GRUPY

Rozważmy działanie dwuargumentowe (operację binarną) w zbiorze A:

$$\boldsymbol{* : A \times A \to A},$$

które każdej parze uporządkowanej elementów ze zbioru A przyporządkowuje pewien element także ze zbioru A.

Przykłady działań dwuargumentowych

- operacja dodawania liczb rzeczywistych,
- operacja mnożenia liczb rzeczywistych,
- operacja mnożenia macierzy kwadratowych tego samego rozmiaru,
- operacja sumowania mnogościowego podzbiorów danego zbioru,
- operacja składania permutacji tego samego rzędu.

Z reguły symbol odwzorowania $*$ umieszczamy pomiędzy parą argumentów i zamiast $*(a, b) = c$ piszemy $a * b = c$

Działanie dwuargumentowe $*$ określamy jako:

łączne, jeśli

$\boldsymbol{(a * b) * c = a * (b * c)}$ dla każdej trójki elementów $a, b, c \in A$

przemienne, jeśli

$\boldsymbol{a * b = b * a}$ dla każdej pary elementów $a, b \in A$

Element $\boldsymbol{e} \in A$ nazywamy **elementem neutralnym** działania dwuargumentowego $*$ w zbiorze A, jeśli

$\boldsymbol{a * e = e * a = a}$ dla każdego $a \in A$

Parę uporządkowaną **$(A, *)$** złożoną ze zbioru i działania dwuargumentowego zdefiniowanego w tym zbiorze nazywamy **grupą**, jeśli

- działanie $*$ jest **łączne**,
- **istnieje** w A **element neutralny** działania $*$,
- dla każdego $a \in A$ istnieje **element odwrotny** $\boldsymbol{a^{-1}} \in A$, taki że

  $\boldsymbol{a * a^{-1} = a^{-1} * a = e}$

Element neutralny jest w grupie określony jednoznacznie.
Każdy element w grupie ma dokładnie jeden element do niego odwrotny.

Grupę nazywamy **grupą przemienną** lub abelową, jeśli działanie $*$ jest przemienne.
Grupę nazywamy **grupą skończoną**, jeśli A jest zbiorem skończonym.

Przykłady grupy skończonej

Zbiór permutacji $S_n = Bij(X, X)$ dla $|X| = n$, z działaniem składania permutacji jest **grupą skończoną** (tzw. grupą symetryczną stopnia n).
$|S_n| = n!$ i dla dowolnych permutacji $f, g, h \in S_n$ spełnione są zależności:

$$\boxed{\begin{gathered} f(gh) = (fg)h \\ fe = ef = f \\ f^{-1}f = ff^{-1} = e \end{gathered}}$$

Grupa symetryczna **nie jest** grupą przemienną dla $n \geq 3$.

Dowolny podzbiór $G \subseteq S_n$ spełniający warunki:

$$f, g \in G \;\Rightarrow\; f\,g \in G \quad \text{dla wszystkich } f \text{ i } g\,,$$

$$f \in G \;\Rightarrow\; f^{-1} \in G \quad \text{dla każdego } f\,,$$

nazywany jest **grupą permutacji stopnia *n***.

Przykłady grup permutacji stopnia 3

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\; p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\; p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\; p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\; p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$G_1 = \{\, e, p_1, p_2, p_3, p_4, p_5 \,\}$$

Tabela grupy G_1:

	e	p_1	p_2	p_3	p_4	p_5
e	e	p_1	p_2	p_3	p_4	p_5
p_1	p_1	e	p_4	p_5	p_2	p_3
p_2	p_2	p_5	e	p_4	p_3	p_1
p_3	p_3	p_4	p_5	e	p_1	p_2
p_4	p_4	p_3	p_1	p_2	p_5	e
p_5	p_5	p_2	p_3	p_1	e	p_4

$$G_2 = \{\, e, p_1 \,\}$$

Tabela grupy G_2:

	e	p_1
e	e	p_1
p_1	p_1	e

Rozważmy dwie grupy $(G_1 , *)$ i $(G_2 , \bullet)$. Odwzorowanie

$$\boldsymbol{z : G_1 \to G_2}$$

nazywamy **izomorfizmem** (grup), jeśli

- z jest **bijekcją** ($z \in Bij\,(G_1 , G_2)$),
- równość $\boldsymbol{z(a * b) = z(a) \bullet z(b)}$ zachodzi dla każdych $a, b \in G_1$

Grupy izomorficzne mają identyczne struktury, tzn. różnią się jedynie oznaczeniem swoich elementów.

