3 文字の置換． $1,2,3$ の 3 つの文字の並べ替えてみると，

$$1\,2\,3,\quad 1\,3\,2,\quad 2\,1\,3,\quad 2\,3\,1,\quad 3\,1\,2,\quad 3\,2\,1$$

の６通りの順列ができる．($\leftarrow$ 何も並べ替えないものも考える)
この並べ替えを，それぞれ

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

と書いて，3 文字の**置換** (permutation) と言う．例えば，

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

とは，$1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 1$ なる並べ替え (=置換) を表す．

定義 (n 次対称群 S_n)． 一般に，n 文字 $\{1,2,\ldots,n\}$ の置換全体の集合を S_n と書く．すなわち

$$S_n := \left\{ \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \;\middle|\; \{i_1,i_2,\ldots,i_n\} \text{ は } \{1,2,\ldots,n\} \text{ の並べ替え} \right\}$$

である．この n 文字の置換全体の集合 S_n を n **次対称群** (symmetric group of degree n) と言う．

> n 次対称群 S_n は，非常に重要な概念である**群**の例になっているので，この様な名前で呼ばれる．一般に，群とは何か (群の定義) については第７回の講義で勉強し，さらに来年度 (2 年生) の代数１では１年間を通して，群の理論 (=群論) を学ぶ．

命題． n **次対称群** S_n は $n!$ 個の元からなる，すなわち集合 S_n の位数は $n!$ である．($\leftarrow \#S_n = n!$).

例． $\#S_2 = 2,\ \#S_3 = 6,\ \#S_4 = 24,\ \#S_5 = 120,\ \#S_6 = 720,\ \#S_7 = 5040,\ \#S_8 = 40320$ など．

定義 (置換の合成 (積))． 2 つの置換 $\sigma, \tau \in S_n$ に対して，新たな置換 $\sigma \circ \tau$ を

$$(\sigma \circ \tau)(i) := \sigma(\tau(i)), \quad (i = 1, \ldots, n)$$

を満たす置換として定義し，置換 $\sigma \circ \tau$ を置換 σ と置換 τ の**合成** (または**積**) という．

置換の合成 (積) の例． 2 つの置換

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

に対して，置換の合成 (積) $\sigma \circ \tau$ とは置換

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

のことであり，置換の合成 (積) $\tau \circ \sigma$ とは置換

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

のことである ($\leftarrow$ 積は右から計算する!).
特に，$\sigma \circ \tau \neq \tau \circ \sigma$ に注意する ($\leftarrow$ このことを，σ と τ は**非可換**ともいう).

定義 (巡回置換)． 置換 $\sigma \in S_n$ が，列を適当に入れ替えて (← 「適当に」の意味については教科書 p.34 を見ること)

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_{r-1} & i_r & i_{r+1} & i_{r+2} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_r & i_1 & i_{r+1} & i_{r+2} & \cdots & i_n \end{pmatrix} \in S_n$$

となるとき，すなわち 置換 $i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_r \mapsto i_1$ を引き起こすとき，置換によって動かない $i_{r+1}, \ldots, i_n$ は省略して，単に

$$\sigma = (i_1\, i_2 \cdots i_{r-1}\, i_r)$$

と表し，**長さ** r **の巡回置換** (cycle) と呼ぶ．但し，σ が何も動かさない置換のとき，すなわち

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

の場合には，$\sigma = (1)$ と書くことにする (動かないものを全て省略すると，何もなくなる為).

巡回置換の例． 置換

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 & 1 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} \in S_5$$

は置換 $2 \mapsto 4 \mapsto 3 \mapsto 2$ を表しているので，

$$\sigma = (2\,4\,3)$$

と書き，σ は長さ 3 の巡回置換である．

命題 (サイクル分解)． 任意の置換 $\sigma \in S_n$ は互いに共通の数字を含まないいくつかの巡回置換の積で書ける．この表示を σ の**サイクル分解** (cycle decomposition) とよぶ.

