代数系入門 解答集

最終更新日：2021 年 2 月 3 日

目次

1　p7

p7.1

Proof. S' を S に含まれない自然数全体の集合とする．このとき，

$$S' = \varnothing$$

であることを示せばよい．

いま $S' \neq \varnothing$ を仮定する．整列性によって， $n_1 \coloneqq \min S'$ が存在する．仮定 (1) により

$$n_1 > 0$$
$$\therefore\ n_1 - 1 \geq 0$$

となる．仮定 (2) において，$n_1 = n$ とする．ここで $n_1 \in S'$ であるから，$0, 1, 2, \ldots, n_1 - 1 \in S$ である．しかしこのとき，

$$0 \leq n_1 - 1 < n_1$$

であるから $n_1 \in S$ となり，これは $n_1 \in S'$ に反する．ゆえに背理法の仮定が誤りであり，$S' = \varnothing$ である．すなわち，S は自然数全体の集合と一致する． □

p7.3

(a)

Proof. n に関する数学的帰納法で示す．$n=1$ のとき，

$$(\text{与式の左辺}) = 1, \quad (\text{与式の右辺}) = \frac{1(1+1)}{2} = 1$$

となり，たしかに与式は成立する．

任意の $n \in \mathbb{N}$ について，与式の成立を仮定すると，

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

である．この両辺に $n+1$ を加えると，

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

となり，$n+1$ のときも与式は成立する．

以上の議論と数学的帰納法により，任意の $n \in \mathbb{N}$ について，

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

が確かに成り立つことが示された． □

(b)

Proof. n に関する数学的帰納法で示す．$n=1$ のとき，

$$(\text{与式の左辺}) = 1, \quad (\text{与式の右辺}) = \frac{1(1+1)(2\cdot 1+1)}{6} = 1$$

となり，たしかに与式は成立する．

任意の $n \in \mathbb{N}$ について，与式の成立を仮定すると，

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

である．この両辺に $(n+1)^2$ を加えると，

$$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \end{aligned}$$

となり，$n+1$ のときも与式は成立する．

以上の議論と数学的帰納法により，任意の $n \in \mathbb{N}$ について，

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

が確かに成り立つことが示された． □

2　p13

p13.3

Proof. 必要条件であることを示す．

与えられた方程式の解 $x_1, \ldots, x_n$ が存在すると仮定する．このとき，

$$\frac{a_1x_1 + \cdots + a_nx_n}{d} = \frac{m}{d}$$

の左辺は整除される．よって右辺は整除され，これで必要条件であることが証明された．

次に，十分条件であることを示す．

$d \mid m$ を仮定する．d の定義と p10：系 1 により，

$$d = a_1u_1 + \cdots + a_nu_n \tag{1}$$

をみたす $u_1, \ldots, u_n \in \mathbb{Z}$ が存在する．ここで，$c \coloneqq m/d$ とすれば，仮定により，$c \in \mathbb{Z}$ である．

ここで，(1) の両辺に c を掛けると，

$$cd = a_1cu_1 + \cdots + a_ncu_n$$

となる．さらに，$i = 1, \ldots n$ について，$cu_i = x_i$ と改めておくと，$cd = m$ により，

$$m = a_1x_1 + \cdots + a_nx_n$$

となり，これで十分条件であることが証明された． □

3　p14

p14.3

Proof. $(a,b)=1$ であるから，ある $x,y\in\mathbb{Z}$ が存在して，

$$ax+by=1 \tag{2}$$

と表される．(2) の両辺に m をかけ，

$$max+mby=m \tag{3}$$

を得る．ここで，

$$a\mid m,\quad b\mid m$$

のそれぞれから

$$ab\mid mb,\quad ab\mid ma$$

となるため．(3) の左辺は ab で割り切れ，ただちに $ab\mid m$ を得る． □

4 p60

p60 3

Proof. 任意の $h, h' \in H$ をとれば,

$$\begin{aligned} & hH \cap K = h'H \cap K \\ \Longrightarrow\ & h^{-1}h' \subset H \cap K \subset K \\ \Longrightarrow\ & hK = h'K \end{aligned}$$

であるから，$hH \cap K \longmapsto hK$ によって定められる H の $H \cap K$ を法とする左剰余類全体から，G の K を法とする左剰余類全体への写像 f を定義することができる.

