WZFT I

I Wegstad

Definicja grupy

Zbiór elementów $G = \{a, b, \dots\}$ z działaniem, które spełnia następujące warunki

$G0: \forall a,b \in G \quad ab \in G$

$G1: \forall a,b,c \in G \quad a(bc) = (ab)c$

$G2: \exists e \in G \; \forall a \in G \quad ae = ea = a$

$G3: \forall a \in G \; \exists a^{-1} \in G : a a^{-1} = a^{-1} a = e$

Przykłady

Trywialne

- $\{1\}$ z mnożeniem $\qquad \{e\}$
- $\{0\}$ z dodawaniem
- $\{1, -1\}$ z mnożeniem $\qquad \{e, b\}, b^2 = e$
- Z_2, C_2

Mniej trywialne:

- dodatnie liczby wymierne z mnożeniem
- przedział $(2, +\infty)$ z działaniem $a \circ b = ab - 2a - 2b + 6$
- pary liczb rzeczywistych $(a,b) \neq (0,0)$ z działaniem $(a,b) \circ (c,d) = (ac - bd, bc + ad)$

• C_n, $n \geq 3$

Elementami grupy są obroty o kąt $\frac{2\pi r}{n}$ ($r=0,1,\ldots,n-1$) wokół osi prostopadłej do wieloboku i przechodzącej przez jego środek. Oznaczając c – obrót o $\frac{2\pi}{n}$,

mamy $c_n^r = (c)^r$, $c^n = c^0 = e$

$$G = \{e, c, c^2, c^3, \ldots, c^{n-1}\}$$

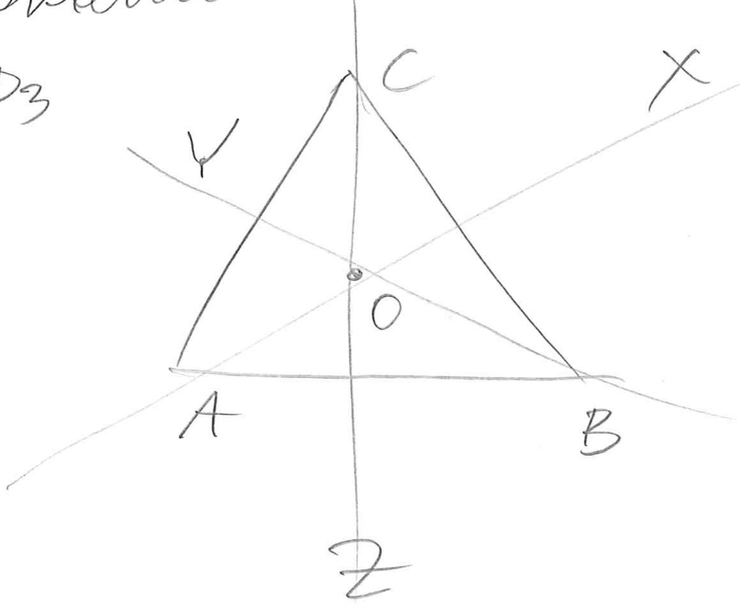
$$c^r c^{r'} = c^{r+r'} = c^{r'+r} = c^{r'} c^r$$

Grupa C_n jest więc przemienna (abelowa)

• D_n, $n \geq 3$

Grupa przekształceń regularnego wieloboku z n nieskierowanymi bokami

D_3



c – obrót o $\frac{2\pi}{3}$ wokół osi prostopadłej do $\triangle ABC$ i przechodzącej przez punkt O

b_1 – obrót o π wokół osi OX

b_2 – obrót o π wokół osi OY

b_3 – obrót o π wokół osi OZ

$b_1 = b$

$b_2 = bc$, $b_3 = bc^2$

$D_3 = gp\{b, c\}$, $b^2 = c^3 = e = (bc)^2$

$D_3 = \{e, c, c^2, b, bc, bc^2\}$, $|D_3| = 6$

Uwaga:

Definiowana jest nawet grupa D_2:

$D_2 = gp\{b, c\}$, $b^2 = c^2 = e = (bc)^2$

$D_2 = \{e, c, b, bc\}$, $|D_2| = 4$

Grupa permutacji S_n

$P = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix}$ $\qquad PQ$ najpierw

$Q = \begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$

Na ogół $PQ \neq QP$

Składanie permutacji na ogół nie jest przemienne!

