

GRUPY I PERMUTACJE

Działanie na zbiorze X to odwzorowanie

$$X \times X \longrightarrow X,$$

$$(x, y) \longmapsto xy.$$

Działanie nazywamy łącznym $\Leftrightarrow$

$$\forall x, y, z \in X : (xy)z = x(yz).$$

Działanie nazywamy przemienne (abelowym)

$$\Leftrightarrow \forall x, y \in X : xy = yx.$$

Elementem neutralnym działania nazywamy element $e \in X$ taki że

$$\forall x \in X : ex = x = xe.$$

Elementem odwrotnym elementu x nazywamy element x^{-1} taki że

$$xx^{-1} = e = x^{-1}x.$$

Półgrupa to niepusty zbiór z łącznym działaniem,
monoid to półgrupa z elementem neutralnym,
grupa to monoid którego każdy element jest odwracalny. $\rightarrow$

Spостrzeżenia:

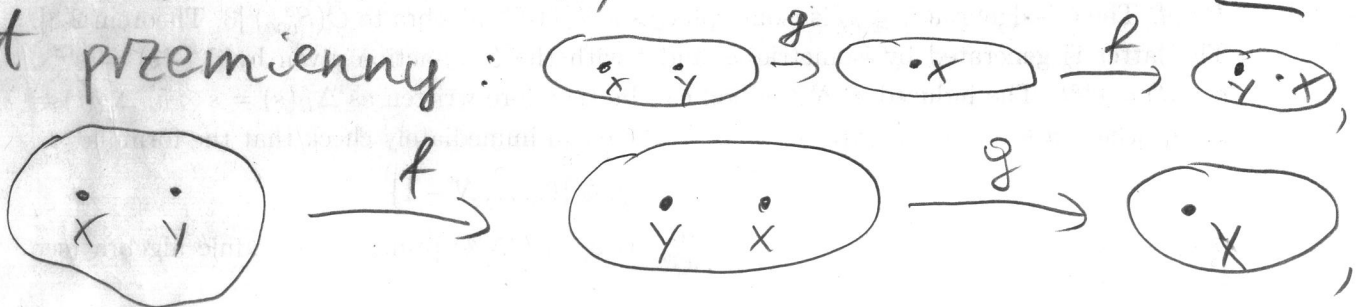
① Jeśli istnieje element neutralny, to jest jedyny: $e = e'e = e'$.

② Jeśli element monoidu jest odwracalny, to jego odwrócenie jest jedyna: $x''x = e = x'x \Rightarrow x''xx' = x'xx' \Rightarrow x'' = x'$. Stąd $(x^{-1})^{-1} = x$, oraz

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Przykłady:

① $X \neq \emptyset$, $M := \text{Map}(X, X)$, $(f \circ g)(x) := f(g(x))$, $e = \text{id}$, jest monoidem. Jeśli X ma co najmniej 2 elementy, to monoid M nie jest przemienny:



$$f(z) := \begin{cases} z & \text{dla } z \notin \{x, y\} \\ x & \text{dla } z = y \\ y & \text{dla } z = x \end{cases}, \quad g(z) = x, \quad \forall z$$

$$(f \circ g)(x) = y, \quad (g \circ f)(x) = x \Rightarrow f \circ g \neq g \circ f.$$

② Przemienne monoidy: $(2^X, \cup, \emptyset)$, $(2^X, \cap, X)$, $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$.

③ Konstrukcja Grothendiecka grup

abelowskich z półgrup przemennych:

Niech $(M, +)$ będzie przemenną półgrupą. Wtedy $G_{(M, +)} := (M \times M) / R_{(M, +)}$

$$R_{(M, +)} := \{((m, n), (p, q)) \in M^4 \mid m + q = p + n\},$$

z działaniem indukowanym danym przez $[(m, n)] + [(p, q)] := [(m + p, n + q)]$

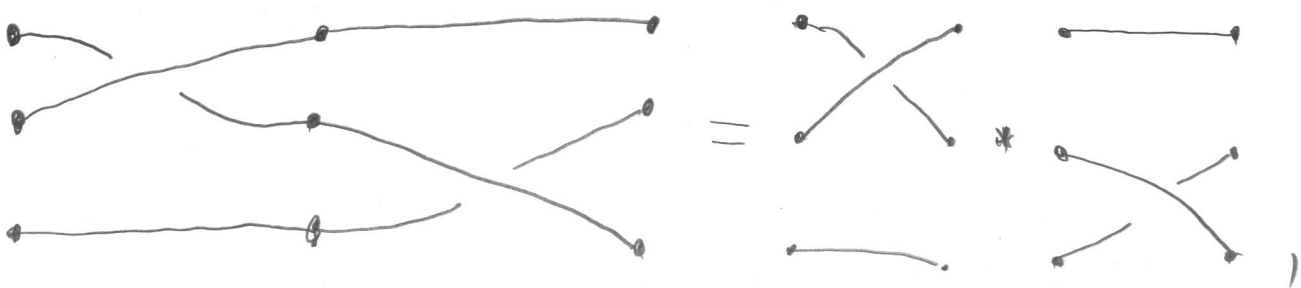
jest grupą abelową z elementem neutralnym $[(m, m)]$ i odwzorowaniem odwrotnościowym $G_M \ni [(m, n)] \mapsto [(n, m)] \in G_M$.

W szczególności $G_{(\mathbb{N}, +)} = \mathbb{Z}$, $G_{(\mathbb{N} \setminus \{0\}, \cdot)} = \mathbb{Q}^+$

$= \{r \in \mathbb{Q} \mid r > 0\}$, to grupy abelowe ze

współodpowiednio na $(+, 0)$ i $(\cdot, 1)$.