命題． 2 つの巡回置換 σ, τ は互いに共通の数字を含まないならば $\sigma \circ \tau = \tau \circ \sigma$．(← **可換**という).

例 (サイクル分解)． 8 文字の置換

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 8 & 7 & 2 & 3 & 1 & 6 \end{pmatrix} \in S_8$$

のサイクル分解は $\sigma = (2\,5) \circ (3\,8\,6) \circ (1\,4\,7)$ で与えられ，$\sigma = (1\,4\,7) \circ (3\,8\,6) \circ (2\,5)$ でもある．

定義 (互換, 隣接互換)． 長さ 2 の巡回置換 $(i\ j)$ を**互換** (transposition) という．互換の中でも特に，隣り合った数字からなる互換 $(i \quad i+1)$ のことを**隣接互換** (elementary transposition) という．

互換と隣接互換の例． (i) 次の置換は $3 \leftrightarrow 4$ を表しており，隣接互換である：

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix} = (3\,4) \in S_5$$

(ii) 置換 $(1\,3) \in S_3$ は $1 \leftrightarrow 3$ を表しており，互換ではあるが隣接互換ではない．
(iii) 置換

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} \in S_5$$

は互換ではないが，サイクル分解は隣接互換の積 $\sigma = (1\,2) \circ (4\,5)$ である．

演習問題 (小テストの予想問題)

[1] 置換

$$\sigma=\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix},\quad \rho=\begin{pmatrix}1&2&3&4&5\\4&2&1&5&3\end{pmatrix}$$

に対して，次の積を計算せよ．但し，答えは $\begin{pmatrix}1&2&3&4&5\\ \multicolumn{5}{|c|}{?}\end{pmatrix}$ の形で書くこと．

(i) $\sigma\circ\tau$　(ii) $\tau\circ\rho$　(iii) $\sigma\circ\rho$　(iv) $(\sigma\circ\tau)\circ\rho$　(v) $\sigma\circ(\tau\circ\rho)$

[2] 次の置換のサイクル分解 (=共通の数字を含まない巡回置換の積) を求めよ．

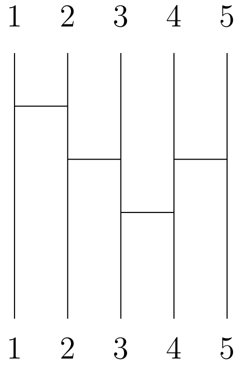
(i) $\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}$ (ii) $\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$ (iii) $\begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix}$ (iv) $\begin{pmatrix}1&2&3&4&5\\3&1&4&5&2\end{pmatrix}$

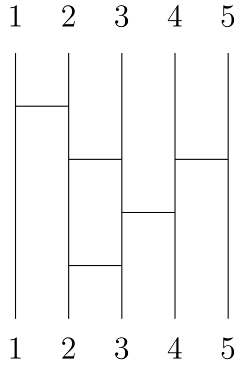
[3] 次の積を計算せよ．但し，答えは巡回置換 $(1\ \boxed{\ ?\ })$ の形で書くこと．

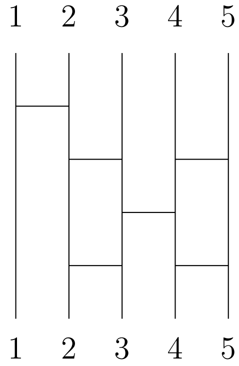
(i) $(1\,2)\circ(2\,3)$　(ii) $(1\,2)\circ(2\,3\,4)$　(iii) $(1\,2\,3)\circ(3\,4\,5)$　(iv) $(1\,2\,3\,4\,5)\circ(1\,3\,4\,2\,5)$

