

WYKŁAD 12

Grupy $(G, \cdot)$
 $\uparrow$
 zbiór

$$\exists c \in G \forall g \in G \quad c \cdot g = g \cdot c$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

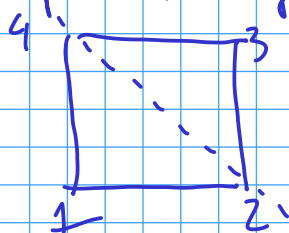
$$\forall g \in G \quad \exists g^{-1} \quad g g^{-1} = g^{-1} g = e$$

Grupa permutacji

$$\sigma: \{1, \dots, n\} \xrightarrow{\text{bij}} \{1, \dots, n\}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \sigma(2) = 3$$

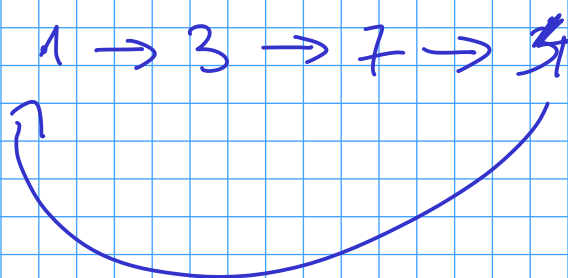
Grupa obr. i sym. kw.



$$\begin{aligned} 1 &\rightarrow 3 \\ 3 &\rightarrow 1 \\ 4 &\rightarrow 4 \\ 2 &\rightarrow 2 \end{aligned}$$

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

cykl



$$i \rightarrow i$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & \dots & & & & 4 \end{pmatrix}$$

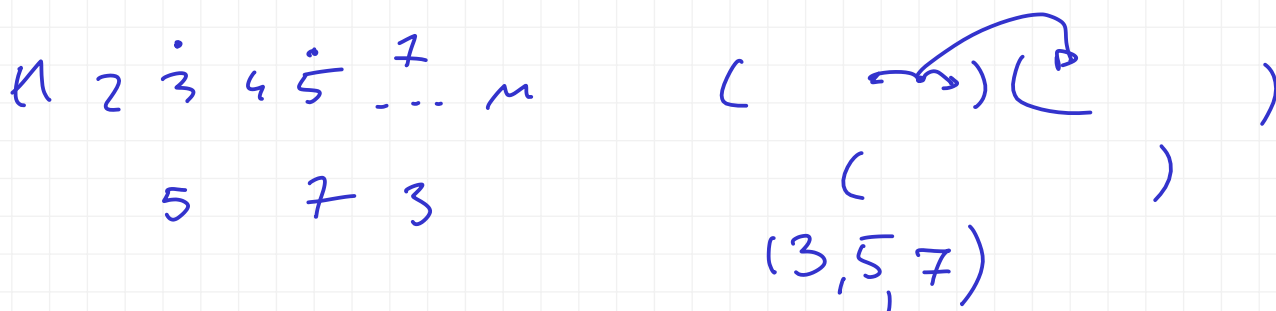
$$\begin{aligned} &(1, 3, 7, 4) \\ &(3, 7, 4, 1) \end{aligned}$$

$$(i, j)$$

$$(i, i+1)$$

- Twierdzenie 15.6.** 1. Każda permutacja σ jednoznacznie (z dokładnością do kolejności cykli) rozkłada się na rozłączne cykle.
2. Cykl długości k jest złożeniem $k - 1$ transpozycji.
3. Każda transpozycja jest złożeniem nieparzystej liczby transpozycji elementów sąsiednich (niekoniecznie rozłącznych).
4. Każda permutacja da się przedstawić jako złożenie transpozycji (niekoniecznie rozłącznych).
5. Każda permutacja da się przedstawić jako złożenie transpozycji sąsiednich (niekoniecznie rozłącznych).
6. Grupa S_n jest generowana przez zbiór transpozycji (sąsiednich).

1. Każda permutacja jedn. rozkłada się na cykle rot:



To do rozkład na cykle:

Diagram illustrating a cycle $(i, i+1, \dots, j)$ with arrows indicating a rotation. A crossed-out diagram shows a cycle (i, j) with an arrow from i to j , and a note $\sigma(i) \neq \sigma(j) ?$.

Jednoznaczne

$$(\quad) (i, i+1, \dots, j) (\quad) (i, i+1, \dots, j) (\quad)$$

$$(i, i+1, \dots, j) \quad (\text{yhl kol. cyk.})$$

Indukcja $\cdot (i, i+1)$ dla $2 \leq i \leq n$

$$(i, i+1) (i+1, \dots, j) = (i, \dots, j)$$

$\uparrow \quad \quad \quad \uparrow$
 $i-1 \leq n \quad \quad \quad i \leq n$

$$\left((i, i+1) (i+1, \dots, j) \right) (j) \rightsquigarrow i+1 \rightsquigarrow i$$

$$\left. \begin{array}{l} (i) \rightsquigarrow (i) \rightsquigarrow i+1 \\ (k) \rightsquigarrow (k+1) \rightsquigarrow k+1 \\ i < k < j \end{array} \right\} (i, \dots, j)$$

