

5 代数系の基礎 (3) – 置換と対称群 –

• 5-1: 置換

定義 5.1. 自然数 n に対して, n 個の文字の集合を $X_n = \{1, 2, \dots, n\}$ とおく. X_n から X_n への全単射写像 $\rho: X_n \rightarrow X_n$ を [n 文字の置換](#), または単に [置換](#) という. n 文字の置換の全体の集合を S_n で表す.

置換 $\rho \in S_n$ によって, $\rho(1) = p_1, \rho(2) = p_2, \dots, \rho(n) = p_n$ であるとき, 置換 ρ を

$$\rho = \begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix}$$

というように表す. ρ は全単射なので, 下段の数列 $p_1, p_2, \dots, p_n$ は数列 $1, 2, \dots, n$ の順列である. 置換 $\rho \in S_n$ をひとつ決めれば, $(1, 2, \dots, n)$ の順列がただ一つ定まるので $|S_n| = n!$ である.

上の表記は写像による文字の対応を表しているだけなので, 上下の組合せさえ変えなければ, 各列の書く順序は換えても良い. また, 何文字の置換であるかが明らか場合は, $\rho(i) \neq i$ となる対応のみを記せば十分である. 例えば, 4 文字の置換 $\rho \in S_4$ について,

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix}$$

としてもよい.

置換 $\varepsilon \in S_n$ が, $\varepsilon(i) = i$ ($i = 1, 2, \dots, n$) であるとき ε を [恒等置換](#) という.

$$\varepsilon := \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

n 文字の置換 $\rho \in S_n$ は全単射なので, 逆写像 $\rho^{-1}: X_n \rightarrow X_n$ が存在して, ρ^{-1} はまた n 文字の置換となる. これを ρ の [逆置換](#) という.

$$\rho = \begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix}, \quad \rho^{-1} = \begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

$n \geq 2$ であるとき, n 文字の置換で 2 つの文字 i, j を入れ替えて, 他の文字は自身に写す置換を [互換](#) といい, $\begin{pmatrix} i & j \end{pmatrix}$ で表す. 特に $\begin{pmatrix} i & i+1 \end{pmatrix}$ を [隣接互換](#) と呼ぶ.

$$\begin{pmatrix} i & j \end{pmatrix} := \begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & n \\ 1 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$$

明らかに,

$$\begin{pmatrix} i & j \end{pmatrix} = \begin{pmatrix} j & i \end{pmatrix} \quad \begin{pmatrix} i & j \end{pmatrix}^{-1} = \begin{pmatrix} i & j \end{pmatrix}$$

が成り立つ.

例 5-1 (1) $n = 2$ のとき, S_2 は次の 2 つの元からなる集合である.

$$\varepsilon = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

(2) $n = 3$ のとき, S_3 は次の 6 つの元からなる集合である.

$$\begin{aligned} \varepsilon &:= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \sigma_1 &:= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & \sigma_2 &:= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \\ \tau_1 &:= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & \tau_2 &:= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, & \tau_3 &:= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \end{aligned}$$

● 5-2: 置換の積

2 つの n 文字の置換 $\sigma, \tau \in S_n$ に対して, これらの合成写像

$$\sigma\tau := \sigma \circ \tau : X_n \longrightarrow X_n, \quad \sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}$$

は再び n 文字の置換となる. この $\sigma\tau$ を σ と τ の **積** という.

例 5-2 S_3 において, σ_1 と τ_1 の積を計算してみよう.

$$\sigma_1\tau_1(1) = \sigma_1(1) = 2, \quad \sigma_1\tau_1(2) = \sigma_1(3) = 1, \quad \sigma_1\tau_1(3) = \sigma_1(2) = 3$$

だから

$$\sigma_1\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau_3$$

である. また,

$$\tau_1\sigma_1(1) = \tau_1(2) = 3, \quad \tau_1\sigma_1(2) = \tau_1(3) = 2, \quad \tau_1\sigma_1(3) = \tau_1(1) = 1$$

だから

$$\tau_1\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_2$$

である. 特に, $\sigma_1\tau_1 \neq \tau_1\sigma_1$ である.

