Działanie grupy na zbiorze

Definicja 0.1 *Niech $(G, \cdot)$ będzie dowolną grupą oraz X niepustym zbiorem, to odwzorowanie $\circ : G \times X \to X$ nazywamy działaniem grupy G na zbiorze X jeślinastępujące warunki są spełnione:*

- $(\forall x \in X)\ e \circ x = x$,
- $(\forall g, h \in G)(\forall x \in X)\ (g \cdot h) \circ x = g \circ (h \circ x)$.

Tak jak w przypadku grup, zamiast pisać $g \circ x$, zastosujemy notację gx albo rzadziej $g \cdot x$.

Przykład 0.1 *Niech $(G, \cdot)$ bedzie grupą i X dowolnym niepustym zbiorem. Wtedy odwzorowanie dane wzorem*

$$G \times X \ni (g, x) \mapsto x \in X$$

jest działaniem G na X.

Przykład 0.2 *Grupa działa na samej sobie tak $g \circ x = g \cdot x$ dla dowolnych elementów $g, x \in G$. Innym przykładem działania jest działanie grupy poprzez automorfizmy wewnętrzne: gla $g, x \in G$ mamy*

$$g \circ x = gxg^{-1}.$$

Definicja 0.2 (Orbita elementu) *Niech grupa G dziala na zbiorze X i niech $x \in X$ będzie jego elementem, to zbiór*

$$Gx = G\{x\} = \{gx \in X :\ g \in G\}$$

bedziemy nazywać orbitą elemtu x. Ogólniej, dla $A \in P(X) \setminus \{\emptyset\}$

$$GA = \{gx \in X :\ (g, x) \in G \times A\}$$

nazywamy orbitą zbioru A.

Fakt 0.1 *Niech grupa G działa na zbiorze X, to wtedy mamy*

- *każda orbita jest niepusta,*
- *każde dwie orbity Gx, Gy są albo rozłączne albo są sobie równe,*
- *$X = \bigcup\{Gx :\ x \in X\}$ (X jest więc rozłączną sumą wszystkich parami różnych orbit).*

Dowòd. *Wprowadźmy następującą relację równoważności na zbiorze X:*

$$(\forall x, y \in X)x \sim y \longleftrightarrow (\exists g \in G)\ y = gx.$$

Zwrotność: niech $x \in X$- dowolny element X, więc $x = ex$, stąd $x \sim x$. Symetria, niech $x \sim y$, to dla pewnego $g \in G$ mamy $y = gx$ więc $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$, więc $y \sim x$. Przechodniość: niech $x \sim y$ i $y \sim z$, to dla pewnych $g, h \in G$ mamy $y = gx$ i $z = hy$, stąd mamy

$$z = hy = h(gx) = (hg)x \longrightarrow x \sim y.$$

Następnie, policzmy klasę abstrakcji elemntu $x \in X$:

$$\begin{aligned}[x]_\sim =& \{y \in X :\ x \sim y\} = \{y \in X :\ (\exists g \in G)y = gx\} \\ =& \{gx \in X :\ g \in G\} = Gx.\end{aligned}$$

Korzystając z twierdzenia o klasach abstrakcji relacji równoważności:

- *dla każdego $x \in X$, $\emptyset \neq [x]_\sim = Gx$,*
- *$(\forall x, y \in X)[x]_\sim \cap [y]_\sim \neq \emptyset \longrightarrow [x]_\sim = [y]_\sim$,*
- *$X = \bigcup X/_\sim = \bigcup\{[x]_\sim : x \in X\} = \bigcup\{Gx :\ x \in X\}$.*

mamy tezę naszego faktu. ■

Definicja 0.3 (Stabilizator) *Niech G działa na zbiorze X oraz $x \in X$ będzie dowolnym elementem zbioru X, to wtedy stabilizatorem elementu x nazywamy*

$$G_x = \{g \in G :\ gx = x\}.$$

Łatwo sprawdzić że stabilizator dowolnego elementu $x \in X$ jest podgrupą grupy G (to znaczy $G_x \leq G$).

Zachodzi następujący fakt.

Fakt 0.2 *Niech grupa G działa na zbiorze X. to dla dowolnego elementu $x \in X$ orbita Gx jest równoliczna z przestrzenią ilorazową G/G_x.*

Dowòd. *Pokażemy, że odwzorowanie*

$$F : Gx \to G/G_x$$

dane wzorem $F(gx) = gG_x = \{gh : h \in G_x\}$ jest dobrze zdefiniowaną bijekcją pomiędzy Gx a G/G_x. Jeśli element orbity $z \in Gx$ ma dwa przedstawnienia $z = gx$ oraz $z = g'x$, to wtedy

$$x = g^{-1}z = g^{-1}(g'x) = (g^{-1}g')x \longrightarrow g^{-1}g' \in G_x \longrightarrow gG_x = g'G_x.$$