$k+1 > i+1$

$(i, \dots, j)$ to π . $j-i$ tr. el. sąsiadnich
 $a_1, a_2, \dots, a_k$

$$(a_1, a_2) (a_2, \dots, a_k)$$

ygh. dŕ k to π $k-1$ transpozycji

$$(a_1, a_2) (a_2, a_3) \dots (a_{k-1}, a_k)$$

3)

$$(i, j)^{-1} = ((i+1, \dots, j) (i, i+1, \dots, i+2) \dots (j-1, j))^{-1}$$

nieparzysta liczba tr. el. sąsiadnich

$$(i+1, \dots, j)^{-1} = ((i+1, i+2) (i+2, i+3) \dots (j-1, j))^{-1}$$

$$(j-1, j) (j-2, j-1), \dots, (i+1, i+2)$$

$$\begin{array}{l} \boxed{i} \rightsquigarrow i+1 \rightsquigarrow j \\ \boxed{j} \rightsquigarrow i \rightsquigarrow i \\ k \rightsquigarrow k+1 \rightsquigarrow k \\ i < k < j \end{array} \quad (i, j)$$

$k+1 > i+1$

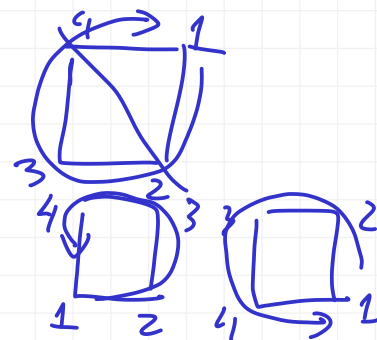
perm $\rightarrow$ π . ygh. π $\rightarrow$ π . transp $\Rightarrow$
 $\rightarrow$ π . transp. el. sąsiadnich

$$S_n = \langle (1, 2), (2, 3), (3, 4), \dots, (n-1, n) \rangle$$

Uwaga. Od teraz alternatywnym sposobem zapisu permutacji jest podanie jej jako iloczynu cykli rozłącznych. Np.:

$$\begin{pmatrix} \overset{\cdot}{1} & \overset{\cdot}{2} & \overset{\cdot}{3} & \overset{\cdot}{4} & \overset{\cdot}{5} & \overset{\cdot}{6} & \overset{\cdot}{7} & \overset{\cdot}{8} & \overset{\cdot}{9} & \overset{\cdot}{10} & \overset{\cdot}{11} & \overset{\cdot}{12} & \overset{\cdot}{13} & \overset{\cdot}{14} \\ 7 & 5 & 4 & 12 & 3 & 13 & 1 & 10 & 14 & 9 & 6 & 2 & 11 & 8 \end{pmatrix} =$$

- $(1, 7)(2, 5, 3, 4, 12)(6, 13, 11)(8, 10, 9, 14)$
- odwr.
- $(1, 7)(12, 4, 3, 5, 2) \dots$



15.2 Permutacje parzyste i nieparzyste.

Ważna funkcja: parzystość permutacji (znak permutacji).

Definicja 15.7 (Inwersje, parzystość permutacji). Dla f będącej bijekcją z podzbioru liczb naturalnych w ten sam zbiór (czyli w szczególności permutacji) *inwersja* to para (i, j) , taka że $i < j$ oraz $f(i) > f(j)$.

Parzystość permutacji to parzystość ilości jej inwersji.

Znak $\text{sgn}(\sigma)$ permutacji σ to $+1$, gdy σ jest parzysta i -1 gdy nieparzysta.

$$i < j \quad f(i) > f(j)$$

Parzystość perm: parzystość liczby inw.

inwersja

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

$1 < 2, 1 < 3, 2 < 3$

$3 > 2, 3 > 1, 2 > 1$

$2 > 1$

$1 < 2, 1 < 3, 2 < 3$

$2 > 1, 3 > 1, 3 > 2$

Lemat 15.8. Niech $\sigma, \sigma' \in S_n$ będą permutacjami. Wtedy

$$\text{sgn}(\sigma'\sigma) = \text{sgn}(\sigma') \text{sgn}(\sigma)$$

Wniosek 15.9. sgn jest homomorfizmem z S_n w $(\{-1, +1\}, \cdot)$.

Dowód: kładąc perm. to zł. tr. el. nieolnów

$$\sigma' \sigma \quad \sigma' = (i, i+1)$$

$$\cdot \operatorname{sgn}((i, i+1)) = -1$$

$$\begin{matrix} k, l \\ k, l \end{matrix} \notin \{i, i+1\} \quad \text{nie ma inw.}$$

$$\begin{matrix} i & i+1 \\ i+1 & i \end{matrix} \quad \text{inw.}$$

$$\begin{matrix} i, j & j \notin \{i, i+1\} \\ i+1, j \end{matrix} \quad \text{nie ma inw.}$$

$$i+1, j \quad j \in \{i, i+1\}$$

$$\cdot \operatorname{sgn}((i, i+1) \sigma) = -\operatorname{sgn}(\sigma) = \operatorname{sgn}((i, i+1)) \operatorname{sgn}(\sigma)$$

$$\cdot k, l \leftarrow \text{dowolne}$$

$$\sigma(k), \sigma(l) \quad i, i+1$$

↑
różnie lirowy

$$1) \{\sigma(k), \sigma(l)\} \cap \{i, i+1\} = \emptyset$$

$$(i, i+1)(\sigma)(k) = \sigma(k)$$

$$(i, i+1)(\sigma)(l) = \sigma(l)$$

$$(k, l) \text{ jest inw. dla } \sigma \Leftrightarrow$$

$$-1 / + \text{ dla } (i, i+1)\sigma$$

$$2) \{\sigma(k), \sigma(l)\} = \{i, i+1\}$$

$$\begin{matrix} k & ? & l \\ \sigma(k) & & \sigma(l) \\ \downarrow & & \downarrow \\ i & & i+1 \\ i+1 & & i \end{matrix}$$