補題 5.2. 写像 $f: X \rightarrow Y, g: Y \rightarrow Z, h: Z \rightarrow W$ に対して,

$$(h \circ g) \circ f = h \circ (g \circ f)$$

が成り立つ. すなわち, 写像の合成は結合法則を満たす.

証明. 任意の $x \in X$ に対して,

$$(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x))), \quad h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x)))$$

だから $(h \circ g) \circ f(x) = h \circ (g \circ f)(x)$ が示された. $x \in X$ は任意だったので, 写像として $(h \circ g) \circ f = h \circ (g \circ f)$ である. $\square$

定理 5.3. 代数系 $(S_n, \circ)$ は群である. このようにして群とみなした S_n を **n 次対称群** と呼ぶ.

証明. S_n における写像の合成が (G1), (G2), (G3) を満たすことを示せば良い.

(G1): **補題 5.2** より, 写像の合成は結合法則を満たすので, 任意の $\sigma, \tau, \rho \in S_n$ に対して $(\sigma\tau)\rho = \sigma(\tau\rho)$ である.

(G2): 恒等置換 $\varepsilon \in S_n$ と任意の置換 $\rho \in S_n$ との積を計算すると

$$\begin{aligned} \rho\varepsilon &= \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix} = \rho \\ \varepsilon\rho &= \begin{pmatrix} \rho(1) & \rho(2) & \cdots & \rho(n) \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(1) & \rho(2) & \cdots & \rho(n) \end{pmatrix} = \rho \end{aligned}$$

である. 恒等置換 ε は代数系 $(S_n, \circ)$ の単位元である.

(G3): 任意に $\rho \in S_n$ に対して, この逆置換 ρ^{-1} を考えれば

$$\rho\rho^{-1} = \rho^{-1}\rho = \varepsilon$$

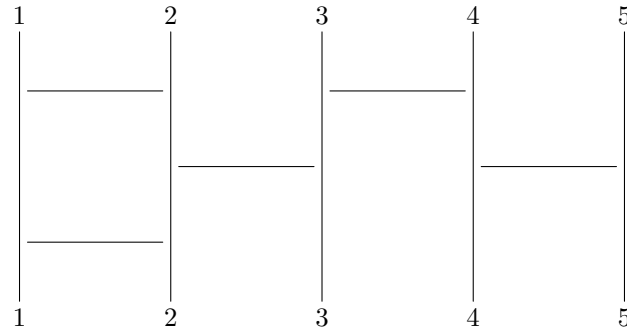
となる. 従って, ρ の逆元は ρ^{-1} である.

以上で代数系 $(S_n, \circ)$ は群である. $\square$

● 5-3: あみだくじ

あみだくじとは、平行な縦棒を何本か引き、隣同士の縦棒を結ぶ横線をいくつか書き加えたものである。本来、あみだくじを用いるときは上端に名前を書き、下端に当たりハズレなどを書くのだが、ここでは上端と下端には $1, 2, \dots, n$ の n 個の文字を振ることにする。あみだくじでは、上端から下に向かって進み、途中の横線は必ず通過して隣の縦棒に移る。

縦棒が n 本のあみだくじの結果は、数列 $1, 2, \dots, n$ の順列であるから、あみだくじは n 文字の置換を定める。



上の例では 5 文字の置換 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$ を与えていることになる。そこで次の疑問が自然に湧いてくる。

任意の置換 $\rho \in S_n$ は、縦棒が n 本のあみだくじで実現することができるだろうか。すなわち、 $n!$ 通り全ての置換をあみだくじで実現出来るだろうか。可能であれば、どのように構成すればよいだろうか。

● 5-4: あみだくじによる実現

補題 5.4. 縦棒が n 本のあみだくじにおいて、上端にある任意の数 i を左端に到達させるあみだくじを構成することができる。

証明. $i = 1$ であれば、横棒を引く必要なく左端に到達する。 $i > 1$ とすると、まず i 番目の縦棒と $i - 1$ 番目の縦棒の間に横線①を引く。 $i = 2$ であれば、これで左端に到達する。 $i > 2$ であれば、 $i - 1$ 番目の縦棒と $i - 2$ 番目の間に横線②を、横線 ① より下の位置にくるように引く。 $i = 3$ であれば、これで到達する。 $i > 3$ であれば、以下、帰納的に $i - 1$ 本の横棒を引いていけば、左端に到達することになる。□