また，任意の $H \cap K$ を法とする H の剰余類 $hH \cap K$，$h'H \cap K$ をとれば,

$$\begin{aligned} & f(hH \cap K) = f(h'H \cap K) \\ \Longrightarrow\ & hK = h'K \\ \Longrightarrow\ & h^{-1}h' \in K \\ \Longrightarrow\ & h^{-1}h' \in H \cap K \quad (\because h^{-1}h' \in H) \\ \Longrightarrow\ & hH \cap K = h'H \cap K \end{aligned}$$

より f は単射なので，K の G における左剰余類全体がなす f の終集合は有限集合だから，f の始集合となる $H \cap K$ の H における左剰余類全体も有限集合で,

$$(H : H \cap K) \leq (G : K)$$

□

Proof. H の G における各左剰余類の代表元全体を

$$A = \{a_1, a_2, \ldots, a_r\}, \quad r = (G : H)$$

K の H における各左剰余類全体の代表元全体を，

$$B = \{h_1, h_2, \ldots, h_s\}, \quad s = (H : K)$$

として，$(a_i, b_j) \longmapsto a_i h_j K$ によって定義される $A \times B$ から G の K を法とする左剰余類全体への写像を f とする．

ここで，f が全単射であることを示せばよい．

任意の $x \in G$ に対して，$x = a_i h_j$ となる $a_i \in A$，$h_j \in B$ があって，同様に，$h = h_j k$ となる $h_j \in B$，$k \in K$ があるから，$x = a_i h_j k$ で，

$$xK = a_i h_j k K = a_i h_j K$$

であるから，f は全射である．

また，

$$a_i h_j K = a_{i'} h_{j'} K$$
$$(1 \leq i, i' \leq r,\ 1 \leq j, j' \leq s)$$

とすると，

$$(a_i h_j)^{-1} (a_{i'} h_{j'}) \in K$$
$$\Longrightarrow {h_j}^{-1} {a_i}^{-1} a_{i'} h_{j'} \in K \subset H$$

ここで，${h_j}^{-1} h_{j'} \in H$ なので，${a_i}^{-1} a_{i'} \in H$ で，A の定義により，

$$a_i = a_{i'}$$

さらに，${h_j}^{-1} h_{j'} \in K$ なので，B の定義により，

$$h_j = h_{j'}$$

ゆえに，$(a_i, h_i) = (a_{i'}, h_{i'})$ となるから f は単射だから f は全単射． □

Proof. n に関する数学的帰納法によって証明する.

(i) $n = 1$ の場合は等号が成立する.

(ii) $n > 1$ として，$n - 1$ の場合を仮定して n の場合を示す.

仮定より,

$$(G : H_1 \cap \cdots \cap H_{n-1}) \leq (G : H_1) \cdots (G : H_{n-1})$$

であり，$H = H_1 \cap \cdots \cap H_{n-1}$ とおくと，問題 3 の結果により,

$$(H_n : H \cap H_m) \leq (G : H)$$

ここで，両辺に $(G : H_n)$ をかければ,

$$(G : H_n)(H_n : H \cap H_n) \leq (G : H)(G : H_n)$$

で，問題 2 の結果より,

$$(G : H_n)(H_n : H \cap H_n) \leq (G : H \cap H_n)$$

だから,

$$(G : H \cap H_n) \leq (G : H)(G : H \cap H_n)$$

すなわち,

$$(G : H_1 \cap H_2 \cap \cdots \cap H_n) \leq (G : H_1) \cdots (G : H_n)$$

よって (i)，(ii) から，群 G の部分群 $H_1, H_2, \ldots, H_n$ それぞれの G における指数が有限であるとき，$H_1 \cap \cdots \cap H_n$ の G における指数も有限で,

$$(G : H_1 \cap \cdots \cap H_n) \leq (G : H_1) \cdots (G : H_n)$$

である. □

5　p73

p73 3

Proof.

$$z \longmapsto \frac{z}{|z|}$$

によって定義される $\mathbb{C}^*$ から T への写像

$$f\colon \mathbb{C}^* \longrightarrow T$$

をとれば，f は明らかに全射であり，任意の $zw \in \mathbb{C}^*$ に対して，

$$f(zw) = \frac{z \cdot w}{|zw|} = \frac{z}{|z|} \cdot \frac{w}{|w|}$$

だから，f は全射準同型である．

　ここで，任意の $z \in \mathbb{C}^*$ に対して，

$$\frac{z}{|z|} = 1 \iff z \in \mathbb{R}^+$$

であるから，

$$\ker f = \mathbb{R}^+$$

よって，準同型定理により，

$$\mathbb{C}^*/\mathbb{R}^+ \cong T$$

□

Proof. まず,

$$f = g \circ \varphi$$

となるような準同型 $g\colon G/N \longrightarrow G'$ の存在を示す.