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

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

$e = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 1 & 2 & \dots & n-1 & n \end{pmatrix}$

$P^{-1} = \begin{pmatrix} p_1 & p_2 & \dots & p_{n-1} & p_n \\ 1 & 2 & \dots & n-1 & n \end{pmatrix}$

Rozkład permutacji na cykle rozłączne

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

$$(1 \to 2 \to 4 \to 1), \quad (3 \to 3)$$

$$P = (124)(3) = (124)$$

Jeśli czegoś nie zapisujemy, dana liczba nie jest zmieniana

- Dowolna permutacja może być zapisana jako iloczyn rozłącznych cykli, które ze sobą komutują (mogą być zapisane w dowolnej kolejności)

- $S_2 = \{e, P_{12}\}$, $C_2 = \{e, c\}$

  $P_{12}P_{12} = e$, $c^2 = e$

  S_2 i C_2 mają identyczne właściwości

- $S_3 = \{e \equiv (\,), (12), (13), (23), (123), (132)\}$

  $D_3 = \{e, b, bc, bc^2, c, c^2\}$, $b^2 = c^3 = (bc)^2 = e$

  S_3 i D_3 mają te same właściwości, można zestawić pary elementów obu grup z zachowaniem ich działania grupowego

  Mówimy, że S_3 i D_3 są izomorficzne i zapisujemy $S_3 \cong D_3$

Transpozycja to cykl dwuelementowy $P_{ij} = (ij)$. Dowolna permutacja może być zbudowana z iloczynów transpozycji. Weźmy cykl

$$(n_1 n_2 \dots n_r) = \underbrace{(n_1 n_2)(n_2 n_3) \cdots (n_{r-1} n_r)}_{\text{iloczyn } r-1 \text{ zachodzących na siebie transpozycji}}$$

Cykl o długości r jest parzysty (nieparzysty) jeśli r jest nieparzyste (parzyste).

Rozkład dowolnej permutacji na cykle rozłączne pozwala określić jej parzystość. Na przykład

$(3\,4\,7)(1\,2)(5\,6)$

$(+1) \cdot (-1) \cdot (-1) = 1$ permutacja parzysta

$(3\,4\,7)(1\,5)$

$(+1) \cdot (-1) = -1$ permutacja nieparzysta

<u>A_n</u> podgrupa składająca się z parzystych permutacji S_n

Podgrupa H grupy G

H jest podgrupą grupy G, jeśli $H \subset G$ i jest grupą. H jest podgrupą właściwą, jeśli $H \neq \{e\}$ oraz $H \neq G$

- Nie wszystkie grupy mają właściwe podgrupy!

  D_n mają właściwe podgrupy

  $$H_2 = \{e, c\} \subset D_2 = \{e, c, b, bc\},$$
  $$b^2 = c^2 = (bc)^2 = e$$

  $$H_3 = \{e, c, c^2\} \subset D_3 = \{e, c, c^2, b, bc, bc^2\},$$
  $$b^2 = c^3 = (bc)^2 = e$$

- Twierdzenie

  Jeśli a jest elementem grupy G i n jest najmniejszą liczbą naturalną taką, że $a^n = e$, to a należy do podgrupy H grupy G, gdzie

  $$H = \{e, a, a^2, \dots, a^{n-1}\}$$

Przykład:

$G = \{1, i, -1, -i\}$ z mnożeniem, $e = 1$, $a = -1$

$(-1)^2 = 1 = e \Rightarrow \{1, -1\}$ jest podgrupą G

Twierdzenie Cayleya
(o przegrupowaniu grupy)

Każda skończona grupa G o rzędzie równym n (o n elementach) jest izomorficzna z pewną podgrupą S_n

Aby udowodnić to twierdzenie, należy przyporządkować każdemu elementowi grupy G permutację w taki sposób, aby zachowane były własności działania grupowego

$g \in G$, $G = \{a_1, a_2, \dots, a_n\}$

Zbiór $\{ga_1, ga_2, \dots, ga_n\}$ musi być równy G, gdyż $g = a_k$ dla pewnego k

Bierzemy dowolny $i \in \{1, 2, \dots, n\}$ i pytamy, czy zachodzi $a_i = g a_j$ dla jakiegoś $j \in \{1, 2, \dots, n\}$.

$$a_k^{-1} / \; a_i = a_k a_j$$

$$a_j = a_k^{-1} a_i$$

$$\{ga_1, ga_2, \dots, ga_n\} = \{a_{\pi_1}, a_{\pi_2}, \dots, a_{\pi_n}\}$$

Dlatego dla każdego elementu G istnieje permutacja

$$g \to \pi(g) = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi_1 & \pi_2 & \cdots & \pi_n \end{pmatrix}$$

Co więcej, mamy jednoznaczne przyporządkowanie $g \Leftrightarrow \pi(g)$!