これにより、先の問の答えは「Yes」となることがわかる。

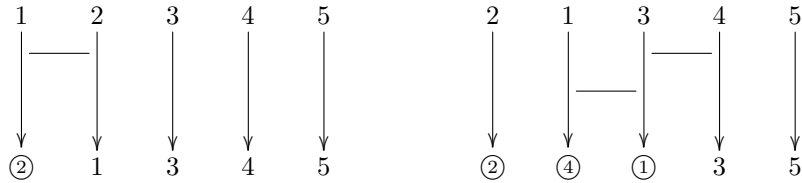
定理 5.5. 任意の置換 $\rho \in S_n$ は、縦棒が n 本のあみだくじで実現することができる。

証明. 置換 ρ が

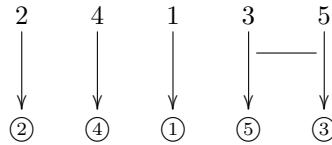
$$\rho = \begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix}$$

であるとする。今、 $p_{k_1} = 1$ であるとする、**補題 5.4** によって k_1 を左端に到達させるように横線を $k_1 - 1$ 本引く。次に、2 番目から n 番目の縦棒のあみだくじに着目すれば、上端の $1, 2, \dots, k_1 - 1, k_1 + 1, \dots, n$ がどこかに到達しているはずである。このとき、 $p_{k_2} = 2$ 、上端にあった k_2 が ℓ_1 番目の縦棒に到達していれば、 ℓ_1 を 2 番目の縦棒に到達するように横線を、これまでに引いた横線よりも下の位置にくるように引く。次に、3 番目から n 番目の縦棒のあみだくじに着目すれば、上端の数のうち k_1, k_2 以外がどこかに到達しているはずである。このとき、 $p_{k_3} = 3$ 、上端にあった k_3 が ℓ_2 番目の縦棒に到達していれば、 ℓ_2 を 3 番目の縦棒に到達するように横線を、これまでに引いた横線よりも下の位置にくるように引く。以下これを繰り返せばよい。□

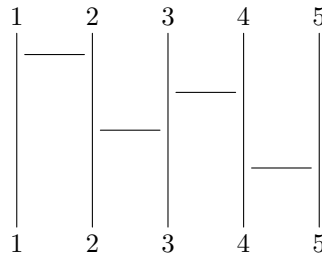
例 5-3 5 文字の置換 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$ を実現するあみだくじを構成しよう. これを作るには, 左端から順番に「2」「4」「1」「5」「3」と到達するように横線を順にを引けば良い. まずは「2」を左端に到達させるように横線を引き, 次にこれの続きで「4」を 2 番目に到達するように横線を引く.



このとき「1」は 3 番目に到達している. 次にこの続きで「5」を 4 番目に到達するように横線を引く.



とすればいい. これらを縦に繋げることで $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$ を実現するあみだくじを構成することができた.



● 5-5: 偶置換, 奇置換

定理 5.5 によれば, 任意の置換はあみだくじで実現できる. ところで, あみだくじで横線を引く操作は, 隣り合っている数字の場所を交換することに相当する. つまり, **あみだくじは, 隣り合う数字の互換を何度か実行したもの** に他ならない. よって, 次が成り立つことが結論付けられる.

命題 5.6. 任意の置換はいくつかの隣接互換の積で表すことができる. すなわち,

$$\forall \rho \in S_n, \exists t \in \mathbb{N} \text{ (s.t.) } \exists (i_1, \dots, i_t) \in \{1, 2, \dots, n-1\}^t \text{ (s.t.) } \rho = (i_1, i_1 + 1)(i_2, i_2 + 1) \cdots (i_t, i_t + 1).$$

置換を隣接互換で表すとき, その表し方は一意的ではない. 例えば

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \ 2)(2 \ 3)(1 \ 2) = (2 \ 3)(1 \ 2)(2 \ 3)$$

などである. しかし, **隣接互換の積で表したときの数の偶奇は表し方に依存せず決まる.**

定義 5.7. 置換 ρ が偶数個の隣接互換の積で表せるとき, ρ を **偶置換** という. 置換 ρ が奇数個の隣接互換の積で表せるとき, ρ を **奇置換** という.