任意の $aN, bN \in G/N$ に対して,

$$\begin{aligned} & aN = bN \\ \Longrightarrow\ & a^{-1}b \in N \\ \Longrightarrow\ & a^{-1}b \in N_0 && (\because N \subset N_0) \\ \Longrightarrow\ & a \equiv b \pmod{N_0} \\ \Longrightarrow\ & f(a) = f(b) \end{aligned}$$

であるから,

$$aN \longmapsto f(a)$$

によって定義される G/N から G' への写像 g が定義でき,

$$\begin{aligned} & g((aN)(bN)) \\ =& g(abN) && (\because N \text{ は正規部分群}) \\ =& f(ab) \\ =& f(a)f(b) && (\because f \text{ は準同型}) \\ =& g(aN)g(bN) \end{aligned}$$

から，g は全射準同型である.

また，f，$g \circ \varphi$ はともに G から G' への写像で，任意の $a \in G$ に対して,

$$\begin{aligned} & g \circ \varphi(a) \\ =& g(aN) \\ =& f(a) \end{aligned}$$

により，$f = g \circ \varphi$ である.

次に，g の一意性を示す．もし，g と異なる G/N から G' の準同型で，$f = g \circ \varphi$ を満足するものが存在するならば，それを

$$g'\colon G/N \longrightarrow G'$$

とおけば，ある $aN \in G/N$ があって,

$$g(aN) \neq g'(aN)$$

すなわち,

$$g'(aN) \neq f(a)$$

で,

$$g'(\varphi(a)) \neq f(a)$$

であるから，$f = g' \circ \varphi(a)$ に矛盾する．よって g は一意的である. □

p73 7

補題 5.1：

G を群，G' を可換群とするとき，G から G' への準同型が存在するならば，G も可換群である．

Proof.

$$f\colon G \longrightarrow G'$$

を G から G' への単射準同型とすると，任意の $a, b \in G$ に対して，

$$\begin{aligned} f(ab) &= f(a)f(b) \\ &= f(b)f(a) \quad (\because G' \text{ は可換}) \\ &= f(ba) \end{aligned}$$

ゆえに，f は単射であるから，

$$ab = ba$$

よって G は可換群である． □

Proof. 問題 6（第 2 章，§ 6）の結果により，準同型 $f\colon G \longrightarrow G'$ の核を N とするとき，$D \subset N$ を示せばよい，

a，b を G の任意の元とすれば，交換子群 D は $aba^{-1}b^{-1}$ の形の G の元全体によって生成される G の部分群であるから，$D \subset N$ と $aba^{-1}b^{-1}$ は同値であり，

$$\begin{aligned} & aba^{-1}b^{-1} \in N \\ \Longleftrightarrow\ & Naba^{-1}b^{-1} = N \\ \Longleftrightarrow\ & Nab = Nba \\ \Longleftrightarrow\ & (aN)(bN) = (bN)(aN) \quad (\because N \text{ は正規部分群}) \end{aligned}$$

であるから，N による G の商群 G/N が可換群であることを示せばよい．

ここで，準同型 $f\colon G \longrightarrow G'$ において，準同型定理により，

$$G/N \cong f(G)$$

を得て，$f(G)$ は可換群 G' の可換な部分群であるから，先の補題により，G/N は可換群である．

これより，$D \subset G$ となって，$f = g \circ \varphi$ となるような G/D から G' への準同型 g が一意に存在する． □

6　p80

p80 1

Proof. G を a を生成元とする巡回群，G' を準同型写像 f による G の準同型像とする．

準同型像の定義により，

$$f(G) = G'$$

だから，

$$\begin{aligned} G' &= \{f(a^k) \mid k \in \mathbb{Z}\} \\ &= \{f(a)^k \mid k \in \mathbb{Z}\} \quad (\because f \text{ は準同型}) \end{aligned}$$

よって，G' は $f(a)$ を生成元とする巡回群． □

p80 2

Proof. $d \neq 1$ のとき，$n = dk$ $(k \in \mathbb{N})$ とすると，a^k を生成元とする G の部分群の位数は d であるから，G は位数が d の部分群をもつ．

また，任意の位数を d $(d \neq 1)$ とする G の部分群は巡回群で，その生成元を $a^{k'}$ $(1 \leq k' \leq n-1)$ とすると，

$$\begin{aligned} & (a^{k'})^d = e \\ \Longrightarrow\ & k'd \in n\mathbb{Z} \\ \Longrightarrow\ & k'd = nl \qquad (l \in \mathbb{N}) \\ \Longrightarrow\ & k'd = (kd)l \quad (\because n = kd) \\ \Longrightarrow\ & k' = kl \end{aligned}$$