Izomorfizm grup oznaczamy symbolicznie $(G_1 , *) \cong (G_2 , \bullet)$.

Przykład izomorfizmu grup

Grupa symetryczna S_3 i grupa nałożeń trójkąta równobocznego na siebie.

$$G_1 = \{ e, p_1, p_2, p_3, p_4, p_5 \} \text{ i } G_2 = \{o_0 , o_1 , o_2 , s_A , s_B , s_C\}$$

o_0 - obrót o 0°,

o_1 - obrót o 120°,

o_2 - obrót o 240°,

s_A - odbicie względem osi symetrii AA′,

s_B - odbicie względem osi symetrii BB′,

s_C - odbicie względem osi symetrii CC′

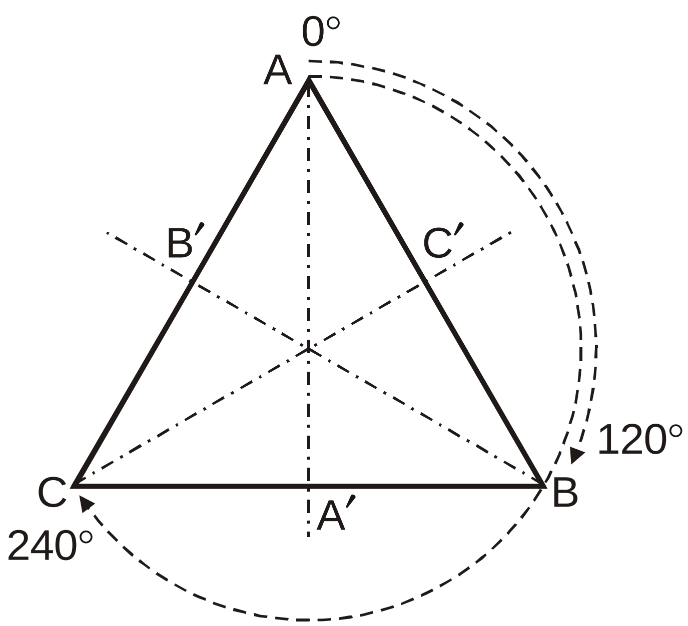


Tabela grupy G_1:

	e	p_1	p_2	p_3	p_4	p_5
e	e	p_1	p_2	p_3	p_4	p_5
p_1	p_1	e	p_4	p_5	p_2	p_3
p_2	p_2	p_5	e	p_4	p_3	p_1
p_3	p_3	p_4	p_5	e	p_1	p_2
p_4	p_4	p_3	p_1	p_2	p_5	e
p_5	p_5	p_2	p_3	p_1	e	p_4

Tabela grupy G_2:

	o_0	o_1	o_2	s_A	s_B	s_C
o_0	o_0	o_1	o_2	s_A	s_B	s_C
o_1	o_1	o_2	o_0	s_C	s_A	s_B
o_2	o_2	o_0	o_1	s_B	s_C	s_A
s_A	s_A	s_B	s_C	o_0	o_1	o_2
s_B	s_B	s_C	s_A	o_2	o_0	o_1
s_C	s_C	s_A	s_B	o_1	o_2	o_0

Izomorfizm:

G_1	e	p_1	p_2	p_3	p_4	p_5
$z(G_1)$	o_0	s_A	s_B	s_C	o_1	o_2

Dla wszystkich par elementów z grupy G_1 zachodzą równości, takie jak np.

$$z(p_1 p_3) = z(p_5) = o_2 = z(p_1)\, z(p_3) = s_A s_C = o_2$$

$$z(p_3 p_5) = z(p_2) = s_B = z(p_3)\, z(p_5) = s_C o_2 = s_B$$

$$z(p_4 p_5) = z(e) = o_0 = z(p_4)\, z(p_5) = o_1 o_2 = o_0$$

itd.

