(g_1N{\cdot}g_2N){\cdot}g_3N = (g_1g_2)N{\cdot}g_3N = ((g_1g_2)g_3)N$ と $g_1N{\cdot}(g_2N{\cdot}g_3N) = g_1N{\cdot}(g_2g_3)N = (g_1(g_2g_3))N$ 及び G での結合則 $g_1(g_2g_3) = (g_1g_2)g_3$ から従う．

e を G の単位元とすると, $eN = N$ が G/N の単位元. 実際, 問題 7.2 より $N \cdot N = N$ だから $gN \cdot eN = gN \cdot N = gN$.

最後に逆元については $(gN)^{-1} = g^{-1}N$. 実際 $g^{-1}N \cdot gN = (g^{-1} \cdot g)N = eN$ で, 同様に $gN \cdot g^{-1}N = eN$.

7.4　準同型写像

問題 7.12. $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$ の両辺に $f(e_G)^{-1}$ をかけて $e_H = f(e_G)$.

$f(g^{-1}) \cdot f(g) = f(g^{-1} \cdot g) = f(e_G) = e_H$ 及び $f(g) \cdot f(g^{-1}) = f(g \cdot g^{-1}) = f(e_G) = e_H$ と逆元の一意性より $f(g^{-1}) = f(g)^{-1}$.

問題 7.13. $i = 1, \ldots, n-1$ に対して隣接互換 $s_i = (i, i+1)$ を考えると, 任意の $\sigma \in S_n$ は s_i 達の積で $\sigma = s_{i_1}s_{i_2}\cdots s_{i_l}$ と書ける (n に関する帰納法で示せる).

$\mathrm{sgn}(s_i) = -1$ は明らか．また $\sigma = s_{i_1}s_{i_2}\cdots s_{i_l}$ なら $\mathrm{sgn}(\sigma) = (-1)^l$ となることが l に関する帰納法で示せる．これから $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$ が分かる．

問題 7.14.
(1) まず部分群であることを示す．問題 7.12 より $e_G \in \mathrm{Ker}\, f$ なので $\mathrm{Ker}\, f \neq \emptyset$. また $g_1, g_2 \in \mathrm{Ker}\, f$ なら $f(g_1g_2) = f(g_1)f(g_2) = e_He_H = e_H$ より $g_1g_2 \in \mathrm{Ker}\, f$. 最後に $g \in \mathrm{Ker}\, f$ なら問題 7.12 より $f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H$ なので $g^{-1} \in \mathrm{Ker}\, f$.
次に $k \in \mathrm{Ker}\, f$ と任意の $g \in G$ について, $f(gkg^{-1}) = f(g)f(k)f(g)^{-1} = f(g)e_Hf(g)^{-1} = e_H$ より $gkg^{-1} \in \mathrm{Ker}\, f$. よって $g\,\mathrm{Ker}\, f g^{-1} = \mathrm{Ker}\, f$ なので $\mathrm{Ker}\, f$ は正規部分群

(2) $f(g_1) = f(g_2)$ なる $g_1, g_2 \in G$ があれば $f(g_1g_2^{-1}) = f(g_1)f(g_2)^{-1} = e_H$ より $g_1g_2^{-1} \in \mathrm{Ker}\, f$. 仮定より $g_1g_2^{-1} = e_G$, 即ち $g_1 = g_2$.

(3) 問題 7.12 より $e_H = f(e_G) \in \mathrm{Im}\, f$ となるので $\mathrm{Im}\, f \neq \emptyset$. また $\mathrm{Im}\, f$ の任意の 2 元 h_1, h_2 は $h_i = f(g_i)$, $g_i \in G$ とかけて, $h_1h_2 = f(g_1)f(g_2) = f(g_1g_2) \in \mathrm{Im}\, f$ となるので, $\mathrm{Im}\, f$ は積で閉じていることが分かる．最後に逆元について, 任意の $h \in \mathrm{Im}\, f$ は $h = f(g)$, $g \in G$ と書けるが, 問題 7.12 より $f(g)^{-1} = f(g^{-1}) \in \mathrm{Im}\, f$ なので $h^{-1} \in \mathrm{Im}\, f$. つまり逆元を取る操作で閉じている.

問題 7.15. 0 以外の複素数のなす乗法群を $\mathbb{C}^\times := (\mathbb{C}\backslash\{0\}, \times, 1)$ と書く．写像 $e : \mathbb{R} \to \mathbb{C}^\times$, $e(x) := \exp(2\pi ix)$ を考える．指数法則から $e(x+y) = e(x)e(y)$ となるので, e は群の準同型である．また $e(x+1) = e(x)$ より $\mathrm{Im}\, e = e([0,1)) = T$. すると準同型定理から $\mathbb{R}/\mathrm{Ker}(e) \simeq T$. 最後に $\mathrm{Ker}(e) = \mathbb{Z}$ から $\mathbb{R}/\mathbb{Z} \simeq T$.

問題 7.16. 行列式を取ることで定まる写像 $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$, $A \mapsto \det(A)$ を考えると, $\det(AB) = \det(A)\det(B)$ よりこれは群準同型.

$\mathbb{R}^*$ の単位元が 1 であることに注意して, $\mathrm{Ker}(\det) = (\det)^{-1}(1) = \mathrm{SL}_n(\mathbb{R})$. 一般に群の準同型写像の核は正規部分群だから, $\mathrm{SL}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R})$ は正規部分群.