ここで，$l > 1$ と仮定すると，

$$1 \leq k < k' = kl \leq n-1$$

から，$a^{k'} = a^{kl}$ となって，$a^1, a^2, \ldots, a^{n-1}$ の内で等しい 2 つのものがとれるようになって矛盾．よって $l = 1$ となって $k' = k$ だから $a^{k'} = a^k$ となって，G の位数を d とする部分群は a^k を生成元とする巡回群に限る． □

p80 3

Proof. d を 0 から $n-1$ までの任意の整数とすると，

$$\begin{aligned}
& (k,n)=1 && \\
\iff & kx+ny=1 && (\exists x,y\in\mathbb{Z}) \\
\iff & kx'+ny'=d && (x'=dx,\ y'=dy) \\
\iff & a^{kx'+ny'}=a^d && (\because (k,n)=1) \\
\iff & (a^k)^{x'}=a^d && (\because (a^n)^{y'}=(e)^{y'}=1) \\
\iff & \{(a^k)^x \mid x\in\mathbb{Z}\}\supset G && \\
\iff & \{(a^k)^x \mid x\in\mathbb{Z}\}=G && (\because \{(a^k)^x \mid x\in\mathbb{Z}\}\subset G)
\end{aligned}$$

であるから，a^k が G の生成元となるための必要十分条件は

$$(k,n)=1$$

である. □

Proof.

$$o(ab) = m, \quad o(ba) = n$$

とおく.

$m < n$ と仮定すると,

$$\begin{aligned} & e = (ab)^m \\ \Longrightarrow \ & ba = b(ab)^m a \\ & = (ba)^{m+1} \end{aligned}$$

ここで, 両辺に左から ba を $n - m - 1$ 個かければ ($n - m - 1 = 0$ のときはなにもかけない),

$$(ba)^{n-m} = (ba)^n = e$$

となって, $m - m < n$ より矛盾だから, $m \geq n$ である. 同様に, $m > n$ と仮定すると矛盾が起こるので, $m \leq n$ で

$$m = n$$

である. □

Proof. a を G のひとつの生成元とする．

$$k \longmapsto a^k$$

によって定義される

$$f\colon \mathbb{Z} \longrightarrow G$$

をとれば，f は全射準同型で，

$$\ker f = n\mathbb{Z}$$

ここで，

$$d \mid n \iff n\mathbb{Z} \subset d\mathbb{Z}$$

より，f の核を含むような $\mathbb{Z}$ の部分群全体を Ω とすると，

$$\Omega = \{d\mathbb{Z} \mid d > 0, d \mid n\}$$

また，G の部分群全体の集合を Ω' として，

$$d\mathbb{Z} \longmapsto f(d\mathbb{Z})$$

によって定義される Ω から Ω' への写像

$$f\colon \Omega \longrightarrow \Omega'$$

を考える．このような $f\colon \Omega \longrightarrow \Omega'$ が単射であることを示せばよい．

Ω' の任意の元 H に対して，$f^{-1}(H)$ は $\mathbb{Z}$ の部分群となり，

$$f^{-1}(H) \supset f^{-1}(e) = \ker f$$

より，$f\colon \mathbb{Z} \longrightarrow G$ の核を含むので，写像 $f^{-1}\colon \Omega' \longrightarrow \Omega$ がとれる．

ここで，任意の $d\mathbb{Z} \in \Omega$ をとると，

$$d\mathbb{Z} \subset f^{-1} \circ f(d\mathbb{Z})$$

で，任意の $x \in f^{-1} \circ f(d\mathbb{Z})$ に対して，

$$\begin{aligned}
& f(x) \in f(d\mathbb{Z}) \\
\Longrightarrow\ & f(x) = f(dl) && (\exists dl \in d\mathbb{Z}) \\
\Longrightarrow\ & x \equiv dl \pmod{n} \\
\Longrightarrow\ & x \equiv dn \pmod{d} && (\because d \mid n) \\
\Longrightarrow\ & x \in d\mathbb{Z}
\end{aligned}$$

だから，

$$f^{-1} \circ f(d\mathbb{Z}) \subset d\mathbb{Z}$$

よって，$f\colon \Omega \longrightarrow \Omega'$ は単射なので，位数 d の G の部分群が一意に定まる． □

p80 8

Proof. G を可換な巡回群とする．ただし，$G \neq \{e\}$ とする．

まず，G が巡回群であることを示す．$G \neq \{e\}$ より，e と異なる G の元 a がとれて，a が生成する G の部分群を H とする．

ここで， G が可換であることにより，G の任意の部分群は正規部分群となって，同時に G は単純群でもあるから，G は真部分群をもたないので，$H \neq \{e\}$ より $H = G$，すなわち，

$$G = \{a^k \mid k \in \mathbb{Z}\}$$

であるから，G は $a \in G$ を生成元とする巡回群.

