Matematyka dyskretna

Wykład 8: Grupy i ich działania

Gniewomir Sarbicki

Literatura

- A. I. Kostrykin *Wstęp do algebry* PWN 2005

Definicja grupy

Definicja:

Grupą nazywamy zbiór G w którym określone jest działanie dwuargumentowe $\star : G \times G \to G$ o własnościach:

- działanie jest łączne: $a \star (b \star c) = (a \star b) \star c$
- działanie posiada element neutralny
  $\exists e \in G \; \forall g \in G \; e \star g = g \star e = g$
- każdy element posiada element odwrotny:
  $\forall g \in G \; \exists g^{-1} \in G \; g \star g^{-1} = g^{-1} \star g = e$

Zwykle opuszcza się symbol działania: $g \star h \overset{ozn}{=} gh$. Ponieważ działanie jest łączne, nie trzeba używać nawiasów.

Grupy, w których działanie grupowe jest dodatkowo przemienne nazywamy **grupami abelowymi**.

Przykłady grup

Przykład: Liczby całkowite z działaniem dodawania tworzą grupę (abelową)

Przykład: Permutacje zbioru n elementowego tworzą grupę (nieabelową, skończoną) oznaczaną jako S_n

Przykład: Obroty w $\mathbb{R}^3$ względem ustalonego punktu tworzą grupę (ciągłą, nieabelową)

Przykład: Przekształcenia symetrii wielokątów foremnych na płaszczyźnie tworzą grupę.

Podgrupy

Definicja:

Podgrupą nazywamy dowolny podzbiór H grupy G, który sam jest grupą z działaniem z grupy G, tzn:

- $\forall g_1, g_2 \in H \ g_1 g_2^{-1} \in H$.

W szczególności $e \in H$ oraz $\forall g \in H \ g^{-1} \in H$.

Przykład: Obroty na płaszczyźnie o wielokrotność kąta $\pi/6$ tworzą skończoną podgrupę grupy obrotów na płaszczyźnie.

Przykład: Liczby całkowite parzyste tworzą nieskończoną podgrupę grupy liczb całkowitych z działaniem dodawania.

Homomorfizmy grup

Definicja:

Homomorfizmem grup $\Phi : G \to H$ nazywamy odwzorowanie pomiędzy grupami, które zachowuje strukturę grupy, tzn:

- $\Phi(gh) = \Phi(g)\Phi(h)$

w szczególności $\Phi(e_G) = e_H$ oraz $\Phi(g^{-1}) = \Phi(g)^{-1}$.

Fakt:

Jądro $\{g \in G : \Phi(G) = e_H\}$
oraz **obraz** $\{h \in H : \exists g \in G\ \Phi(g) = h\}$
homomorfizmu Φ są podgrupami odpowiednio G i H.

Homomorfizmy grup

Definicja:

Homomorfizm grup, który jest injekcją (odwzorowanie różnowartościowe) nazywamy **monomorfizmem**.

Definicja:

Homomorfizm grup, który jest surjekcją (odwzorowanie "na") nazywamy **epimorfizmem**.

Definicja:

Homomorfizm grup, który jest bijekcją (odwzorowanie wzajemnie jednoznaczne) nazywamy **izomorfizmem** grup.

Przykłady homomorfizmów

Przykład: Istnieje homomorfizm pomiędzy grupą przekształceń symetrii n-kąta foremnego a grupą permutacji jego wierzchołków. Każdemu przekształceniu symetrii można przypisać permutację wierzchołków, którą ono powoduje. Przypisanie to jest monomorfizmem grup.

W przypadku trójkąta równobocznego jest to jednocześnie epimorfizm, zatem grupa jego symetrii jest izomorficzna z S_3.

W przypadku wielokątów o większej liczbie wierzchołków nie jest to już epimorfizm i grupa symetrii takiego n-kąta foremnego jest właściwą podgrupą grupy S_n.

Przykłady homomorfizmów

Niech G będzie grupą obrotów o wielokrotność kąta $\pi/6$.

Przykład: Homomorfizm grup $\Phi : (\mathbb{Z}, +) \to G$, dany wzorem $n \to e^{i\frac{2\pi}{6}n}$ jest epimorfizmem. Jego jądrem jest zbiór liczb całkowitych podzielnych przez 6. Zbiór ten jest podgrupą $\mathbb{Z}$.