①

zmienia się parz

lirowa inw. zmienia się o 1

$$3) (\{\sigma(k), \sigma(l)\} \cap \{i, i+1\}) = 1$$

$$\sigma(k) = i$$

$$\sigma(l) \in \{i, i+1\}$$

$$\begin{matrix} k & l \\ \downarrow & \downarrow \\ i & \sigma(l) \\ i+1 & \sigma(l) \end{matrix}$$

← nie zmienia się lirowa inw.

$\text{sgn}(\sigma' \cdot \sigma) = \text{sgn}(\sigma') \cdot \text{sgn}(\sigma)$
 prawdziwa dla $\sigma' \in \text{tr. cl. s\u0119niedziuch}$

$$\sigma = \prod_{i \in I} t_i$$

$$\sigma' = \prod_{j \in J} t_j$$

$$\text{sgn}(\sigma' \cdot \sigma) = \text{sgn}\left(\prod_{j \in J} t_j \prod_{i \in I} t_i\right)$$

$$\parallel$$

$$(-1)^{|J|+|I|}$$

$$\prod_{j \in J} t_j \quad \parallel \quad \prod_{i \in I} t_i$$

$$\text{sgn}(\sigma') \cdot \text{sgn}(\sigma)$$

$$\parallel$$

$$(-1)^{|J|} \cdot (-1)^{|I|}$$

Lemat 15.10. • Cykl parzysty jest permutacją nieparzystą.

$$\text{dl } k \Rightarrow \text{dl } k-1 \text{ trans } \Rightarrow \text{sgn}(\sigma) = (-1)^{k-1} = -1$$

- Cykl nieparzysty jest permutacją parzystą.

$$(-1)^{k-1}$$

- Parzystość permutacji to parzystość ilości cykli parzystych w rozkładzie na cykle rozłączne.



- Permutacje parzyste stanowią podgrupę A_n , która ma $\frac{n!}{2}$ permutacji.

Przykład 15.11. Zwykle w celu policzenia parzystości danej explicite permutacji najłatwiej jest to zrobić licząc jej przedstawienie w postaci cykli rozłącznych. Przykładowo, dla rozważanej wcześniej permutacji

$$\text{nh}(\sigma) = \text{mww}(2, 5, 3, 4) = 60$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 5 & 4 & 12 & 3 & 13 & 1 & 10 & 14 & 9 & 6 & 2 & 11 & 8 \end{pmatrix} =$$

$$(1, 7) (2, 5, 3, 4, 12) (6, 13, 11) (8, 10, 9, 14)$$

$$\text{sgn}(\sigma) = (-1)^2 = 1 \leftarrow \text{parzysta}$$

15.3 Wyznacznik

Wartość wyznacznika macierzy $M = (a_{ij})_{i,j=1,\dots,n}$ można zadać wprost jako:

$$|(a_{ij})_{i,j=1,\dots,n}| = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n a_{i\sigma(i)} = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n a_{\sigma(i)i}.$$

Prosty dowód pozostawiamy jako ćwiczenie.

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \underset{1}{\text{sgn}(\text{id})} a_{11} a_{22} + \underset{-1}{\text{sgn}(\sigma)} a_{1\sigma(1)} a_{2\sigma(2)} = a_{11} a_{22} - a_{12} a_{21}$$

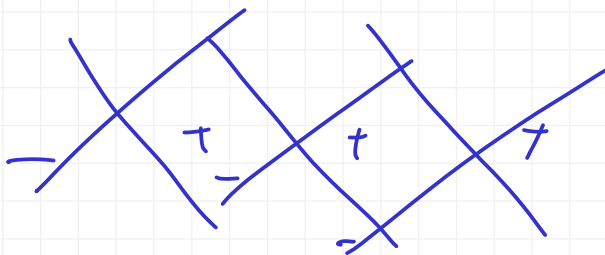
$\begin{matrix} a_{12} & a_{21} \\ \sigma(1) & \sigma(2) \\ 2 & 1 \end{matrix}$

3x3

$\sigma \in S_3$

6

3 par
3 niep.



Nie jest d.

Rozdział 16

Działania grupy na zbiorze

16.1 Mnożenie podzbiorów grupy

W podzbiorach grupy G definiujemy działanie:

$$U \cdot W = \{uw : u \in U, w \in W\}.$$

Łatwo sprawdzić, że jest ono łączne, czyli

$$U \cdot (W \cdot V) = (U \cdot W) \cdot V = U \cdot W \cdot V.$$

z tak zdefiniowanym działaniem są monoidem (mają jedność, jest to $\{e\}$).

$$\mathbb{Z}, + \quad \{1,3\} + \{1,3\} = \{2,3\} \quad \mathbb{Z}^6, \cdot$$

$$\{a\} \cdot \{b\} = ab \quad \{a\} \cdot B = aB$$

Dla zbiorów jednoelementowych zwykle będziemy opuszczać nawiasy oznaczające zbiór i pisać $a \cdot U$ lub po prostu aU , opuszczając znak działania grupowego.