Gdyby zachodziło $g a_i = g' a_i \,/\, a_i^{-1}$

$$\Rightarrow g = g'$$

To przyporządkowanie zachowuje strukturę obu grup:

$$\pi(g_2 g_1) = \pi(g_2)\pi(g_1)$$

$$\pi(g_2 g_1) \Rightarrow \{g_2 \underline{g_1 a_1}, g_2 \underline{g_1 a_2}, \dots, g_2 \underline{g_1 a_n}\}$$

$$= \{g_2 a_{\pi_1}, g_2 a_{\pi_2}, \dots, g_2 a_{\pi_n}\} =$$

$$= \{a_{\pi'\pi(1)}, a_{\pi'\pi(2)}, \dots, a_{\pi'\pi(n)}\},$$

gdzie $g_1 \Leftrightarrow \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi_1 & \pi_2 & \cdots & \pi_n \end{pmatrix}$

$$g_2 \Leftrightarrow \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi'_1 & \pi'_2 & \cdots & \pi'_n \end{pmatrix}.$$

Mamy n różnych permutacji $\pi(g_i)$, które stanowią podzbiór wszystkich $n!$ permutacji w S_n. Jest to podzbiór zamknięty ze względu na składanie permutacji, a więc podgrupa.

Elementy sprzężone w grupie i klasy sprzężenia

$a, b \in G$ są sprzężone, jeśli istnieje element $g \in G$: $a = gbg^{-1}$.

Sprzężenie stanowi relację równoważności

(1) zwrotność $\quad a \sim a$

$g = e \quad a = eae^{-1}$

(2) symetryczność

$a \sim b \iff \exists g \in G : a = gbg^{-1}$

$\iff g^{-1}ag = b \iff b = (g^{-1})a(g^{-1})^{-1}$

(3) przechodniość

$(a \sim b) \wedge (b \sim c) \Rightarrow a \sim c$

$\exists g_1, g_2 \in G : a = g_1 b g_1^{-1}$

$b = g_2 c g_2^{-1}$

$a = g_1 g_2 c g_2^{-1} g_1^{-1} = (g_1 g_2) c (g_1 g_2)^{-1}$

Klasy równoważności relacji sprzężenia dzielą grupę na rozłączne podzbiory

Przykłady

(1) C_n

Dla każdej grupy abelowej klasy sprzężenia są jednoelementowe

$$gag^{-1} = a$$

(2) D_3

(e) $\qquad e = geg^{-1}$

(c, c^2)

(b, bc, bc^2)

(3) S_n

klasy sprzężenia odpowiadają dokładnie rozkładowi na cykle!

Dowolna permutacja P może być zapisana w postaci

$$P = (a_1 a_2 \ldots a_{l_1})(b_1 b_2 \ldots b_{l_2})(c_1 c_2 \ldots c_{l_3}) \ldots$$

, porządkując długość cykli tak że $l_1 \geqslant l_2 \geqslant l_3 \ldots \geqslant l_r$, aby uzyskać tzw. partycję (rozkład) n: $l_1 + l_2 + \ldots + l_r = n$, gdzie tym razem cykle jednoelementowe muszą być zapisane explicite!

Rozważmy ogólne sprzężenie $QPQ^{-1} =$ 11

$$\begin{pmatrix} a_1 a_2 \dots a_{l_1} b_1 b_2 \dots b_{l_2} \dots \\ A_1 A_2 \dots A_{l_1} B_1 B_2 \dots B_{l_2} \dots \end{pmatrix}$$

$$(a_1 a_2 \dots a_{l_1})(b_1 b_2 \dots b_{l_2})$$

$$\begin{pmatrix} A_1 A_2 \dots A_{l_1} B_1 B_2 \dots B_{l_2} \dots \\ a_1 a_2 \dots a_{l_1} b_1 b_2 \dots b_{l_2} \end{pmatrix} =$$

$$= (A_1 A_2 \dots A_{l_1})(B_1 B_2 \dots B_{l_2}) \dots$$

Sprzężona permutacja ma dokładnie taką samą strukturę cykli!

Dlatego klasy sprzężenia S_n dane są przez wypisanie różnych partycji S_n

Przykład: partycje dla $n=3$

(1) $l_1 = l_2 = l_3 = 1$ $(\,)$

(2) $l_1 = 2,\ l_2 = 1$ $(23), (13), (12)$

(3) $l_1 = 3$ $(123), (132)$

Warstwy

$H \subset G$ jest podgrupą G. $H = \{h_1, h_2, \dots, h_r\}$
Lewą warstwą elementu $g \in G$, gH, jest zbiór $gH := \{gh_1, gh_2, \dots, gh_r\}$

(1) Liczba elementów warstwy jest równa liczbie elementów H, czyli r.