Twierdzenie (Cayley)

Każda grupa skończona jest izomorficzna z pewna grupą permutacji.

Za pomocą grup permutacji można zatem opisywać z dokładnością do izomorfizmu wszystkie grupy skończone.

WPROWADZENIE DO OGÓLNEJ TEORII ZLICZANIA

Rozważmy dowolny zbiór skończony A ($|A| = n$) i pewną grupę G permutacji zbioru A.

Zdefiniujmy następującą relację binarną R_G w zbiorze A:

$$\boldsymbol{a\, R_G\, b} \text{ dla } a, b \in A \iff \text{istnieje permutacja } p \in G, \text{ taka że } \boldsymbol{p(a) = b}$$

$\boldsymbol{R_G}$ nazywana jest **relacją indukowaną** w zbiorze A przez grupę G.

O wprowadzeniu relacji indukowanej mówi się również, że grupa G **działa** na zbiorze A.

Przykład relacji indukowanej

$A = \{1, 2, 3, 4\}$; $G = \{e, p_1, p_2, p_3\}$, gdzie $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$,

$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$, $p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

Tablica relacji R_G:

	1	2	3	4
1	**1**	**1**	0	0
2	**1**	**1**	0	0
3	0	0	**1**	**1**
4	0	0	**1**	**1**

Twierdzenie

Relacja indukowana $R_G \subseteq A \times A$ w zbiorze A przez grupę permutacji G tego zbioru, jest relacją **równoważności**.

Każda relacja równoważności w zbiorze A dzieli ten zbiór na rozłączne klasy abstrakcji $A = \bigcup_{a \in A} a \mid R_G$, gdzie $a \mid R_G = \{x \in A\colon a\, R_G\, x\}$.

Każdą z klas abstrakcji relacji indukowanej przez grupę permutacji G działającą na zbiorze A nazywamy **orbitą działania** grupy G.
Zatem zbiór klas abstrakcji $A \mid R_G$, to zbiór orbit działania grupy G.
Liczbę orbit działania grupy G oznaczamy symbolem $\boldsymbol{o(G)}$.
Wyznaczenie liczby $o(G)$ jest pierwszym zagadnieniem rozważanym w ogólnej teorii zliczania.

1. przykład wyznaczania orbit działania grupy permutacji

$A = \{1, 2, 3, 4\}$; $G = \{e, p_1, p_2, p_3\}$, gdzie $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$,

$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$, $p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

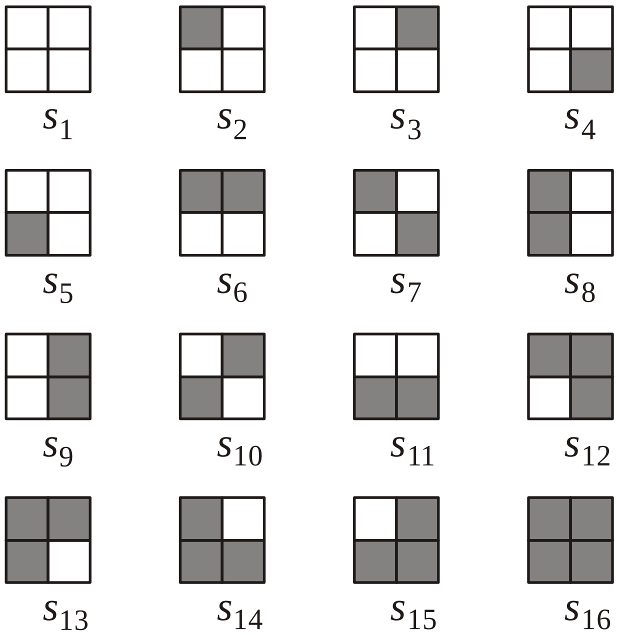
Tablica relacji R_G:

	1	2	3	4
1	**1**	**1**	0	0
2	**1**	**1**	0	0
3	0	0	**1**	**1**
4	0	0	**1**	**1**

Orbity działania grupy G: $1 \mid R_G = \{1, 2\}$, $3 \mid R_G = \{3, 4\}$ i $o(G) = 2$

2. przykład wyznaczania orbit działania grupy permutacji

Mamy zadany zbiór wszystkich dwukolorowych szachownic o 4 polach.



$$A = \{s_1, s_2, ..., s_{16}\}$$

Ile wzorów szachownic można rozróżnić, jeśli szachownice mogą być dowolnie obracane na płaszczyźnie wokół swego środka?

Zauważmy, że niektóre szachownice są nierozróżnialne, bo mogą zostać nałożone po dokonaniu pewnego obrotu, jak np. s_7 i s_{10}.

Należy rozważyć obroty o 0°, 90°, 180° i 270°, bo tylko one pozwalają nakładać na siebie szachownice o 4 polach.

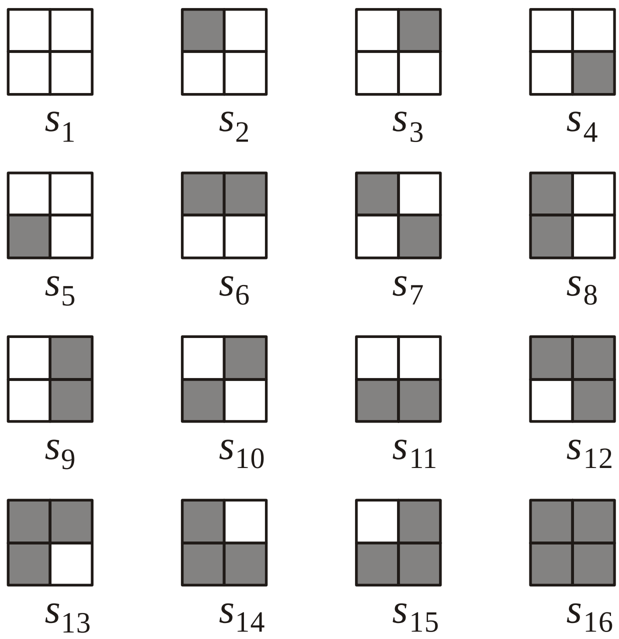
Przechodzenie jednej szachownicy w drugą po dokonaniu każdego z wymienionych obrotów można zapisać w postaci permutacji zbioru A:

permutacja e odpowiada obrotowi o 0°,

permutacja p_1 odpowiada obrotowi o 90°,

permutacja p_2 odpowiada obrotowi o 180° i

permutacja p_3 odpowiada obrotowi o 270°.



$$e = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \\ s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \end{pmatrix}$$

$$p_1 = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \\ s_1 & s_3 & s_4 & s_5 & s_2 & s_9 & s_{10} & s_6 & s_{11} & s_7 & s_8 & s_{15} & s_{12} & s_{13} & s_{14} & s_{16} \end{pmatrix}$$

$$p_2 = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \\ s_1 & s_4 & s_5 & s_2 & s_3 & s_{11} & s_7 & s_9 & s_8 & s_{10} & s_6 & s_{14} & s_{15} & s_{12} & s_{13} & s_{16} \end{pmatrix}$$

$$p_3 = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \\ s_1 & s_5 & s_2 & s_3 & s_4 & s_8 & s_{10} & s_{11} & s_6 & s_7 & s_9 & s_{13} & s_{14} & s_{15} & s_{12} & s_{16} \end{pmatrix}$$