Będziemy też korzystać z rozdzielności mnożenia względem sumy (mnożnościowej), tzn.:

$$U(V \cup W) = UV \cup UW \quad \text{oraz} \quad (V \cup W)U = VU \cup WU.$$

Fakt 16.1. Niech G grupa, $H \leq G$ to jej podgrupa. Wtedy:

- $gG = Gg = G$;

- $gH = H \iff Hg = H \iff gH \subseteq H \iff Hg \supseteq H \iff gH \supseteq H \iff Hg \subseteq H \iff g \in H$.

• $g \cdot G \subseteq G$
 $g \cdot g' \in G$
 $G \subseteq g \cdot G$
 $g \cdot (g \cdot g') \supseteq G$
 $g \cdot H = H$

$=$
 $g \in H$
 $g \cdot 1 \in H$
 $\Downarrow$
 $g \in H \Rightarrow gH = Hg = H$

$gH \subseteq H$
 $g \cdot e \in H$
 $g \in H$

$Hg \supseteq H$
 $e \in Hg$
 $e = h \cdot g$
 $e \cdot g^{-1} \in H \cdot g \cdot g^{-1} = H$
 $g^{-1} \in H$

16.2 Działanie grupy na zbiorze $G \xrightarrow{\text{hom}} \text{Aut}(C)_S$

Definicja 16.2 (Działania grupy na zbiorze). Mamy zbiór obiektów kombinatorycznych C oraz grupę permutacji jego elementów $S(C)$, oznaczaną przez S .

Działanie grupy G na C to homomorfizm z G w S . Zwykle zapisujemy to działanie jako $g(c)$ lub nawet gc , pomijając homomorfizm.

Działanie będziemy też rozszerzali do podzbiorów G w naturalny sposób: jeśli G działa na C to dla $U \subseteq G$ definiujemy

$\varphi(g)(c) = c'$
 $g(c) = c'$
 $G \ni U(c) = \{gc : g \in U\}$
 $Uc = \{gc : g \in U\}$

Grupa obieramy

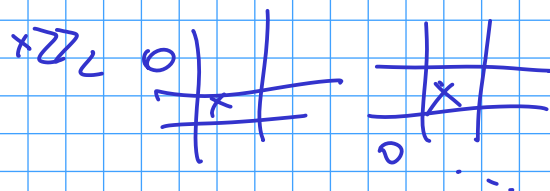
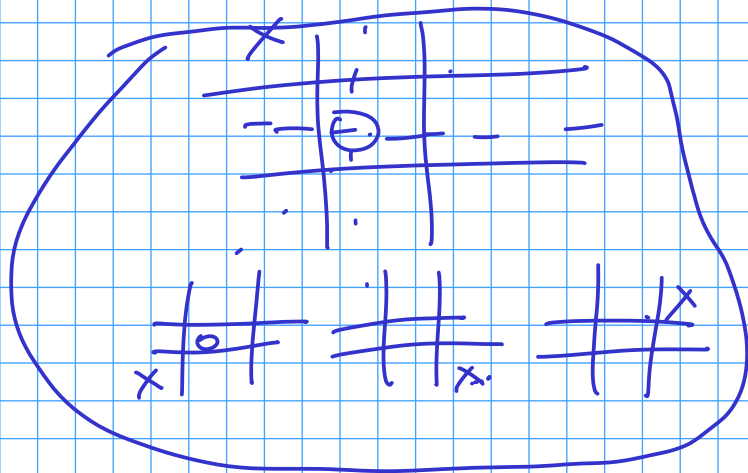
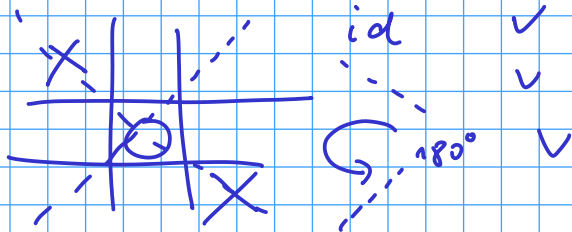
$\mathbb{Z}_2$

ram $0 \leftrightarrow X$

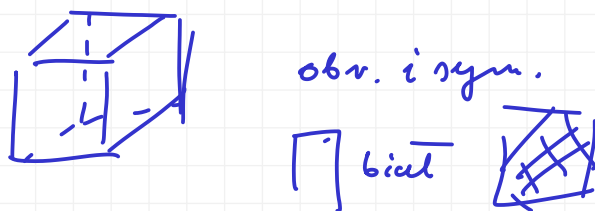


Orbita elementu c : $Gc = \{g(c) : g \in G\}$ (oznaczamy jako O_c)

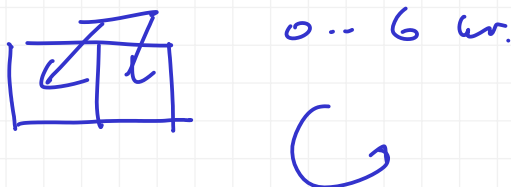
Stabilizator elementu c : $\{g \in G : g(c) = c\}$, oznaczamy jako G_c . Zauważmy, że G_c to największy zbiór taki że $G_c c = c$.



Przykład 16.3. Rozpatrzmy zbiór sześciennych kostek ze ścianami pomalowanymi na białło lub czarno. Działa na nim grupa obrotów (obrotów i odbić) sześcianu. Zauważmy, że grupa obrotów ma fizyczną interpretację, grupa obrotów i odbić już nie bardzo.