小テスト 5-1 次の記述が正しいければ ○, 間違っていれば × を選択せよ.

- (1) 5 文字の置換は全部で 120 個存在する.
- (2) 置換 σ と τ の積 $\sigma\tau$ による 1 の行き先を計算するには, まず $\sigma(1)$ を計算して, その結果を τ で計算すれば良い.
- (3) 3 文字の置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ の逆置換は $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ である.
- (4) 縦棒が n 本のあみだくじは置換に対応し, 任意の置換はあみだくじで実現できるので, 写像 $\{\text{縦棒が } n \text{ 本のあみだくじ}\} \rightarrow S_n; \text{あみだくじ } A \mapsto A \text{ に対応する置換}$ は全単射である.
- (5) 恒等置換 ε はあみだくじで表すときに横線を引かなくてもよいから隣接互換で表すことができず, 偶置換でも奇置換でもない.

小テスト 5-2 4 文字の置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 4 \\ 4 & 1 & 2 \end{pmatrix} \in S_4$ に対して, 次の問いに答えよ.

- (1) $\sigma\sigma$ を計算せよ.
- (2) $\sigma\tau$ を計算せよ.
- (3) $\begin{pmatrix} 1 & 2 \end{pmatrix} \tau^{-1}$ を計算せよ.
- (4) $\sigma^{-1}\tau\sigma$ を計算せよ.
- (5) σ を隣接互換の積で表せ.

演習問題 5-1 3 次対称群 S_3 の演算表を作成しなさい. また, それぞれの置換に対する逆元を求めよ.

演習問題 5-2 置換 σ に対して, σ^k を $\overbrace{\sigma\sigma\cdots\sigma}^k$ と定義する. 次の置換 σ に対して, $\sigma^k = \varepsilon$ となる最小の $k > 0$ を求めよ.

- (1) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$
- (2) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 1 & 7 & 2 & 6 \end{pmatrix}$

演習問題 5-3 置換 $\sigma \in S_n$ に対して, σ の **符号** $\text{sgn}(\sigma)$ を

$$\text{sgn}(\sigma) := \begin{cases} 1 & \text{if } \sigma \text{ が偶置換,} \\ -1 & \text{if } \sigma \text{ が奇置換} \end{cases}$$

と定義する. 次の問いに答えよ. ただし, 和 $\sum_{\sigma \in S_n} b_\sigma$ は, S_n のすべての σ にわたって b_σ たちの和を表す.

- (1) 全ての 2 文字の置換 $\sigma \in S_2$ と全ての 3 文字の置換 $\tau \in S_3$ に対して, $\text{sgn}(\sigma)$ と $\text{sgn}(\tau)$ を計算せよ.
- (2) 2 次正方行列 $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ に対して, 次の値を計算せよ.

$$\sum_{\sigma \in S_2} \text{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)}$$

- (3) 3 次正方行列 $\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ に対して, 次の値を計算せよ.

$$\sum_{\sigma \in S_3} \text{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} a_{3\sigma(3)}$$

● 5-A : 隣接互換の積で表したときの数の偶奇は表し方に依存せず決まることの証明

まず注意しておきたいのは、置換はいくつかの隣接互換の積でかけることは示したが、実は必ずしも隣接互換とは限らないようないくつかの互換の積で表すことができる。もちろん、隣接互換は互換なので、**命題 5.6** は、「任意の置換はいくつかの互換の積で表すことが出来る」という主張よりも条件が強い。