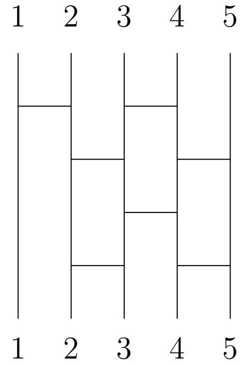
[4] (前問の (i),(ii),(iii) の様に) 巡回置換 $(1\,2\,\cdots\,n)$ はどこで切っても巡回置換の積
$(1\,2\,\cdots\,r-1\ r)\circ(r\ \ r+1\,\cdots\,n-1\ \ n)$ と等しくなるか？

[5] 縦の棒が n 本のあみだくじに，左から順に番号 $1,\ldots,n$ を付ける．このあみだくじによって $\{1,\ldots,n\}$ の置換 $\sigma\in S_n$ が１つ定まる．次のあみだくじに対応する $\sigma\in S_5$ の元は何か？
$\sigma=\begin{pmatrix}1&2&3&4&5\\ \multicolumn{5}{|c|}{?}\end{pmatrix}\in S_5$ の形とそのサイクル分解を共に答えること．

(i)


(ii)


(iii)


(iv)


[6] **問**　逆に，任意の置換 $\sigma\in S_n$ に対し，σ に対応するあみだくじは必ず存在するだろうか？

次の (i)〜(ii) を解きながら，**問**の答えを考えてみよう．また，存在する場合にはどのように作ったらよいだろうか．(ヒント　それぞれ１つ前の問を参考にしながら考えてみる)

(i)-1 巡回置換 $(1\,2\,3\,4\,5)$ に対応するあみだくじを横棒４本だけを使って作れ．
(ヒント　分からない場合には，$(1\,2),(1\,2\,3),(1\,2\,3\,4)$ と順に考えてみる)
(i)-2 巡回置換 $(1\,2\,3\,4\,5)$ を４つ隣接互換の積で書け．
(ヒント　分からない場合には，**[4]** を繰り返し使ってもよい)
(i)-3 長さ r の巡回置換 $(j_1\,j_2\,\cdots\,j_r)$ は $r-1$ 個の互換の積で表せる事を示せ (具体的に書く)．
(i)-4 一般に，置換 $\sigma\in S_n$ はいくつかの互換の積で表せる事を説明せよ．

(ii)-1 互換 $(1\,5)$ に対応するあみだくじを横棒を７本で４種類以上書け．
(ヒント　分からない場合にはまず，$(1\,2),(1\,3),(1\,4)$ と徐々に数字を離してみる)
(ii)-2 互換 $(1\,5)$ を７つ隣接互換の積として $(1\,2)\circ\boxed{\ ?\ }\circ(1\,2)$ の形で表せ．
(ii)-3 一般に，任意の互換 $(i\,j)$ は隣接互換の積で表される事を，実際に書いて示せ．

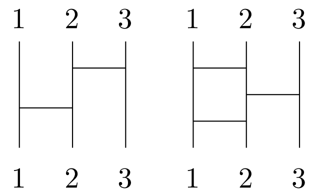
(iii) **問**の答えを書き，なぜかを (分かりやすく) 説明せよ．

(iv) 上記 (i)-(iii) を参考にして，次の置換に対応するあみだくじを実際に書け．但し，取り除ける横棒 (連続した横棒 $|\!\!=\!\!|$ など) は取り除いて，出来る限り横棒の数を少なくすること．
(iv)-1　$(1\,2\,3\,5\,4)$　(iv)-2　$(1\,3\,2\,4\,5)$　(iv)-3　$(1\,5\,3\,4\,2)$

あみだくじの原理　任意の置換 $\sigma \in S_n$ に対し，σ に対応するあみだくじが存在する．

あみだくじの原理は次の (I),(II),(III) から従う．
(I) 任意の置換 $\sigma \in S_n$ は互いに共通の数字を含まない，
幾つかの巡回置換の積で書ける (=サイクル分解)．
(II) 長さ r の巡回置換 $(j_1\ j_2\ \cdots j_r)$ は $r-1$ 個の互換の積で書ける．
(III) 任意の互換 $(i\ j)$ は隣接互換の積で書ける．