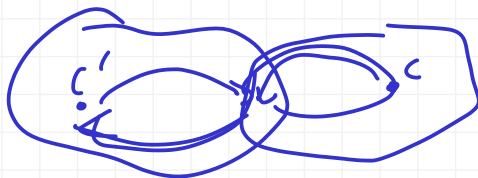
Rozpatrzmy zbiór możliwych kostek domina (pola od 0 do 6). Działa na niej grupa obrotów (obrotów i odbić) prostokąta. Podobnie, grupa obrotów ma sens fizyczny, obrotów i odbić mniej (chyba że są ze szkła).



Lemat 16.4. Niech G działa na zbiorze C , zaś $s \in C$. Wtedy stabilizator G_s jest podgrupą G .

Prosty dowód pozostawiamy jako ćwiczenie.

Lemat 16.5. Niech G działa na zbiorze C , zaś $c, c' \in C$. Wtedy $O_c, O_{c'}$ są równe lub rozłączne.



$$O_c \cap O_{c'}$$

$$1) O_c \cap O_{c'} = \emptyset \quad \text{albo}$$

$$2) O_c \cap O_{c'} \ni c''$$

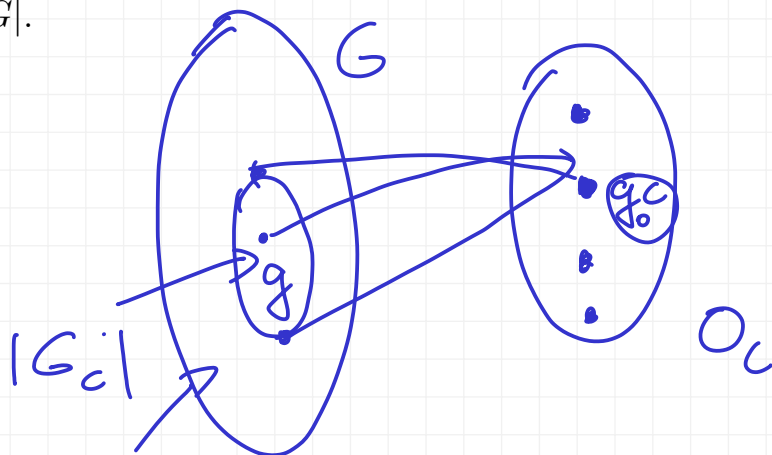
$$\begin{aligned} & \text{podgrupa} \\ & g c = g' c' \\ & (G g)(c) = (G g')(c') \end{aligned}$$

$$/ \cdot G$$

$$\begin{aligned} G(c) &= G(c') \\ O_c &= O_{c'} \end{aligned}$$

Lemat 16.6. Niech G działa na zbiorze C , zaś $s \in C$. Wtedy $|O_s| \cdot |G_s| = |G|$.

Wniosek 16.7. Niech G działa na zbiorze C , zaś $s \in C$. Wtedy $|O_s|$ oraz $|G_s|$ dzielą $|G|$.



ustalamy g_0

$$g_0 c$$

$$\{g : g c = g_0 c\}$$

$$g_0 \cdot G_c$$

$$|G| / |G_c| = |O_c| \Rightarrow |O_c| \cdot |G_c| = |G|$$

$$g_0 \cdot G_c \subseteq \{g : g c = g_0 c\}$$

$$g_0 \cdot G_c = \{g : g c = g_0 c\}$$

$$g \circ c = g \circ c \quad \text{---} \quad g = g \circ g_c$$

$\swarrow$ $\nwarrow$ $\uparrow$
 G_c

$$g \circ g_c^{-1} = g \circ g_c^{-1} \circ g \circ c = c \circ c = c$$

$\swarrow$ $\nwarrow$ $\uparrow$
 G_c

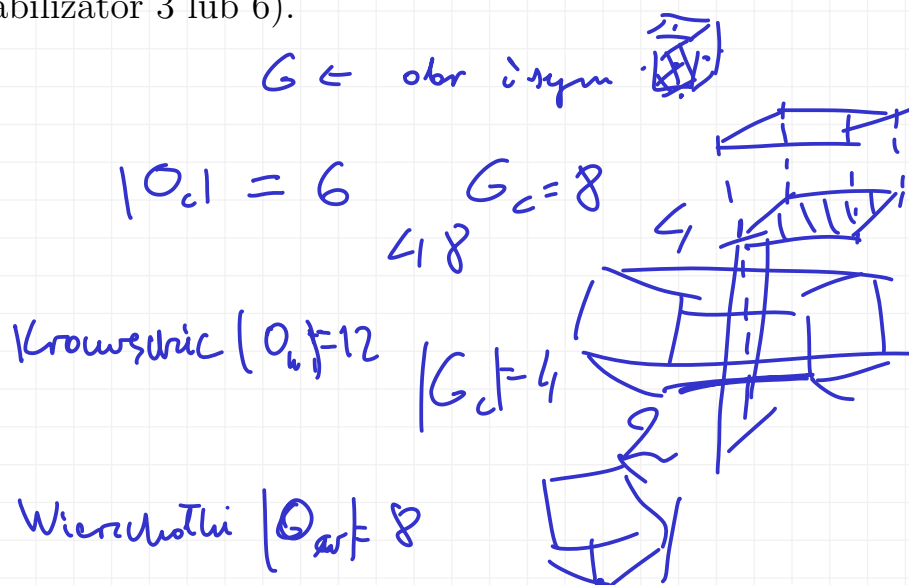
$$g \circ g_c^{-1} \circ g \in G_c \quad \text{---} \quad / g_c$$