ここで，G が無限巡回群であると仮定すると，a^2 を生成元とする G の部分群 $\{(a^2)^k \mid k \in \mathbb{Z}\}$ がとれて，これは G の真部分群となるので矛盾する．よって，G は有限巡回群.

次に，G の位数が合成数 mn $(m, n > 1)$ であると仮定すると，a^m が生成する G の部分群 $\{(a^m)^k \mid k \in \mathbb{Z}\}$ は位数を n $(1 < n < o(G) = mn)$ とする G の真部分群であるから，矛盾する．よって，G の位数は素数であるから，可換な単純群は位数が素数の巡回群. □

10

Proof. 商群 $\mathbb{Q}/\mathbb{Z}$ の任意の元 x をとれば，ある $\dfrac{n}{m} \in \mathbb{Q}$ $(m \in \mathbb{N}, n \in \mathbb{Z})$ があって，

$$x = \frac{n}{m} + \mathbb{Z}$$

ここで，m 個の x の和をとると，

$$\begin{aligned}
&\underbrace{x + x + \cdots + x}_{m \text{ 個}} \\
&= \underbrace{\left(\frac{n}{m} + \frac{n}{m} + \cdots + \frac{n}{m}\right)}_{m \text{ 個}} + (\mathbb{Z} + \mathbb{Z} + \cdots + \mathbb{Z}) \\
&= n + \mathbb{Z} && (\because \mathbb{Z} + \mathbb{Z} = \mathbb{Z}) \\
&= \mathbb{Z} && (\because n \in \mathbb{Z})
\end{aligned}$$

であるから，

$$o(x) \leq m \in \mathbb{N}$$

ゆえに，$\mathbb{Q}/\mathbb{Z}$ の任意の元の位数は有限である. □

Proof. まず，前半部分を証明する．

$$A = \{x \in S \mid f(x) \neq x\}$$

として，A の元の個数が偶数であることを示す．

$f = I_S$ のとき，$A = \varnothing$ で $|A| = 0$.

$f \neq I_S$ のとき，ある $x \in S$ があって，$f(x) \neq 0$ なので，$x \in A$ より $A \neq \varnothing$.

ここで，A のある元 a に対して，

$$f(a) = b \quad (a \neq b)$$

とすれば，

$$\begin{aligned} & f \circ f(a) = f(b) \\ \Longrightarrow\ & a = f(b) \qquad\qquad (\because f \circ f = I_S) \end{aligned}$$

より，$b \in A$ である．

さらに．a，b と異なる $c \in A$ があれば，同様に，$f(c) = d$ $(c \neq d)$ があって，$d \in A$.

ここで，f が単射であることにより，

- $a \neq c$ から $b \neq d$ $(\because f(a) = b,\ f(c) = d)$
- $b \neq c$ から $a \neq d$ $(\because f(b) = a,\ f(c) = d)$

なので，

$$\{a, b\} \cap \{c, d\} = \varnothing$$

さらに，a，b，c，d と異なる A の元をとって，同様な操作を繰り返せば，有限回で終わり，A は 2 つの元をもつ互いに交わらない集合 $\{a, b\}, \{c, d\}, \ldots$ の合併集合となるので，A の元の個数は偶数個.

これを用いると，位数を偶数とする有限群 G の $x \longmapsto x^{-1}$ によって定義される置換 g をとれば，$g(x) \neq x$ を満たす $x \in G$ の個数は偶数個なので，$g(x) = x$ を満たす $x \in G$ の個数も偶数個である．

よって，

$$B = \{x \in G \mid g(x) = x\}$$

とすると，B の元の個数は偶数個で，$g(e) = e^{-1} = e$ より $e \in B$ で，$|B| \geq 2$ であるから，e と異なる B の元 s がとれて，

$$\begin{aligned} & g(s) = s \\ \Longrightarrow\ & s^{-1} = s \\ \Longrightarrow\ & s^2 = e \end{aligned}$$

ゆえに，$s \neq e$ から，s を生成元とする G の部分群は $\{e, s\}$ なので，$o(s) = 2$.

よって，位数が偶数の有限群は，位数 2 の元を含む． □

Proof. 任意の N の元 x をとれば，Lagrange の定理より，x の位数は $o(N) = m$ の約数なので，$x^m = e$. ゆえに，

$$N \subset \{x \in G \mid x^m = e\} \tag{4}$$

次に，$\{x \in G \mid x^m = e\} \subset N$ を示す. 任意の $x \in \{x \in G \mid x^m = e\}$ をとり，xN が生成する商群 G/N の部分群を H とおくと，

$$o(H) \mid o(G/N) = (G : H)$$

より，$o(H)$ と m は互いに素であるから，$(xN)^m$ も H の生成元となる.