Zbiór podanych permutacji z działaniem złożenia tworzy grupę

$$G = \{e, p_1, p_2, p_3\}.$$

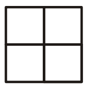
Tabela grupy G :

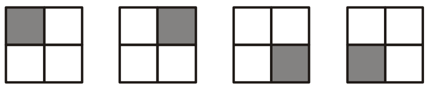
	e	p_1	p_2	p_3
e	e	p_1	p_2	p_3
p_1	p_1	p_2	p_3	e
p_2	p_2	p_3	e	p_1
p_3	p_3	e	p_1	p_2

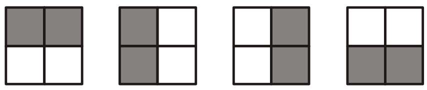
Tablica relacji indukowanej R_G:

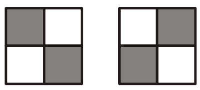
	s_1	s_2	s_3	s_4	s_5	s_6	s_8	s_9	s_{11}	s_7	s_{10}	s_{12}	s_{13}	s_{14}	s_{15}	s_{16}
s_1	1															
s_2		1	1	1	1											
s_3		1	1	1	1											
s_4		1	1	1	1											
s_5		1	1	1	1											
s_6						1	1	1	1							
s_8						1	1	1	1							
s_9						1	1	1	1							
s_{11}						1	1	1	1							
s_7										1	1					
s_{10}										1	1					
s_{12}												1	1	1	1	
s_{13}												1	1	1	1	
s_{14}												1	1	1	1	
s_{15}												1	1	1	1	
s_{16}																1

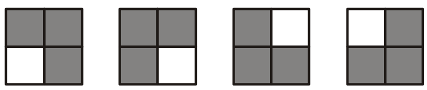
Orbity działania grupy permutacji G na zbiorze szachownic A:

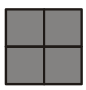
$\{ s_1 \}$ 

$\{ s_2, s_3, s_4, s_5 \}$ 

$\{ s_6, s_8, s_9, s_{11} \}$ 

$\{ s_7, s_{10} \}$ 

$\{ s_{12}, s_{13}, s_{14}, s_{15} \}$ 

$\{ s_{16} \}$ 

Zatem $o(G) = 6$ i tyle jest rozróżnialnych wzorów szachownic.

Element $a \in A$ nazywamy **niezmiennikiem** permutacji *p* zbioru A, jeśli $\boldsymbol{p(a) = a}$.

Liczbę niezmienników permutacji *p* oznaczamy $\boldsymbol{Inv(p)}$.

Przykład wyznaczania liczby niezmienników

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

$p(3) = 3$, $p(4) = 4$, $p(7) = 7$, a zatem $Inv(p) = 3$

<u>Twierdzenie</u> (Burnside)

Liczba orbit działania grupy permutacji *G* działającej na zbiorze *A*

dana jest równością: $$o(G) = \frac{1}{|G|} \sum_{p \in G} Inv(p)$$

(liczba orbit działania grupy permutacji = liczba klas abstrakcji, na które relacja równoważności R_G indukowana przez grupę *G* działającą na zbiorze *A*, dzieli ten zbiór)

William Burnside (1852 – 1927)

Przykład wyznaczania liczby orbit działania grupy permutacji

Rozważamy ponownie zbiór wszystkich dwukolorowych szachownic o 4 polach: $A = \{s_1, s_2, ..., s_{16}\}$, $G = \{e, p_1, p_2, p_3\}$.

$$e = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \end{pmatrix}$$

$$p_1 = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \\ \bullet & & & & & & & & & & & & & & & \bullet \\ s_1 & s_3 & s_4 & s_5 & s_2 & s_9 & s_{10} & s_6 & s_{11} & s_7 & s_8 & s_{15} & s_{12} & s_{13} & s_{14} & s_{16} \end{pmatrix}$$

$$p_2 = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \\ \bullet & & & & & & \bullet & & & \bullet & & & & & & \bullet \\ s_1 & s_4 & s_5 & s_2 & s_3 & s_{11} & s_7 & s_9 & s_8 & s_{10} & s_6 & s_{14} & s_{15} & s_{12} & s_{13} & s_{16} \end{pmatrix}$$

