

GRUPY I PERMUTACJE

Piotr M. Hajac
Uniwersytet Warszawski

Wykład 2, 09.10.2013

Typeset by Jakub Szczepanik.

Działania

Definition

Działanie na zbiorze X to odwzorowanie

$$X \times X \ni (x, y) \longmapsto xy \in X.$$

Działanie nazywamy **łącznym** $\Leftrightarrow$

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

Działanie nazywamy **przemienne** (abelowym) $\Leftrightarrow$

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

Definition

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

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

Definition

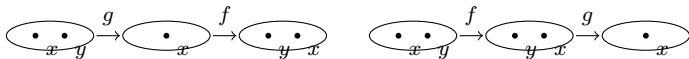
- ❶ **Półgrupa** to niepusty zbiór z łącznym działaniem.
- ❷ **Monoid** to półgrupa z elementem neutralnym.
- ❸ **Grupa** to monoid którego każdy element jest odwracalny.

Spostrzeżenia:

- ❶ Jeśli istnieje element neutralny, to jest jedyny: $e = ee' = e'$.
- ❷ Jeśli element monoidu jest odwracalny, to jego odwrotność jest jedyna: $x''x = e = x'x \Rightarrow x''xx' = x'xx' \Rightarrow x'' = x'$.
- ❸ Z jedyności odwrotności otrzymujemy $(x^{-1})^{-1} = x$ oraz $(xy)^{-1} = y^{-1}x^{-1}$.

Przemienne i nieprzemienne monoidy

- 1 Przemienne monoidy: $(2^X, \cup, \emptyset)$, $(2^X, \cap, X)$, $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$.
- 2 $X \neq \emptyset$, $M := \text{Map}(X, X)$, $(f \circ g)(x) := f(g(x))$, $e = \text{id}$, jest monoidem. Jeśli X ma co najmniej 2 elementy, to monoid M nie jest przemienny:



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

$$((f \circ g)(x) = y \quad \text{i} \quad (g \circ f)(x) = x) \implies f \circ g \neq g \circ f.$$

Konstrukcja Grothendiecka i warkocze

- 3 **Konstrukcja Grothendiecka** grup abelowych z półgrup przemiennych: Niech $(M, +)$ będzie przemienną półgrupą. Wtedy $G_M := (M \times M)/R_M$, gdzie

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

jest grupą abelową ze względu na działanie indukowane dane przez $[(m, n)] + [(p, q)] := [(m + p, n + q)]$. Elementem neutralnym jest $[(m, m)]$, a odwzorowanie odwrotnościowe to $G_M \ni [(m, n)] \mapsto [(n, m)] \in G_M$. W szczególności $G_{\mathbb{N}} = \mathbb{Z}$ oraz $G_{\mathbb{N} \setminus \{0\}} = \mathbb{Q}^+ := \{r \in \mathbb{Q} \mid r > 0\}$, to grupy abelowe odpowiednio ze względu na $(+, 0)$ i $(\cdot, 1)$.

- 4 **Grupa warkoczy** na n włosach:

$$e := \text{three parallel strands} = \left(\text{crossing} \right)^{-1} * \left(\text{crossing} \right)$$

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

Bijekcje i permutacje

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

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

Definition

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 .

Znak permutacji i transpozycje

Grupa S_n ma $n! := 1 \cdot 2 \cdot \dots \cdot n$ elementów. Na S_n możemy zdefiniować funkcję znakową

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

Definition

Znakiem permutacji σ nazywamy liczbę
 $\operatorname{sgn}(\sigma) := \operatorname{sign}(S(\sigma)) \in \{\pm 1\}.$

Definition

Transpozycją nazywamy permutację τ_{ij} , $i \neq j$, daną przez

$$\tau_{ij}(k) := \begin{cases} k & \text{dla } k \notin \{i, j\} \\ j & \text{dla } k = i \\ i & \text{dla } k = j \end{cases} .$$

Twierdzenie o znaku permutacji

Lemma

Dla każdej permutacji σ i każdej transpozycji τ_{kl} zachodzi

$$S(\sigma \circ \tau_{kl}) = -S(\sigma).$$

Lemma

Każdą permutację można przedstawić jako złożenie skończonej ilości transpozycji.

Korzystając z powyższych lematów, obliczamy

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

Stąd oraz z faktu że $S(\text{id}) > 0$ wynika teraz:

Theorem

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

Dowód lematu o znaku

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

$$\begin{aligned} &= (\sigma(k) - \sigma(k+1)) \prod_{i < j, i, j \in \{1, \dots, k-1, k+2, \dots, n\}} (\sigma(j) - \sigma(i)) \prod_{i=k, k+1 < j \leq n} (\sigma(j) - \sigma(k+1)) \\ &\quad \prod_{i=k+1 < j \leq n} (\sigma(j) - \sigma(k)) \prod_{1 \leq i < k=j} (\sigma(k+1) - \sigma(i)) \prod_{1 \leq i < k, k+1=j} (\sigma(k) - \sigma(i)) \\ &= -(\sigma(k+1) - \sigma(k)) \prod_{i < j, i, j \in \{1, \dots, k-1, k+2, \dots, n\}} (\sigma(j) - \sigma(i)) \\ &\quad \prod_{k+1 < j \leq n} (\sigma(j) - \sigma(k)) (\sigma(j) - \sigma(k+1)) \prod_{1 \leq i < k} (\sigma(k+1) - \sigma(i)) (\sigma(k) - \sigma(i)) \\ &= -S(\sigma). \end{aligned}$$

Z drugiej strony, ponieważ $\tau_{kl} = \tau_{lk}$, bez straty ogólności założmy że $k < l$, i zauważmy że

$$\tau_{kl} = \tau_{kk+1} \circ \tau_{k+1, k+2} \circ \dots \circ \tau_{l-1, l} \circ \tau_{l-2, l-1} \circ \dots \circ \tau_{k, k+1}.$$

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

Dowód lematu o przedstawieniu

Dowód: Niech $\sigma \in S_n$. Rozłóżmy $\{1, \dots, n\}$ na klasy równoważności względem relacji

$$R_\sigma := \left\{ (i, \sigma^k(i)) \mid i \in \{1, \dots, n\}, k \in \mathbb{N} \right\}.$$

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

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

(Takie permutacje nazywamy cyklami.)

Z drugiej strony, $\gamma_i^\sigma = \text{id}$ lub

$$\gamma_i^\sigma(k) = \tau_{\sigma^{m_i-1}(k_i)\sigma^{m_i}(k_i)} \circ \dots \circ \tau_{\sigma(k_i)\sigma^2(k_i)} \circ \tau_{k_i\sigma(k_i)},$$

gdzie $m_i + 1$ to liczba elementów klasy $[k_i]$. ■