$$\cancel{g \circ g_c^{-1}} \circ g \in g \circ G_c$$

$$g \in g \circ G_c$$

Przykład 16.8. Rozpatrzmy sześcian i grupy: obrotów oraz obrotów i symetrii, rozpatrujemy działanie na zbiorze ścian. Popatrzmy na ustaloną ścianę. Wielkość jej orbity to 6. Wielkość stabilizatora to 4 (dla obrotów) lub 8 (dla obrotów i odbić). Czyli rzędy tych grup to 24 lub 48.

Wyjdzie tyle samo, gdybyśmy rozpatrywali wierzchołki (orbita ma 8 elementów, stabilizator 3 lub 6).



$$|G_\omega| = 6 \quad 3$$

Obroty

$$|O_\omega| = 8$$



$$(G_\omega)_{\omega'}$$

$$G_{\omega, \omega'} = 2$$

redu. $\downarrow$

$$|G| = |G_c| \cdot |O_c|$$

$$8 \cdot 3_\omega \cdot 2 = 48$$

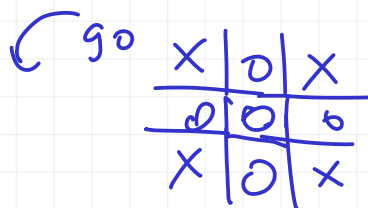
$$O_\omega \quad O_{\omega'} \cdot G_{(\omega, \omega')}$$

$$O_{\omega'} = 3$$

16.3 Lemat Burnside'a

Zliczanie orbit działania grupy odpowiada zliczaniu „nierozróżnialnych” względem działania grupy obiektów, np. kostek nierozróżnialnych ze względu na obrót itp.

Przykład 16.9. Rozważmy planszę do gry w kółko i krzyżyk. Każde pole ma przypisany jeden z trzech symboli: kółko, krzyżyk lub nic. Naszą grupą będzie grupa symetrii kwadratu. Dwie plansze, które można na siebie przeprowadzić przy użyciu elementów tej grupy uważamy za „identyczne” (bo ten sam gracz wygrywa, taka sama jest strategia itp.). Takie „identyczne” plansze to dokładnie orbita planszy względem działania tej grupy. A czym są „różne” plansze? To dokładnie różne orbity. Pytając o różne plansze, pytamy o zbiór orbit.



Pokażemy, jak policzyć moc zbioru orbit.

Definicja 16.10 (Punkty stałe). Dla grupy G działającej na zbiorze $\mathcal{C}$ mówimy, że $c \in \mathcal{C}$ jest punktem stałym $g \in G$ jeśli $g(c) = c$. Zbiór punktów stałych g oznaczamy przez

$$\text{fix}(g) = \{c \in \mathcal{C} : g(c) = c\}.$$

Twierdzenie 16.11 (Lemat Burnside'a). Niech G działa na zbiorze $\mathcal{C}$ a $\mathcal{O}$ będzie zbiorem orbit tego działania. Wtedy

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|.$$

↑
Sumujemy liczbę punktów stałych

$$|\{(g, c): g(c) = c\}|$$

$$\sum_g \underbrace{\left(\sum_{c: g(c)=c} 1 \right)}_{| \text{fix}(g) |} = \sum_g \sum_{c \in \text{fix}(g)} 1 = \sum_g | \text{fix}(g) |$$

$$\sum_c \underbrace{\sum_{g: g(c)=c} 1}_{|G_c|} = \sum_c \sum_{g \in G_c} 1$$

$$= \sum_c |G_c| \quad |G| = |O_c| \cdot |G_c|$$

$$= |G| \sum_c \frac{1}{|O_c|}$$

$$= |G| \cdot \sum_{O \in \mathcal{O}} \sum_{c \in O} \frac{1}{|O|}$$

$$= |G| \cdot \sum_{O \in \mathcal{O}} |O| \cdot \frac{1}{|O|}$$

$$= |G| \cdot \sum_{O \in \mathcal{O}} 1$$

$$= |G| \cdot |\mathcal{O}|$$

$$\sum_g | \text{fix}(g) |$$

$$\Rightarrow |\mathcal{O}| = \frac{1}{|G|} \cdot \sum_{g \in G} | \text{fix}(g) |$$

Przykład 16.12 (Kontynuacja Przykładu 16.9). Rozważmy planszę do gry w kółko i krzyżyk. Każde pole ma przypisany jeden z trzech symboli: kółko, krzyżyk lub nic. Naszą grupą będzie grupa symetrii kwadratu. Policzmy liczbę punktów stałych dla poszczególnych przekształceń:


 e

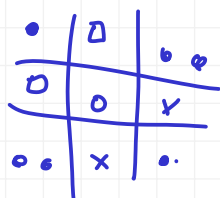
3^9

 O_{90°


3^3

 O_{270°


3^3

 O_{180°


3^5

symetria wzdłuż przekątnej (dwie takie symetrie)

$$\frac{1}{8} \cdot (3^9 + 2 \cdot 3^3 + 3^5 + 4 \cdot 3^6)$$



3^6

symetria przez bok (dwie takie symetrie)