ここで,

$$\begin{aligned} &(xN)^m \\ =&x^m N \qquad (H \text{ は } G \text{ の正規部分群}) \\ =&eN \qquad (x^m = e) \\ =&N \end{aligned}$$

なので,

$$H = \langle N \rangle = \{H\} = \langle xN \rangle$$

であるから，$xN = N$ でなくてはならない（実際 $xN \neq N$ とすると $xN \in \langle xN \rangle = \{N\}$ となって矛盾が起きる.）.

ゆえに，$x \in N$ が得られるので,

$$\{x \in G \mid x^m = e\} \subset N \tag{5}$$

(1)，(2) により，

$$N = \{x \in G \mid x^m = e\}$$

□

Proof. $o(G)=n$ とおき，n に関する数学的帰納法によって証明する．

(i) $n=1$ のとき
$G=\{e\}$ で，G は e によって生成される巡回群である．

(ii) $1\leq k<n$ を満たす任意の $k\in\mathbb{N}$ に対して，その 2 つの異なる部分群がつねに異なる位数をもつような位数 k の群が巡回群であると仮定して，n の場合を示す．
まず，条件より，等しい位数を持つ 2 つの G の部分群は等しいので，任意の G の部分群 H_1 と任意の $x\in G$ をとれば，$o(H_1)=o(xH_1x^{-1})$ なので，$H_1=xH_1x^{-1}$ で，$H_1x=xH_1$ であるから，G の任意の部分群は正規である．
ここで，$o(G)=n>1$ より，Sylow の第一定理から，G は位数が素数の部分群 H を含む．また，H の単位元以外の元によって生成される H の部分群は，Lagrange の定理より，H 自身と異なるので，H は巡回群となる．
さらに，H は G の部分群なので，G において正規であるから，商群 G/H をとることができ，G から G/H への自然な準同型 f をとれば，f は全射準同型であるから，G の H を含むような部分群全体と，G/H の部分群全体の間に全単射が存在し，任意の G/H の部分群 P' に対して，G の H を含むような部分群が一意に存在して，$P'=f(P)=P/H$ となるから，条件より G/H の 2 つの異なる部分群もつねに異なる位数をもつ．よって，帰納法の仮定により，H による G の商群 G/H も巡回群となる．
ここで，G/H の生成元を bH とおき，b が生成する G の部分群を K とおくと，H の位数は素数なので，$H\subset K$ または $H\cap K=\{e\}$ である（実際に，$H\cap K\neq\{e\}$ として，$c\neq e$ なる $c\in H\cap K$ をとれば，$H=\langle c\rangle\subset K$ となる．）．
$H\subset K$ の場合は，商群 K/H がとれて，明らかに $K/H\subset G/H$ で，任意の $x\in G/H$ をとれば，ある $k\in\mathbb{Z}$ $(0\leq k\leq(G:H)-1)$ がとれて，

$$\begin{aligned}x&=(bH)^k\\&=b^kH\in\langle b\rangle/H=K/H\end{aligned}$$

なので，$G/H\subset K/H$．これより，$G/H=K/H$ が得られ，$o(K)=o(G)$ かつ条件より，$K=G$．よって，$H\subset K$ の場合は G は生成元を b とする巡回群である．
次に，$H\cap K=\{e\}$ の場合を考える．まず，巡回群 G/H の位数 G/H が $o(K)$ より大きいとすると，$bH,b^2H,\ldots,b^{(G:H)-1}H$ の中に H が現れてしまい矛盾であるから，

$$(G:H)\leq o(K)\tag{6}$$

また，$H\cap K=\{e\}$ のとき，第二同型定理より（H は正規部分群）$KH/H\cong K/H\cap K=K$ で，特に位数について，$(KH:H)\mid(G:H)$ なので，$o(K)\mid(G:H)$ を得る．よって $o(K)\leq(G:H)$ なので，(3) と合わせて，

$$o(K)=o(b)=(G:H)\tag{7}$$

を得る．
さらに，H の生成元を a とすると，H，K が正規部分群であることにより，H の生成元 a，K の生成元 b に対して，

$$aba^{-1}b^{-1}\in H\cap K=\{e\}$$

よって，

$$ab=ba\tag{8}$$

であり，H の位数が素数であることと K が巡回群であることに注意すれば，$o(H)\mid o(K)$，すなわち $o(a)\mid o(b)$ と仮定すると，K は $o(H)$ に等しい位数の部分群，すなわち，条件より，H を含んでしまうので，