では、隣接互換の積で表したときの数の偶奇は表し方に依存せず決まることを証明しよう。直接証明する方法もあるが、ここでは多項式の「差積」を使う方法を紹介する。 n 変数 $x_1, \dots, x_n$ の **差積** とは、 $1 \leq i < j \leq n$ となる全ての i, j について $(x_i - x_j)$ の積をとった n 変数多項式であり、これを $\Delta(x_1, \dots, x_n)$ で表す。

$$\Delta(x_1, \dots, x_n) := \prod_{1 \leq i < j \leq n} (x_i - x_j) = \underbrace{(x_1 - x_2) \cdots (x_1 - x_n)}_{i=1 \text{ の部分}} \underbrace{(x_2 - x_3) \cdots (x_2 - x_n)}_{i=2 \text{ の部分}} \cdots \underbrace{(x_{n-1} - x_n)}_{i=n \text{ の部分}}$$

もうひとつ概念を用意する。 n 変数 $x_1, \dots, x_n$ の多項式 $P(x_1, \dots, x_n)$ と置換 $\sigma \in S_n$ が与えられたとき、この変数 $x_1, \dots, x_n$ に $x_{\sigma(1)}, \dots, x_{\sigma(n)}$ を代入して得られる新たな多項式を σP で表すことにしよう。つまり、

$$(\sigma P)(x_1, \dots, x_n) = P(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

である。このとき、任意の置換 $\sigma, \tau \in S_n$ に対して $(\sigma\tau)P = \sigma(\tau P)$ である。実際、

$$\begin{aligned} \sigma(\tau P)(x_1, \dots, x_n) &= \tau P(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \\ &= P(x_{\tau(\sigma(1))}, \dots, x_{\tau(\sigma(n))}) \\ &= P(x_{\tau\sigma(1)}, \dots, x_{\tau\sigma(n)}) \\ &= (\sigma\tau)P(x_1, \dots, x_n) \end{aligned}$$

である。

さて、隣接互換 $\sigma \in S_n$ に対して、

$$\sigma\Delta = -\Delta$$

が成り立つ。これは次のように証明することができる。 $\sigma = (i \ i+1)$ であるとする。このとき、 $\sigma\Delta(x_1, \dots, x_n)$ は $\Delta(x_1, \dots, x_n)$ の因数の中で x_i と x_{i+1} を入れ替えたものである。そこで変化する因数を全て拾い出してみよう。まず、 $(x_k - x_i)$ と $(x_k - x_{i+1})$ ($k = 1, 2, \dots, i-1$) が σ によって互いにうつる。また、 $(x_i - x_\ell)$ と $(x_{i+1} - x_\ell)$ ($\ell = i+2, i+3, \dots, n$) も σ によって互いにうつる。最後に、 $(x_i - x_{i+1})$ は σ によって $(x_{i+1} - x_i) = -(x_i - x_{i+1})$ にうつる。この部分は σ によって (-1) 倍されることがわかり、全体として $\sigma\Delta = -\Delta$ が成り立つことがわかった。

以上で証明を実行するための準備はすべて整ったので、証明にうつろう。

定理. 任意の $\sigma \in S_n$ をいくつかの隣接互換の積で表したとき、その個数の偶奇は表し方に依らない。

証明. $\sigma \in S_n$ が隣接互換 $\tau_1, \tau_2, \dots, \tau_s, \rho_1, \rho_2, \dots, \rho_t$ を用いて以下のように 2 通りで表されていたとする。

$$\sigma = \tau_1\tau_2 \cdots \tau_s = \rho_1\rho_2 \cdots \rho_t$$

このとき、

$$\sigma\Delta = (\tau_1\tau_2 \cdots \tau_s)\Delta = (\tau_1\tau_2 \cdots \tau_{s-1})(\tau_s\Delta) = -(\tau_1\tau_2 \cdots \tau_{s-1})\Delta = \cdots = (-1)^s\Delta$$

であり、一方で

$$\sigma\Delta = (\rho_1\rho_2 \cdots \rho_t)\Delta = (\rho_1\rho_2 \cdots \rho_{t-1})(\rho_t\Delta) = -(\rho_1\rho_2 \cdots \rho_{t-1})\Delta = \cdots = (-1)^t\Delta$$

となる。従って、 s の偶奇と t の偶奇は一致しなければならない。□