3^6

$$\begin{array}{c|c|c}
 1 & 2 & 3 \\
 \hline
 4 & 5 & 6 \\
 \hline
 7 & 8 & 9
 \end{array}$$

$$(1, 7, 9, 3)(2, 4, 8, 6)(5)$$

$g \quad 3^3$

Zauważmy, że powyższy sposób liczenia liczby punktów stałych niejawnie korzysta z rozbicia na cykle: jeśli rozpiszemy przekształcenie g jako złożenie cykli rozłącznych na polach (jak wyżej), to wtedy wszystkie pola w jednym cyklu muszą mieć ten sam symbol. I odwrotnie: jeśli plansza spełnia warunek, że wszystkie elementy w jednym cyklu g mają to samo pole, to jest ona punktem stałym g . Czyli jeśli g ma k cykli, to ma 3^k punktów stałych.

Przykładowo, obrót o 90 stopni (w lewo lub prawo) ma rozbicie na cykle

$$(1, 3, 9, 7)(2, 4, 6, 8)(5)$$

zaś symetria względem prostej poziomej

$$(1, 7)(2, 8)(3, 9)(4)(5)(6)$$

$$\begin{array}{c|c|c}
 3 & 2 & 1 \\
 \hline
 6 & 5 & 4 \\
 \hline
 9 & 8 & 7
 \end{array}$$

3^6

Rozdział 17

Warstwy, Twierdzenie Lagrange'a

17.1 Warstwy

Najprostsze działanie grupy na sobie: przez mnożenie (z lewej strony). Dla całej grupy niewiele to daje. Ale co jeśli będziemy mnożyli tylko przez elementy z podgrupy?

Co się dzieje z podzbiorami? A dokładniej: z podgrupą?

Definicja 17.1 (Warstwa). Niech $H \leq G$ będzie podgrupą. Definiujemy naturalne działanie $h \in H$ na G :

$$h(g) = hg$$

$$C \leftarrow G \\ \text{Aut}(G) \leftarrow H$$

Orbita elementu g jest postaci

$$Hg$$

Zwyczajowo nazywamy ją warstwą prawostronną H dla g w G .

Warstwa lewostronna jest postaci

$$gH$$

$$h'h(g) = (h'h)g$$

też jest orbitą, ale dla mniej oczywistego działania

$$h(g) = gh^{-1}$$

$$h(g) = gh^{-1}$$

Zbiór warstw lewostronnych H w G oznaczamy przez G/H .

$$G:H = |G/H|$$

Należy sprawdzić, że to drugie działanie jest dobrze określone (zadanie).

My będziemy myśleć głównie o warstwach lewostronnych (choć naturalniejsza jest definicja dla prawostronnych)

Lemat 17.2. Niech $H \leq G$.

$$(gH) = (g'H)$$

- Każde dwie warstwy H w G są równoliczne.
- Każde dwie warstwy lewostronne (prawostronne) H w G są rozłączne lub identyczne.

$$(g'g^{-1})gH = g' \cancel{g^{-1}g}H = g'H =$$

$$gH \xrightarrow{\text{map}} g'H$$

$$\begin{aligned} |gH| &\geq |g'H| \\ |g'H| &\geq |gH| \end{aligned}$$

$$\begin{array}{ccc} & H = eH = He & \\ \underbrace{gH} & & \underbrace{Hg} \end{array}$$

Uwaga. Uwaga! Warstwy lewostronne i prawostronne mogą mieć nietrywialny przekrój!

Lemat 17.3. Niech $H \leq G$. Wtedy

$$\bullet \quad g_0 H = g_1 H \iff g_1^{-1} g_0 \in H \iff g_0^{-1} g_1 \in H$$

$$\bullet \quad H g_0 = H g_1 \iff g_1 g_0^{-1} \in H \iff g_0 g_1^{-1} \in H$$

$$g_0 H = g_1 H \quad / \quad g_0^{-1}$$

$$H = g_0^{-1} g_1 H$$

$$\Downarrow$$

$$g_0^{-1} g_1 \in H$$

$$g_0^{-1} g_1 H = H \quad / \quad g$$

$$g_1 H = g_0 H$$

Wniosek 17.4. W grupie skończonej

- (Twierdzenie Lagrange'a) Rząd podgrupy dzieli rząd grupy.

$$H \leq G \Rightarrow |H| \mid |G|$$

Wzrosty H

$|G| \cdot k = |G|$

- Rząd elementu dzieli rząd grupy.

$$\{e, g, g^2, \dots, g^{\text{ord}(g)-1}\} \leq G$$

- Każda grupa o p -pierwszym elementach jest cykliczna i każdy jej element (poza e) jest generatorem.

$$\langle g \rangle \leq G \quad 1, p$$

- Dla każdego a zachodzi $a^{|G|} = e$.

$$a^{|G|} = a^{\text{ord}(a) \cdot k} = e^k = e$$

Wniosek 17.5 (Małe Twierdzenie Fermat'a). Jeśli $p \nmid a$ to $a^{p-1} \bmod p = 1$.

$$(\mathbb{Z}_p \setminus \{0\}, \cdot)$$

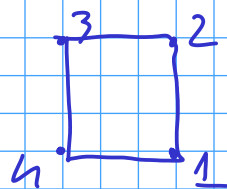
$p-1$

$$\underline{a^{p-1}} = a^{(r_h(a))h} = e = \underline{1}$$

Definicja 17.6 (Indeks podgrupy). Indeks podgrupy H względem grupy G to ilość warstw lewostronnych H w G , oznaczamy przez $G : H$.