Dowód:
Liczba elementów warstwy mogłaby jedynie być mniejsza od r, gdyby zachodziło $gh_i = gh_j$.
Mnożąc z lewej strony przez g^{-1} dostalibyśmy jednak $h_i = h_j$, co nie może zachodzić!

(2) Możemy zbudować relację równoważności $a \sim b \Leftrightarrow b \in aH$

(a) zwrotność

$a \sim a$

$a \in aH$, bo H zawiera e

(b) symetryczność

$(a \sim b) \Rightarrow (b \sim a)$

$a \sim b \Leftrightarrow b \in aH \Leftrightarrow \exists i \in \{1, 2, \dots, r\}$

$b = ah_i \Leftrightarrow a = bh_i^{-1} = bh_j$,

gdzie $h_j = h_i^{-1}$. W takim razie

$a \in bH$

(3) przechodniość

$(a\sim b) \wedge (b\sim c) \Rightarrow (a\sim c)$

$a\sim b \Leftrightarrow b\in aH$

$b\sim c \Leftrightarrow c\in bH$

$b\in aH \Leftrightarrow b = ah_i\,,\ h_i\in H$

$c\in bH \Leftrightarrow c = bh_j\,,\ h_j\in H$

$c = bh_j = a\underbrace{h_ih_j}_{h_k} = ah_k,\ h_k\in H$

Dlatego $c\in aH$, więc $a\sim c$

Ta relacja równoważności dzieli grupę G na rozdzielne klasy równoważności, w tym przypadku równoliczne rozłączne warstwy!

Dla grupy skończonej możemy te warstwy ponumerować

$g_1H, g_2H, \dots, g_sH$.

Zbiór warstw oznaczamy G/H.

Przy naszych oznaczeniach mielibyśmy więc s warstw z r różnymi elementami, co oznacza że liczba elementów grupy G, $|G|$ (rząd G) można zapisać w postaci

$$|G| = s\cdot r$$

Twierdzenie Lagrange'a

Rząd podgrupy H grupy G musi być dzielnikiem rzędu grupy G.

Podgrupy normalne

Podgrupa normalna spełnia

$$\forall g \in G : gHg^{-1} = H$$

albo

$$\forall g \in G : gH = Hg$$

albo

$$h \in H \Rightarrow g h g^{-1} = h' \in H, \forall g \in G$$

Zbiór warstw podgrupy normalnej G/H może być wyposażony w strukturę grupy przez odpowiednią definicję działania na warstwach

$$(g_1 H)(g_2 H) := (g_1 g_2) H$$

Czy takie działanie stanowi grupę?

① łączność

$$(g_1 H)\left[(g_2 H)(g_3 H)\right] =$$

$$(g_1 H)(g_2 g_3) H = g_1(g_2 g_3) H =$$

$$= (g_1 g_2) g_3 H = \left[(g_1 H)(g_2 H)\right] g_3 H$$

c.b.d.u.

(2) element neutralny

Jej rolę pełni $E = eH = H$, ponieważ:

$$(eH)(gH) = (eg)H = gH$$

$$(gH)(eH) = (ge)H = gH$$

(3) element odwrotny

$$(gH)(g^{-1}H) = (gg^{-1})H = eH = H = E$$

$$(g^{-1}H)(gH) = (g^{-1}g)H = eH = H = E$$

Kluczowe jest sprawdzenie spójności definicji: działanie na warstwach nie może zależeć od wyboru reprezentantów w definicji działania na warstwach

$$g_1H = g_1'H \quad , \quad g_2H = g_2'H$$

Czy zachodzi

$$(g_1H)(g_2H) = (g_1'H)(g_2'H) \quad ?$$

$$g \in gH$$

$$g' \in gH \Rightarrow g' = gh \text{ dla pewnego } h \in H$$

$$(g_1'H)(g_2'H) = g_1'g_2'H =$$

$$= g_1h_1g_2\underbrace{h_2H}_{\substack{H \\ \text{dla } h_2 \in H}} = g_1h_1\underline{g_2H} \overset{\text{H jest normalna}}{=} g_1h_1\underline{Hg_2}$$

$$\underset{h_1H = H}{=} g_1Hg_2 \underset{\text{H jest normalna}}{=} g_1g_2H$$