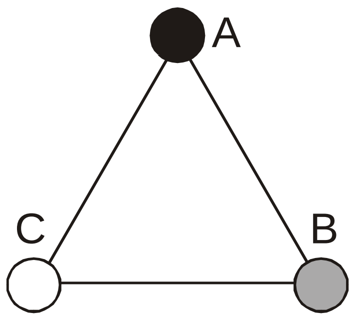
$$p_3 = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} \\ \bullet & & & & & & & & & & & & & & & \bullet \\ s_1 & s_5 & s_2 & s_3 & s_4 & s_8 & s_{10} & s_{11} & s_6 & s_7 & s_9 & s_{13} & s_{14} & s_{15} & s_{12} & s_{16} \end{pmatrix}$$

$$Inv(e) = 16,\ \ Inv(p_1) = 2,\ \ Inv(p_2) = 4,\ \ Inv(p_3) = 2$$

$$o(G) = \frac{1}{|G|}\left(Inv(e) + Inv(p_1) + Inv(p_2) + Inv(p_3)\right) = \frac{1}{4}(16 + 2 + 4 + 2) = 6$$

Przykład zastosowania tw. Burnside'a

Mamy możliwość kolorowania wierzchołków trójkąta równobocznego trzema kolorami. Na ile rozróżnialnych sposobów można to zrobić, jeśli trójkąt może być obracany w trzech wymiarach?



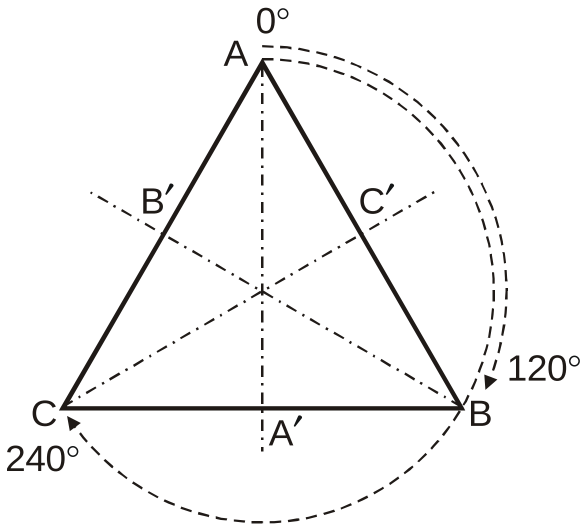
Zbiór A wszystkich możliwości pokolorowania oznaczonych wierzchołków trójkąta zawiera $3^3 = 27$ elementów.

Grupa nałożeń trójkąta równobocznego składa się z 6 elementów

$$G = \{o_0, o_1, o_2, s_A, s_B, s_C\}$$

Każdemu z elementów tej grupy odpowiada permutacja zbioru A.

$|A| = 27$ i $|G| = 6$



Liczba niezmienników = liczba pokolorowań pasujących po nałożeniu

$Inv(o_0) = 27$, $Inv(o_1) = 3$, $Inv(o_2) = 3$,

$Inv(s_A) = 9$, $Inv(s_B) = 9$, $Inv(s_C) = 9$.

Liczba orbit działania grupy permutacji G wynosi zatem:

$$o(G) = \frac{1}{|G|}\sum_{p\in G} Inv(p) = \frac{1}{6}(27+3+3+9+9+9) = 10$$

Każda orbita działania (klasa abstrakcji relacji indukowanej R_G) zawiera pokolorowania nierozróżnialne przy dowolnym obracaniu trójkąta. Zatem wzorów rozróżnialnych bez względu na obrócenie trójkąta jest właśnie tyle, ile jest orbit działania grupy G, czyli **10** :