$\mathbb{C}$ - ciało liczb zespolonych.

$(\mathbb{C}, +)$ - liczby zespolone z dodawaniem

$+$ - przemienne, łączne, 0, $-$.

$(\mathbb{C} \setminus \{0\}, \cdot)$ - liczby zespolone $\neq 0$ z mnożeniem

$\cdot$ - przemienne, łączne, 1, z^{-1}.

$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\} \rightsquigarrow (\mathbb{T}, \cdot)$ - przemienne, łączne, 1, u^{-1}.

$u, v \in \mathbb{T} \Rightarrow u \cdot v \in \mathbb{T}$ $\quad (\sqrt[n]{1}, \cdot)$ - skończony zbiór

Definicja: Niech G będzie zbiorem niepustym oraz $\cdot : G \times G \to G$ będzie działaniem dwuargumentowym.

Mówimy, że $(G, \cdot)$ jest grupą jeśli

i) $\exists\, e \in G \;\; \forall a \in G \quad e \cdot a = a \cdot e = a$ - istnienie elementu neutralnego.

ii) $\forall a, b, c \in G \quad (a\, b)\, c = a\, (b\, c)$ - łączność działania

iii) $\forall a \in G \; \exists\, b \in G : \; ab = ba = e$.

Jeśli $\forall a, b \in G$ mamy $a \cdot b = b \cdot a$ to mówimy, że $(G, \cdot)$ jest grupą przemienną.

Grupa permutacji S_n zbioru $\{1, \ldots, n\}$.

$S_n = \{ \sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ gdzie σ jest bijekcją $\}$.

σ jest bijekcją jeśli istnieje $\varrho : \{1, \ldots, n\} \to \{1, \ldots, n\}$ i że $\varrho \circ \sigma = id$ & $\sigma \circ \varrho = id$

ϱ nazywamy odwrotnością σ i oznaczamy σ^{-1}

Działanie w S_n jest składaniem bijekcji

Dla $\sigma_1, \sigma_2 \in S_n$ definiujemy $\sigma_1 \circ \sigma_2$ t. że

$(\sigma_1 \circ \sigma_2)(i) = \sigma_1(\sigma_2(i))$ dla $i \in \{1, \ldots, n\}$

Element neutralny: $e \in S_n$ $\quad e = id \quad id(i) = i$.

Element odwrotny: ϱ jest elementem odwrotnym do σ jest takie, że $\varrho(\sigma(i)) = i$.

Łączność: $\sigma_1 \circ (\sigma_2 \circ \sigma_3)(i) = \sigma_1((\sigma_2 \circ \sigma_3)(i)) = \sigma_1(\sigma_2(\sigma_3(i)))$

$((\sigma_1 \circ \sigma_2) \circ \sigma_3)(i) = (\sigma_1 \circ \sigma_2)(\sigma_3(i)) = \sigma_1(\sigma_2(\sigma_3(i)))$

Liczba elementów grupy $S_n = n!$ Np $|S_3| = 3! = 6$.

Elementy $S_3 = \left\{ \begin{pmatrix} 1 2 3 \\ 1 2 3 \end{pmatrix}, \begin{pmatrix} 1 2 3 \\ 2 1 3 \end{pmatrix}, \begin{pmatrix} 1 2 3 \\ 3 2 1 \end{pmatrix}, \begin{pmatrix} 1 2 3 \\ 1 3 2 \end{pmatrix}, \begin{pmatrix} 1 2 3 \\ 2 3 1 \end{pmatrix}, \begin{pmatrix} 1 2 3 \\ 3 1 2 \end{pmatrix} \right\}$

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

Wniosek S_3 jest grupą nieprzemienną

$$\neq$$

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

Stwierdzenie. Niech $(G,\cdot)$ będzie grupą oraz $f\in G$ spełnia $af=f\cdot a=a$ dla wszystkich $a\in G$ to $f=e$

Jeśli $a\cdot b=e=ba$ & $a\tilde{b}=\tilde{b}a=e$ to $b=\tilde{b}$.

Dowód Zauważmy, że $e=ef=f$.

Dalej $b=b\cdot e=b(a\tilde{b})=(ba)\cdot\tilde{b}=e\tilde{b}=\tilde{b}$ $\boxtimes$

Definicja jeśli $a,b\in G$ oraz $ab=b\cdot a=e$ to b nazywamy elementem odwrotnym a i oznaczamy $b=a^{-1}$.