Przykład: Odwzorowanie $\Phi : \mathbb{Z}_6 \to G$ dane wzorem $[n] \to e^{i\frac{2\pi}{6}n}$ jest izomorfizmem grup.

Działanie grupy na zbiorze

Definicja:

Działaniem grupy G na zbiorze Ω nazywamy dowolne odwzorowanie $I : G \times \Omega \to \Omega$ o własnościach:

- $\forall x \in \Omega \; I_e x = x$
- $\forall g, h \in G \; \forall x \in \Omega \; I_g(I_h x) = I_{gh} x$

Przykład: Działanie grupy obrotów na wektory stojące (kontrawariantne) w $\mathbb{R}^2$ (mnożenie lewostronne):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Działanie grupy na zbiorze

Przykład: Działanie grupy obrotów na wektory leżące (kowariantne, np. wektor siły) w $\mathbb{R}^2$ (mnożenie prawostronne):

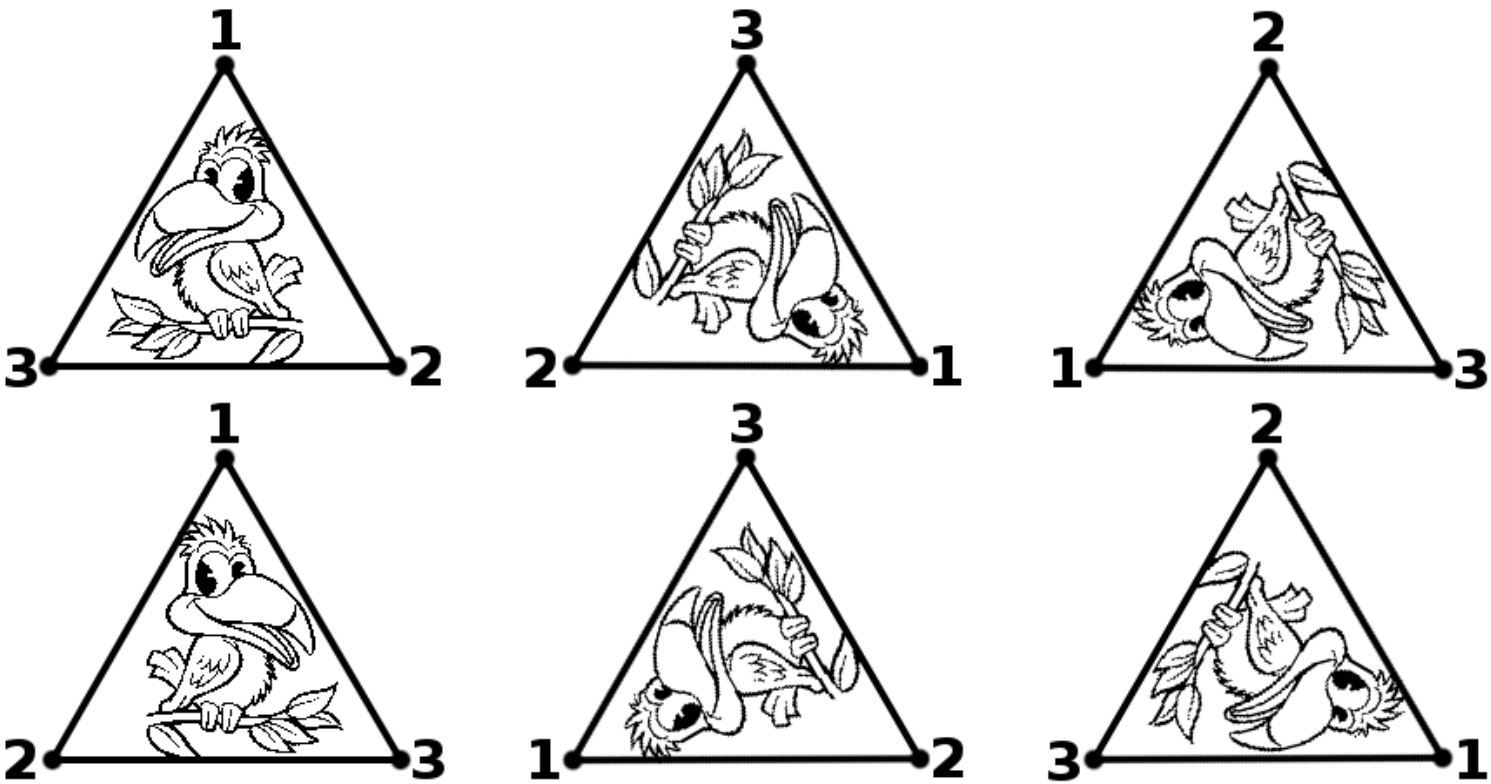
$$\begin{bmatrix} x' & y' \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$$