また任意の $a \in \mathbb{R}^*$ に対し, 対角行列 $A = \mathrm{diag}(a, 1, \ldots, 1)$ は $A \in \mathrm{GL}_n(\mathbb{R})$ かつ $\det(A) = a$ を満たすので, 準同型 det は全射.

以上の議論と準同型定理 $\mathrm{GL}_n(\mathbb{R})/\operatorname{Ker}(\det) \simeq \operatorname{Im}(\det)$ から $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathbb{R}^*$ が得られる.

7.5 群の中心

問題 7.17. (1) まず部分群であることを示す. $e \in Z(G)$ は明らか. $z_1, z_2 \in Z(G)$ なら, 任意の $g \in G$ に対し $g(z_1z_2) = z_1gz_2 = (z_1z_2)g$ なので $z_1z_2 \in G$. $z \in Z(G)$ の逆元 z^{-1} について, 任意の $g \in G$ に対し $z^{-1}g = (g^{-1}z)^{-1} = (zg^{-1})^{-1} = gz^{-1}$ なので $z^{-1} \in Z(G)$.

次に正規部分群であることを示す. $z \in Z(G)$ と任意の $g \in G$ に対し $gzg^{-1} = gg^{-1}z = z$ なので $gzg^{-1} \in Z(G)$. よって任意の $g \in G$ に対し $gZ(G)g^{-1} = Z(G)$ なので $Z(G)$ は正規部分群.

(2) 巡回群 $G/Z(G)$ の生成元を $aZ(G)$ と書くと, $(aZ(G))^n = a^nZ(G)$ より G の任意の元は a^nz ($n \in \mathbb{Z}$, $z \in Z(G)$) と書ける. すると G の任意の 2 元 g_1, g_2 について, $g_1 = a^mz_1$, $g_2 = a^nz_2$ とおけば $g_1g_2 = a^mz_1a^nz_2 = a^{m+n}z_1z_2 = a^nz_2a^mz_1 = g_2g_1$. つまり G は可換群であり, $G = Z(G)$ である.

問題 7.18. 答えは 0 でないスカラー行列全体.

$Z(G)$ の元 $Z = (z_{ij})_{i,j=1}^n$ と対角行列 $A = \mathrm{diag}(a_1, a_2, \cdots, a_n) \in \mathrm{GL}_n(\mathbb{R})$ (但し $i \neq j$ なら $a_i \neq a_j$) について, $AZ = ZA$ の (i, j) 成分を比較して $a_iz_{ij} = z_{ij}a_j$. よって $i \neq j$ なら $z_{ij} = 0$. また $i \neq j$ として置換行列 E_{ij} ((i, j) 成分と (j, i) 成分が 1, $k \neq i, j$ なら (k, k) 成分が 1, ほかの成分は 0) を考えると, $E_{ij}Z = ZE_{ij}$ から $z_{ii} = z_{jj}$. よって $Z = z_{11}E_n$ (スカラー行列) でなければならない. 逆に 0 でないスカラー行列が中心元であることは明らか.

問題 7.19. $n = 1$ 及び $n \geq 3$ なら $Z(S_n) = \{e\}$, $Z(S_2) = S_2$.

$n \geq 2$ の場合は明らかなので $n \geq 3$ とする. $z \in Z(S_n) \setminus \{e\}$ を任意に取って固定する. $z \neq e$ より $z(i) = j \neq i$ なる $1 \leq i, j \leq n$ がある. $n \geq 3$ より $k \neq i, j$ なる $1 \leq k \leq n$ が取れる. $s := (j, k)$ とすると $szs^{-1}(i) = sz(i) = s(j) = k \neq i$. よって $szs^{-1} \neq z$. これは $z \in Z(G)$ に反する. よって $Z(S_n) = \{e\}$.

問題 7.20. (1) 全単射が群をなすことは既知とする (§3.1, 例 3.1 参照). $\operatorname{Aut} G$ がその部分群であることを示せば良い. 恒等写像 id_G は準同型なので $\mathrm{id}_G \in \operatorname{Aut} G$. 準同型の合成は準同型だから $\operatorname{Aut} G$ は積で閉じている. また自己同型 f の逆写像 f^{-1} は準同型だから, 特に自己同型であり, $\operatorname{Aut} G$ に含まれる. よって部分群である.

(2) $g \in G$ を任意に取って固定する. 写像 $c_g : G \to G$ を $c_g(g') := gg'g^{-1}$ と定義すると, $c_g(g_1g_2) = c_g(g_1)c_g(g_2)$ 及び $c_{g^{-1}}c_g = \mathrm{id}_G$ から, c_g が G の自己同型であることが分かる (c_g を**内部自己同型写像** (**inner automorphism**) と呼ぶ).

すると $Z(\operatorname{Aut} G)$ の任意の元 z について $c_gz = zc_g$. 特に任意の $g' \in G$ について $c_g(z(g')) = z(c_g(g'))$, つまり $gz(g')g^{-1} = z(gg'g^{-1})$. z が準同型であることを用いて右辺を変形すると $gz(g')g^{-1} = z(g)z(g')z(g)^{-1}$. つまり $(z(g)^{-1}g)z(g')(z(g)^{-1}g)^{-1} = z(g')$. g' は任意に取っていて, また z が全単射であることから $(z(g)^{-1}g)G = G(z(g)^{-1}g)$. よって $z(g)^{-1}g \in Z(G)$.

仮定より $Z(G) = \{e\}$ だから, $z(g) = g$. g は任意に取っていたから $z = \mathrm{id}_G$ である.

以上です.