Własności ($G\ni a\mapsto a^{-1}\in G$)

(1) $(a^{-1})^{-1}=a$, (2) $(ab)^{-1}=b^{-1}a^{-1}$ dla wszystkich $a,b\in G$.

(3) jeśli $a\cdot x=ay\Rightarrow x=y$ (4) jeśli $x\cdot a=y\cdot a\Rightarrow x=y$.

Definicja

Mówimy, że $\sigma\in S_n\setminus\{e\}$ jest cyklem długości k jeśli istnieją różne elementy $\{i_1,\dots,i_k\}\subset\{1,\dots,n\}$ t. że.

- gdy $i\notin\{i_1,\dots,i_k\}$ to $\sigma(i)=i$.
- gdy $i=i_j$ $j=1,\dots,k$ to $\sigma(i_j)=\begin{cases}i_{j+1} & j\neq k\\ i_1 & j=k\end{cases}$

Cykl zadany j.w. oznaczamy symbolem $\sigma=(i_1,i_2,\dots,i_k)$. Cykl długości 2 nazywamy transpozycją

$S_3=\{id,(12),(13),(23),(123),(132)\}$

Mówimy, że cykle $\sigma=(i_1,\dots,i_k)$ oraz $\varrho=(j_1,\dots,j_l)$ są rozłączne jeśli $\{i_1,\dots,i_k\}\cap\{j_1,\dots,j_l\}=\phi$.

Zauważmy, że wówczas $\sigma\circ\varrho=\varrho\circ\sigma$ (Np $(12)(34)=(34)(12)=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$)

Twierdzenie Każda permutacja $\sigma\in S_n\setminus\{e\}$ jest złożeniem cykli rozłącznych.

Dowód: Niech $i\in\{1,\dots,n\}$: $\sigma(i)\neq i$. Rozważmy $\{\sigma^k(i): k\in\mathbb{N}\}$

$=\{i,\sigma(i),\sigma(\sigma(i)),\sigma(\sigma(\sigma(i))),\dots\}\subset\{1,\dots,n\}$

Niech $k_\sigma=\min\{k\in\mathbb{N}:\exists l<k : \sigma^k(i)=\sigma^l(i)\}$

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

Stwierdzenie. Niech $(G,\cdot)$ będzie grupą oraz $f\in G$ spełnia $a f = f\cdot a = a$ dla wszystkich $a\in G$ to $f=e$.
Jeśli $a\cdot b = e = b a$ & $a\tilde{b} = \tilde{b} a = e$ to $b=\tilde{b}$.

Dowód Zauważmy, że $e = e f = f$.

(3) jeśli $a\cdot x = a\cdot y \Rightarrow x=y$ (4) jeśli $x\cdot a = y\cdot a$

Zauważmy, że $\sigma^{k_0}(i)=i$. Rzeczywiście, jeśli $\sigma^{k_0}(i)=\sigma^{l}(i)$, $0<l<k_0$ to to $\sigma^{k_0-l}(i)=i$, i $k_0-l<k_0$ oraz spełnia warunek powyżej sprzeczność. Zatem $(i,\sigma(i),\ldots,\sigma^{k_0-1}(i))$ jest cyklem.
Jeśli $\sigma\neq(i,\ldots,\sigma^{k_0-1}(i))$ to $\exists\ j\notin\{i,\sigma(i),\ldots,\sigma^{k_0-1}(i)\}$ t. że $j\neq\sigma(j)$. Powtarzamy powyższy argument dla j-ta $\rightsquigarrow$ $(j,\sigma(j),\ldots,\sigma^{k_1-1}(j))$ - drugi cykl.
Jeśli $\{i,\sigma(i),\ldots,\sigma^{k_0-1}(i)\}\cap\{j,\sigma(j),\ldots,\sigma^{k_1-1}(j)\}\neq\emptyset$ to cykle są równe, a zatem cykle te są rozłączne.

Itd. Otrzymane w ten sposób cykle są rozłączne a σ jest ich złożeniem $\square$

Przykład

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\8&7&6&3&4&5&1&2\end{pmatrix}=(1\,8\,2\,7)(3\,6\,5\,4)$$