Wartość jest taka sama, jeśli weźmiemy warstwy prawostronne. Zwykle zajmujemy się przypadkiem, kiedy indeks podgrupy jest skończony (a najczęściej tym, że obie grupy są skończone).

Przykład 17.7. Naszą grupą będą obroty i odbicia kwadratu; niech wierzchołki kwadratu będą ponumerowane 1, 2, 3, 4, w kolejności przeciwniej do ruchu wskazówek zegara, 1 w prawym dolnym rogu. Ta grupa ma 8 elementów (identyczność, obrót o 90° , 180° , 270° , symetrie względem przekątnych, symetria pionowa i symetria pozioma) i możemy o niej myśleć jak o podgrupie S_4 , czyli te elementy to $e; (1, 2, 3, 4); (1, 3)(2, 4); (1, 4, 3, 2); (1, 3); (2, 4); (1, 4)(2, 3); (1, 2)(3, 4)$.



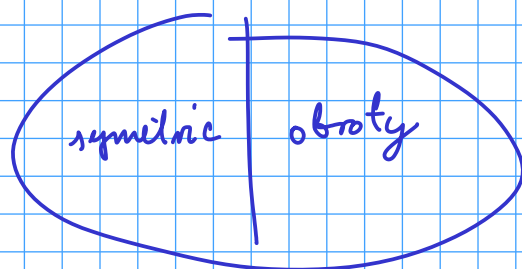
8 el.

same obrot

$\angle$

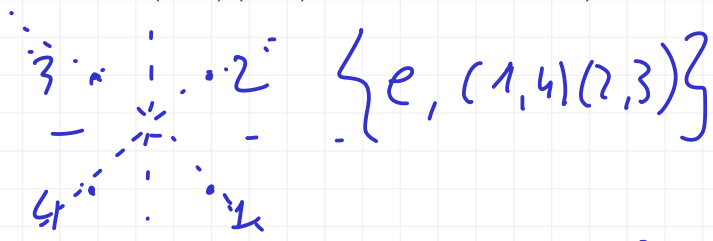
8 el.

$|H| = 4$



Weźmy podgrupę obrotów, ma 4 elementy $e; (1, 2, 3, 4); (1, 3)(2, 4); (1, 4, 3, 2)$.

Weźmy grupę generowaną przez symetrię pionową, ta grupa ma dwa elementy (symetria pionowa $(1, 4)(2, 3)$ i identyczność e).



$$\begin{aligned} \{e, (1,4)(2,3)\} \cdot e &= \{e, (1,4)(2,3)\} \\ \{e, (1,4)(2,3)\} \cdot (1,2,3,4) &= \{(1,2,3,4), (1,3)(2)(4)\} \\ \{e, (1,4)(2,3)\} \cdot (4,3,2,1) &= \{(1)(2,4)(3), (4,3,2,1)\} \\ \{e, (1,4)(2,3)\} \cdot (1,2)(3,4) &= (1,2)(3,4); (1,3)(2,4) \end{aligned}$$

6

Przykład 17.8. Grupa permutacji na 3 elementach (S_3). Podgrupa generowana przez cykl $(1, 2, 3)$ ma 3 elementy. Czyli ma dwie warstwy (ta podgrupa: permutacje parzyste i pozostałe elementy: permutacje nieparzyste).

Podgrupa generowana przez cykl $(1, 2)$ (innymi słowy: wszystkie permutacje, które trzymają 3 w miejscu). Ma dwa elementy, czyli ma 3 warstwy lewostronne i 3 prawostronne.

$$(1,2)(3); e$$

$$\{(1,2)(3), e\} \cdot e = \{(1,2)(3); e\} \quad 3 \rightarrow 3$$

$$\{(1,2)(3), e\} \cdot (1,3) = (1,3,2) \quad ; (1,3) \quad 1 \rightarrow 3$$

$$\{(1,2)(3), e\} \cdot (2,3) = (2,3,1) \quad ; (2,3) \quad 2 \rightarrow 3$$

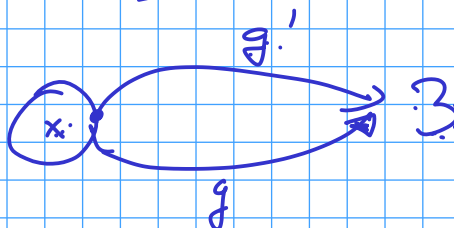
$$Hg = Hg^{-1}$$

$$H = Hg^{-1}g$$

$$g^{-1}g^{-1} \in H$$

$H \leftarrow$ „perm. nie ruchojść 3“

$$(g^{-1}g^{-1})(3) = 3$$



Wartuj lewotranne

$g^{-1}, g \in$ ta sama wart. lew., $g^{-1}H = gH$

$$g^{-1}g^{-1} \in H$$

- $3 \rightarrow 3$ $\left[(1,2)(3); (1)(2)(3) \right]$
- $3 \rightarrow 1$ $\left[(3,1)(2); (3,1,2) \right]$
- $3 \rightarrow 2$ $\left[(3,2)(1); (3,2,1) \right]$