$H \cap K = \{e\}$ に矛盾するから，

$$o(a) \nmid o(b)$$

これと $o(a)$ が互いに素であることにより，$o(a)$ と $o(b)$ は互いに素であるから，(4)，(5) により，

$$\begin{aligned} o(ab) &= o(a) \circ o(b) \\ &= o(H)o(G:H) \\ &= o(G) \end{aligned}$$

ゆえに，$H \cap K$ のとき，G は H の生成元と K の生成元との積を生成元とする巡回群となる．

□

p95 3

Proof. 必要条件であることを示す．φ を G/H から G/K への G-同型写像とする．また，$\varphi(H) = aK$ とする．ここで，任意の G の元 x に対して，$x \cdot aK = aK$ であることは，$K = \varphi(H)$ と G- 同型写像の性質より，明らかに $\varphi(x \cdot H) = \varphi(H)$ と同値であり，さらに φ が単射であることにより，$x \cdot H = H$，すなわち $x \in H$ と同値である．よって，H は G/H の元 aK の安定部分群に他ならない．また，ここで，aK の安定部分群は，任意の $x \in G$ に対して，$x \cdot aK = aK$ であることが，$a^{-1}xa \in K$，$x \in aKa^{-1}$ と同等だから，aKa^{-1} となる．したがって，$H = aKa^{-1}$ で，H，K は共役部分群である．

十分条件であることを示す．$H = aKa^{-1}$ $(a \in G)$ とすると，H は推移的と G-集合 G/K の元 aK の安定部分群であるから，G の G/K における置換表現は，G の G/aK における置換表現，すなわち，G の G/H における置換表現に同値である． □

p95 4

補題 6.1：

2 つの置換表現

$$\rho\colon G \longrightarrow S(x), \quad \rho'\colon G \longrightarrow S(x')$$

が同値ならば，

$$\ker\rho = \ker\rho'$$

である．

Proof. 2 つの置換表現が同値であることの定義により，任意の $a \in G$，任意の $x \in X$ に対して，

$$\varphi(a \cdot x) = a \cdot \varphi(x)$$

となるような X から X' への全単射である G-同型写像 φ がとれる．但し，$\rho(a)(x)$ を $a \cdot x$，$\rho'(a)(x')$ を $a \cdot x'$ とかくことにする．

ここで，$\ker\rho$ の任意の元 c をとれば，$\rho(c) = I_X$ であるから，任意の $x \in X$ に対して，

$$c \cdot x = x$$

である．さらに，$\varphi(c \cdot x) = \rho(x)$ なので，

$$c \cdot \varphi(x) = \varphi(x)$$

である．ここで，$\varphi(x)$ は X' 全体を動くから，

$$\rho'(c) = I_{X'}$$

となる．さらに，$c \in \ker\rho'$ なので

$$\ker\rho \subset \ker\rho'$$

また，$\ker\rho'$ の任意の元 c をとれば，$\rho'(c) = I_{X'}$ より，任意の $x' \in X'$ に対して，

$$c \cdot x' = x'$$

ここで，φ は全射だから，ある $x \in X$ がとれて，$x' = \varphi(x)$ なので，$c \cdot \varphi(x) = \varphi(x)$ より，$\varphi(c \cdot x) = \varphi(x)$ である．さらに，φ は単射だから，$c \cdot x = x$．ここで，x' は任意だから，x は X 全体を動き，

$$\rho(c) = I_X$$

ゆえに，$c \in \ker\rho$．よって，

$$\ker\rho' \subset \ker\rho$$

であり， $\ker\rho = \ker\rho'$ である． □

Proof. 可換群 G の，任意の忠実な推移的置換表現

$$\rho\colon G \longrightarrow S(X)$$

をとる．

ここで，ρ は推移的なので，X のある元 x_0 の安定部分群 H をとれば，ρ は G の G/H における置換表現

$$\rho'\colon G \longrightarrow S(G/H)$$

に同値である（但し，任意の $a \in G$ に対し，ρ'_a は $xH \longmapsto a \cdot xH = axH$ によって定められるとする．）．

よって，ρ が忠実な置換表現であることにより，$\ker\rho = \{e\}$ だから，先の補題により，$\ker\rho' = \{e\}$.

一方，H は G が可換群であることにより，正規部分群で，任意の $a, x \in G$ に対し，$a \in H$ ならば $x^{-1}ax \in H$ で，これは x と ax が H を法として左合同であることを意味するので，

$$axH = xH$$

よって，$a \cdot xH = xH$ であるから，xH は G/H 全体を動くので．$\rho'(a) = I_{G/H}$ で，$a \in \ker\rho' = \{e\}$．ゆえに $H \subset \{e\}$.