Teraz jednoznaczność: niech $F(gx) = F(g'x)$, to wtedy $gG_x = g'G_x$ a stad mamy $g^{-1}g' \in G_x$ a stąd $g^{-1}g'x = x$ co daje nam $gx = g'x$. Następnie surjekcja odwzowrowania F: dla dowolnej warstwy $\tau \in G/G_x$ istnieje $g \in G$, dla którego mamy $\tau = gG_x = F(gx)$. ■

Wniosek 0.1 *Jeżeli grupa skończona G działa na zbiorze X i s jest ustaloną orbitą pewnego elementu zbioru X, to dla każdych $x, y \in s$ stabilizatory G_x, G_y mają taką samą moc jak i również $G/G_x, G/G_y, s$ są równoliczne.*

Dowòd. *Niech $x, y \in s$, to wówczas $Gx = s = Gy$, więc na mocy Faktu 0.1 mamy*

$$|G/G_x| = |Gx| = |s| = |Gy| = |G/G_y|$$

oraz

$$|G_x| = \frac{|G|}{|G/G_x|} = \frac{|G|}{|G/G_y|} = |G_y|.$$

■

Twierdzenie 0.1 (Cauchy) *Niech $(G, \cdot)$ będzie grupą skończoną, p będzie ustaloną liczbą pierwszą taką że $p|rzG$, to istnieje $x \in$ rzędu p.*

Dowòd. *Niech X będzie zbiorem zdefiniowanym następująco:*

$$X = \{(x_0, \ldots, x_{p-1}) \in G^p : \ x_0 \cdot \ldots \cdot x_{p-1} = e\}.$$

Wię jego moc jest równa G^{p-1} a więc jest podzielna przez liczbę p. Rozważmy grupę cykliczną H rzędu p, której generator $\sigma \in H$ działa na zbiorze X następujaco: dla dowolnego $x = (x_0, \ldots, x_{p-1})$ mamy

$$\sigma x = \sigma(x_0, \ldots, x_{p-1}) = (x_1, \ldots x_{p-1}, x_0)$$

Zauważmy że $\sigma X \subseteq X$ i dla dowolnych $x = (x_0, \ldots, x_{p-1})$ i $k \in \mathbb{Z}_p$ mamy $\sigma^k(x_0, \ldots, x_{p-1}) = (x_k, x_{k+1 \mod p}, \ldots, x_{k-1 \mod p})$. Pokażemy że H działa na zbiorze X. Dla dowolnego $x \in X$ mamy $\sigma^0 x = x$ i dla dowolnych $k, l \in \mathbb{Z}_p$ $\sigma^k(\sigma^l x) = \sigma^{k+l \mod p} x$.

Ponieważ $rzH = p$, to wtedy dla dowolnego $x \in H$ mamy $|Hx| = |H/H_x| \in \{1, p\}$ (ponieważ $rzH_x | rzH$).

Poniważ orbity stanowią klasy abstrakcji relacji równoważności, X jest sumą razłącznych parami orbit i wtedy

$$X = \bigcup \{s : \ s \in X/_\sim \wedge |s| = 1\} \cup \bigcup \{s : \ s \in X/_\sim \wedge |s| = p\}.$$

Więc, mamy

$$|G^{p-1}| = |X| = |\bigcup\{s:\ s \in X/_\sim \wedge |s| = 1\}| + |\bigcup\{s:\ s \in X/_\sim \wedge |s| = p\}|,$$

Wiemy że $p||X|$ *oraz* $p||\bigcup\{s:\ s \in X/_\sim \wedge |s| = p\}|$ *ponieważ zbiór* $\bigcup\{s:\ s \in X/_\sim \wedge |s| = p\}$ *jest sumą rozłączną wszystkich* p *elementowych orbit. Więc liczba orbit jednoelementowych jest dodatnią liczbą podzielną przez* p*. Więc istnieją elementy w grupie rzędu* p*.* ■

Nadmienię tutaj, że Cauchy udowdnił to twierdzenie w przypadku grup abelowych.

Następne twierdzenie odgrywa ważną rolę w kombinatoryce skończonej.

Twierdzenie 0.2 (Lemat Burnside'a) *Niech skończona grupa* G *działa na zbiorze* X *o skończonej mocy. Wtedy liczba wszystkich orbit jest zadana równością:*

$$l_{orbit} = \frac{1}{|G|}\sum_{g\in G}\chi(g),$$

gdzie $\chi(g) = |\{x \in X:\ gx = x\}|$ *jest charakterem elementu* g*.*

Dowód. *Obliczmy moc następującego zbioru*

$$W = \{(g, x) \in G \times X:\ gx = x\}$$

na dwa sposoby. Z jednej strony mamy:

$$|W| = \sum_{x\in X}|W^x| = \sum_{x\in X}|\{g \in G:\ gx = x\}| = \sum_{x\in X}|G_x|$$