例　(1 2 3)　(1 3)



特に，(II) 及び (III) は次の命題から従い，あみだくじを具体的に作る事が可能である．

命題 (大根切りの法則)． 長さ r の巡回置換 $\sigma = (j_1\ j_2\ \cdots j_r)$ は $r-1$ 個の互換の積で書ける：

$$\sigma = (j_1\ j_2) \circ (j_2\ j_3) \circ \cdots \circ (j_{r-2}\ j_{r-1}) \circ (j_{r-1}\ j_r).$$

命題 (回文の法則)． 任意の互換 $\sigma = (i\ j),\ i < j$ は隣接互換の積によって (回文のようにして)

$$\sigma = (i\ i+1) \circ (i+1\ i+2) \circ \cdots \circ (j-2\ j-1) \circ (j-1\ j) \circ (j-2\ j-1) \circ \cdots \circ (i+1\ i+2) \circ (i\ i+1)$$

と表せる．特に，$k := j - i$ とすれば σ は $2k-1$ 個の隣接互換の積である．

注意．「大根切りの法則」と「回文の法則」は私が勝手につけた名前なので，この授業以外では決して使ってはいけない．横棒を減らすテクニックである,「連鎖」「回転大根切り」は授業内で！

レポート課題 (提出期限 5 月 6 日)

[1] **(全員提出) 課題名「教科書の前半部分の感想」**
教科書の 77 ページまでを最低 3 回以上読み，感想を提出する．その際，自分が納得できたことあるいは理解できた部分を 5 つ以上挙げて，具体例とともに記号やその使い方について説明を加えること (どの部分についてなのかとページ数を明らかにすること)．

[2] (自由提出) 課題名「フェルマーの最終定理について調べたこと」を提出する．また，自分なりの考察を加えて提出することがのぞましい．例えば,「$n \geq 3$ 以上の整数に対して $x^n + y^n = z^n$ を満たす自然数の組 $(x, y, z) \in \mathbb{N}^3$ が存在しないことを示すには，n が 4 のとき及び n が奇素数の場合のみを示せば十分である (教科書 p.48 参照)」「$n = 3$ のとき，$x^3 + y^3 = z^3$ をみたす自然数の組 $(x, y, z) \in \mathbb{N}^3$ は存在しないことを示す」など．

[3] (自由提出) 課題名「ピタゴラスの定理についての考察」$x^2 + y^2 = z^2$ を満たす自然数の組 (x, y, z) は無限にあり，またどのようにしたら全て得られるかをレポートとしてまとめて提出する．

[4] (自由提出) 課題名「素数は無限にあるか？」に答え，証明する．また，100 までの素数を全て見つけ，(i) 4 で割って 1 余る素数，(ii) 4 で割って 3 余る素数，はどちらが多いかを答える．200 まではどうか？ より一般に，(i) と (ii) について成り立つことを予想し，出来れば証明する．

レポート提出に関する注意事項

(1) A4 用紙に表紙を付け，表紙には**課題名・氏名・学籍番号・課題提出日**を明記する (学部のレポート用表紙を用いてもよい)．自由提出は 3 つの内 2 つまで．また，2 つ以上の課題は別々に出すこと．
(2) レポートは自分のノートとは違い，他人が読む事を前提にして書かなければならない．
(3) 論点を明確にし，できる限り完結にかくこと．(文章能力も問われる)
(4) 字が極端に汚い，または明らかに他人のレポートを写しただけのものは採点しない．
(5) 調べた本，Web サイトは必ず明記すること (Web の情報は間違っている事が多々あるので十分に注意を払うこと)．Web ですぐに調べられることのみを写したレポートは採点しない．
(6) 一緒に課題に取り組んだ人がいる場合には，協力者の氏名を表紙に明記すること．
(7) 提出場所は，5/6 の授業の開始前に教卓へ直接提出とする．(4/22 でも可)