よって，$H = \{e\}$ だから，G の G/H における置換表現 $\rho'\colon G \longrightarrow G/H$ は，G の左正則表現となるので，可換群 G の任意の忠実な推移的置換表現は G の左正則表現と同値である． □

p95 6：

Proof. 位数 p^n の群を G，位数 p^{n-1} の群を H とする．

G の G/H における置換表現の核を N とすれば，準同型定理により，G/N から $o(S(G/H))$ への単射準同型が存在するので，

$$(G:H) \mid p! = o(S(G/H))$$

ここで，N は H の共役部分群全体の共通部分であるから H に含まれるので，$N \subsetneq G$ で，Lagrange の定理により，$(G:H)$ は p のべきだから，$(G:H) = p$.

ゆえに，$o(N) = p^{n-1}$，$N \subset H$ より，$H = N$ で，H は G の正規部分群． □

7 p105

p105.1

補題 7.1：

G を群，H を G の部分群とすれば，$(G:H) = 2$ のとき，H は G の正規部分群．

Proof. $(G:H) = 2$ より，G の H を法とする左剰余類全体の個数は 2 で，写像 $aH \longmapsto Ha^{-1}$ によって，左剰余類全体と右剰余類全体は一対一に対応するので，右剰余類全体の個数も 2 である．

したがって，群 G は任意の $a \notin H$ に対して，H と aH，H と Ha に類別できる．これより，G から H を除いた集合を考えれば

$$aH = Ha \tag{9}$$

また，$a \in H$ なる G の元については，明らかに

$$aH = Ha \tag{10}$$

(9)，(10) から，G は H の正規部分群． □

Proof. 背理法によって，A_4 が位数を 6 とする部分群をもたないことを示す．

H を位数を 6 とする A_4 の部分群であると仮定すると，

$$o(A_4) = \frac{4!}{2} = 12 = 2 \cdot 6$$

より，H は先の補題から G の正規部分群となる．

ここで，4 次対称群 S_4 の共役類について調べれば，任意の $\sigma, \tau \in S_n$ が共役であるための必要十分条件は，それぞれをどの 2 つを互いに素な巡回置換の積で表したときに同じ分解型をもつことであるから，S_n の共役類は，分解型 $[4]$，$[1,3]$，$[2,2]$，$[1,1,2]$，$[1,1,1,1]$ に一対一対応する．

また，分解型が $[4]$，$[1,3]$，$[2,2]$，$[1,1,2]$，$[1,1,1,1]$ である 4 文字の置換全体がなす共役類はそれぞれ，6 個の元からなる 4 文字の巡回置換全体，8 個の元からなる 3 文字の巡回置換全体，3 個の元からなる互いに素な互換全体の積，6 個の元からなる互換全体，1 個の元からなる恒等置換のみの集合となるから，交代群 A_4 は，分解型が $[1,3]$，$[2,2]$，$[1]$ となる 4 文字の置換全体がつくる 3 つの共役類の和集合となる（$o(A_4) = 12 = 8 + 3 + 1$）．

ここで，一般に群 G の正規部分群が G のいくつかの共役類の和集合として表されることを利用すると，H は A_4 の正規部分群であるから，H は A_4 のいくつかの共役類の和集合として表されなければならないが，上により，共役類の元の個数は 8，3，1 に限るので，できない．

よって，A_4 が単位群 A_4 の他に正規部分群をもつとすれば，位数 4 の

$$\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

のみで，位数 6 の正規部分群をもたない． □

p105.3

Proof. $o(G) = p^e s$ $((p, s) = 1)$ とすると，Lagrange の定理より，

$$\begin{aligned} & o(G) \\ =& p^e s \\ =& o(N)(G : N) \end{aligned}$$

であるから，条件により $((G : N), p^e) = 1$ なので，$(G : N) \mid s$ で，$p^e \mid o(N)$．よって，Sylow の第 1 定理より，N は G の 1 つの pSylow 群 P を含む．

ここで，N は G の正規部分群であるから，任意の $x \in G$ に対して，

$$\begin{aligned} & P \subset N \\ \Longrightarrow\ & xPx^{-1} \subset xNx^{-1} = N \end{aligned}$$

よって，Sylow の第 2 定理により，任意の 2 つの pSylow 群は共役であるから，N は任意の pSylow 群を含む． □

p105.4

Proof. 有限群の任意の p 部分群はある pSylow 群に含まれるので，$K \subset P$ となる G の pSylow 群 P がとれる．

ここで，K は正規であるから，任意の $x \in G$ に対して，

$$K = xKx^{-1} \subset xPx^{-1}$$

ゆえに Sylow の第 2 定理により，位数が p のべきの正規部分群 K は，任意の pSylow 群に含まれる． □