Niech $Orb = \{Gx:\ x \in X\}$ *będzie zbiorem wszystkich orbit, wtedy ostatnią sumę można zapisać następująco:*

$$\begin{aligned}\sum_{x\in X}|G_x| &= \sum_{s\in Orb}\sum_{x\in s}\frac{|G_x||G/G_x|}{|G/G_x|} \overset{Tw\ Lagrange'a}{=} \sum_{s\in Orb}\sum_{x\in s}\frac{|G|}{|G/G_x|}\\ &= |G|\sum_{s\in Orb}\sum_{x\in s}\frac{1}{|G/G_x|} \overset{Wnz\ Faktu\ 0.1}{=} |G|\sum_{s\in Orb}\sum_{x\in s}\frac{1}{|s|}\\ &= |G|\sum_{s\in Orb}\frac{1}{|s|}\sum_{s\in Orb}1 = |G|\sum_{s\in Orb}1 = |G||Orb|.\end{aligned}$$

Z drugiej strony

$$|W| = \sum_{g\in G}|\{x \in X:\ gx = x\}| = \sum_{g\in G}\chi(g).$$

Więc ostatecznie mamy

$$|G||Orb| = \sum_{g \in G} \chi(g),$$

co daje wzór, który chcieliśmy udowodnić. ■

Przykład 0.3 *Niech będą dane dodatnie liczby naturalne $m, n \in \mathbb{N}$, takie że $m \leq n$. Rozważmy naszyjnik m-kolorowy z n paciorkami. oczywiście wszystkich takich naszyjników jest m^n. Powiemy, że dwa takie naszyjniki są identyczne, jeśli po pewnym obrocie (o kąt $\frac{2k\pi}{n}$, $k \in \mathbb{Z}_n$) jeden przechodzi w drugi. Niech więc grupa cykliczna $(\mathbb{Z}_n, +_n)$ działa na zbiorze*

$$X = \{0, 1, \ldots, m-1\}^n$$

w sposób następujący $k \circ (x_0, \ldots, x_{n-1}) = (x_{0+_n k}, \ldots, x_{n-1+_n k})$ dla dowolnego $k \in \mathbb{Z}_n$. Wszystkie naszyjniki równoważne stanowią orbitę pewnego elementu zbioru X, tak więc liczba nierównoważnych naszyjników jest rowna liczbie wszystkich parami różnych orbit. W cely wyznaczenia tej liczby wystarczy wyznaczyć wszystkie charaktery grupy $\mathbb{Z}_n$, tj. $\chi(g) = |\{x \in X : \ g \circ x = x\}|$ dla kazdego $g \in \mathbb{Z}_n$. Weźmy dowolne $k \in \mathbb{Z}_n$, wtedy wybrany naszyjnik obracamy o kąt $\frac{2k\pi}{n}$ więc $x_0 = x_k, x_1 = x_{1+_n k}, \ldots, x_{n-1} = x_{n-1+_n k}$. W takim razie paciorki oddalone od siebie o $d = NWD(k, n)$ miejsc muszą mieć ten sam kolor, co więcej taki naszyjnik jest wyznaczony przez pierwsze $x_0, x_1, \ldots, x_{d-1}$ paciorki, które przesuwamy cyklicznie o d miejsc w prawo i d ostatnich paciorków przejdzie na pierwszych d w ten sposób, że kolory będą takie same. Aby to wjasnic wystarczy zauważyć, że istnieją liczby całkowite $a, b \in \mathbb{Z}$ dla których spełnione jest równanie

$$ak + bn = d.$$

Stąd a-razy stosując przesuniecie w naszyjniku wszystkich paciorków o k miejsc (jesli $a < 0$, to przesuwamy paciorki w naszyjniku w przeciwną stronę, wtedy jesli będziemy obracać naszyjnik o $n - k$ paciorków $-a$ razy, to 0 paciorek przesunie sie na miejsce x_d i viceversa), to 0-wy paciorek po wykonaniu pełnych b obrotów znajdzie sie w miejscu paciorka x_d, więc $x_0 = x_d$, $x_0 = x_{2d}, \ldots x_0 = x_{ld}$, gdzie l jest możliwie najwiekszą liczba, dla której $ld < n$ a ponieważ $d|n$, wiec $(l+1)d = n$ i wtedy x_{ld} przejdzie na x_0 po przesunieciu wszystkich paciorków naszego naszyjnika o d miejsc. Więc $\chi(k) = m^{NWD(k,n)}$ dla $k \in \mathbb{Z}$ i ostatecznie liczba orbit (nierównoważnych naszyjników) jest równa

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = \frac{1}{n} \sum_{k \in \mathbb{Z}_n} m^{NWD(k,n)}.$$

W przypadku, gdy $n = p$ jest liczbą pierwszą mamy

$$l_{orbit} = \frac{1}{p}(m^p + (p-1)m^1) = \frac{m^p + (p-1)m}{p}.$$

Niech teraz $n = 6$, $m = 3$, wtedy nierównoważnych naszyjników jest

$$\frac{1}{6}(3^6 + 3^1 + 3^2 + 3^3 + 3^2 + 3^1) = \frac{780}{6} = 130.$$

Robert Rałowski