④ Grupa uarkaczy na n włosach:



$$e := \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array}, \quad \left(\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \right)^{-1} = \left(\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \right).$$

Dla $n > 1$ grupa uarkoway jest zawsze nieskończona.

⑤ $X \neq \emptyset$, $\text{Bij}(X) := \{f \in \text{Map}(X, X) \mid f \text{ jest bijectyj}\}$
 $(f, g) \mapsto f \circ g$, $e = \text{id}$, jest grupa. Jeśli X ma co najmniej
 3 elementy, to $\text{Bij}(X)$ nie jest grupą
 abelową:

$$f(a) := \begin{cases} a & \text{dla } a \notin \{x, y, z\} \\ z & \text{dla } a = x \\ x & \text{dla } a = y \\ y & \text{dla } a = z \end{cases}, \quad g(a) := \begin{cases} a & \text{dla } a \notin \{x, y, z\} \\ x & \text{dla } a = x \\ z & \text{dla } a = y \\ y & \text{dla } a = z \end{cases},$$

$(f \circ g)(x) = z \neq y = (g \circ f)(x)$. Jeśli X
 jest zbiorem skończonym, to $(\text{Bij}(X), \circ, \text{id})$
 nazywamy grupą permutacji. Jeśli $X =$
 $\{1, 2, \dots, n\}$, to jego grupę permutacji
 oznaczamy przez S_n . Grupa S_n ma
 $n! := 1 \cdot 2 \cdot \dots \cdot n$ elementów.

Na S_n możemy zdefiniować funkcję

$$S_n \ni \sigma \mapsto S(\sigma) := \prod_{\substack{i < j \\ i, j \in \{1, \dots, n\}}} (\sigma(j) - \sigma(i)) \in \mathbb{Z} \setminus \{0\}.$$

Permutację τ_{ij} , $i \neq j$, daną przez $\tau_{ij}(k) := \begin{cases} k & \text{dla } k \neq \{i, j\} \\ j & \text{dla } k = i \\ i & \text{dla } k = j \end{cases}$

nazwujemy transpozycją.

Lemat: $S(\sigma \circ \tau_{ij}) = -S(\sigma)$

Dowód: Zauważmy najpierw że $S(\sigma \circ \tau_{kk+1}) =$

$$\prod_{\substack{i < j \\ i, j \in \{1, \dots, k-1, k+2, \dots, n\}}} (\sigma(j) - \sigma(i)) \prod_{\substack{i=k, k+1 < j \leq n}} (\sigma(j) - \sigma(i)) \prod_{\substack{i=k+1 < j \leq n}} (\sigma(j) - \sigma(k))$$

$$\prod_{\substack{i < k=j}} (\sigma(k+1) - \sigma(i)) \prod_{\substack{1 \leq i < k, k+1=j}} (\sigma(k) - \sigma(i)) =$$

$$= -(\sigma(k+1) - \sigma(k)) \prod_{\substack{i, j \in \{1, \dots, k-1, k+2, \dots, n\} \\ i < j}} (\sigma(j) - \sigma(i)) \prod_{k+1 < j \leq n} (\sigma(j) - \sigma(k)) (\sigma(j) - \sigma(k+1))$$

$$\prod_{1 \leq i < k} (\sigma(k) - \sigma(i)) (\sigma(k+1) - \sigma(i)) = -S(\sigma).$$

Z drugiej strony, $\tau_{kl} = \tau_{lk}$, założymy więc $k < l$ i zauważymy że $\tau_{kl} = \tau_k \circ \tau_{k+1} \circ \dots \circ \tau_{l-1} \circ \tau_{l-2} \circ \dots \circ \tau_{k+1}$.

Stąd $S(\sigma \circ \tau_{kl}) = (-1)^{l-k+l-1-k} S(\sigma) = -S(\sigma)$. ■

Znakiem permutacji nazywamy liczbę

$$\boxed{\text{sgn}(\sigma) := \text{sign}(S(\sigma)) \in \{\pm 1\}}.$$

Lemat: Każdą permutację można przedstawić jako złożenie skończonej ilości transpozycji.

Dowód: Rozłożymy $\{1, \dots, n\}$ na klasy równoważności względem relacji $R_\sigma := \{(i, \sigma^k(i)) \mid k \in \mathbb{N}\}$.

Wtedy r_σ będzie ilością wszystkich klas równoważności. Wtedy $\sigma = \gamma_1^\sigma \circ \dots \circ \gamma_{r_\sigma}^\sigma$, gdzie

$\gamma_i^\sigma(k) := \begin{cases} k & \text{dla } k \notin [k_i] \\ \sigma(k) & \text{dla } k \in [k_i]. \end{cases}$ Z drugiej strony, $\gamma_i^\sigma = \text{id}$ lub

$\gamma_i^\sigma = \tau_{\sigma(k_i) \sigma^2(k_i)} \circ \tau_{\sigma(k_i) \sigma^3(k_i)} \circ \dots \circ \tau_{\sigma(k_i) \sigma^{m_i}(k_i)}$, gdzie m_i+1 to liczba elementów klasy $[k_i]$. ■

Na koniec zauważymy że $\exists S(\text{id}) > 0$ oraz

$$S(\sigma) = S(\text{id} \circ \sigma) = S(\text{id} \circ \tau_{i_1 j_1} \circ \dots \circ \tau_{i_k j_k}) = (-1)^k S(\text{id}),$$

wynika

Twierdzenie: $\boxed{\sigma = \tau_{i_1 j_1} \circ \dots \circ \tau_{i_k j_k} \Rightarrow \text{sgn}(\sigma) = (-1)^k}$