Przykład: Działanie grupy obrotów na macierze odwzorowań liniowych z $\mathbb{R}^2$ do $\mathbb{R}^2$ odpowiadające obrotom układu współrzędnych (działanie poprzez sprzężenie):

$$A' = O(\alpha) A O^{-1}(\alpha)$$

Działanie grupy na zbiorze

Przykład: Grupa symetrii trójkąta równobocznego odwzorowuje trójkąt równoboczny w siebie.



Orbity

Definicja:

Orbitą punktu x w zbiorze Ω pod działaniem I grupy G nazywamy podzbiór:

$$I_G(x) = Gx = \{y \in \Omega : \ \exists g \in G \ I_g(x) = y\}$$

Fakt:

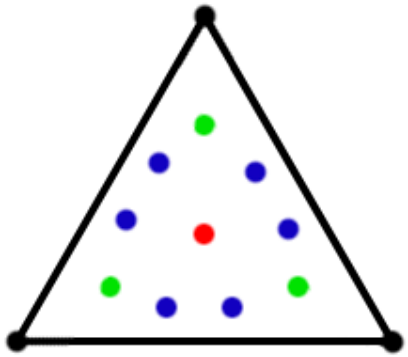
Pod działaniem I grupy G zbiór Ω rozpada się na sumę rozłącznych orbit.

Fakt:

Każdy zbiór niezmienniczy na działanie grupy jest sumą orbit. Orbita jest najmniejszym (w sensie inkluzji) takim zbiorem.

Przykłady orbit

Przykład: Rozważmy działanie grupy symetrii trójkąta równobocznego na jego punkty. Otrzymamy trzy rodzaje orbit - jedno-, trzy- i sześciopunktowe.

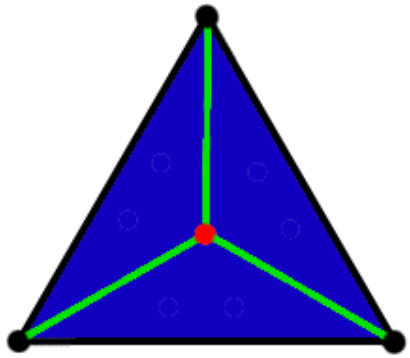


Przykład: Rozważmy działanie grupy obrotów na wektory płaszczyzny poprzez mnożenie lewostronne przez macierz obrotu. Orbitą działania punktu odległego o r od początku układu współrzędnych jest okrąg o promieniu r.

Przykład: Rozważmy działanie na globus grupy obrotów wokół jego osi. Orbitą punktu na globusie pod takim działaniem grupy obrotów jest południk przechodzący przez ten punkt.

Przykłady orbit

Przykład: Rozważmy działanie grupy symetrii trójkąta równobocznego na jego punkty. Otrzymamy trzy rodzaje orbit - jedno-, trzy- i sześciopunktowe.



Przykład: Rozważmy działanie grupy obrotów na wektory płaszczyzny poprzez mnożenie lewostronne przez macierz obrotu. Orbitą działania punktu odległego o r od początku układu współrzędnych jest okrąg o promieniu r.

Przykład: Rozważmy działanie na globus grupy obrotów wokół jego osi. Orbitą punktu na globusie pod takim działaniem grupy obrotów jest południk przechodzący przez ten punkt.

Przykłady orbit

Definicja: Działanie takie, że $\forall x_1, x_2 \in \Omega \ \exists g \in G \ x_2 = gx_1$ nazywamy **przechodnim**. Cały zbiór Ω jest orbitą względem takiego działania.

Przykład: Rozważmy działanie grupy linowej na $\mathbb{R}^2 \setminus \{0\}$ poprzez mnożenie lewostronne.

Pomiędzy każdymi dwoma wektorami można przejść za pomocą pewnej operacji liniowej (nawet więcej niż jednej), zatem działanie to jest przechodnie.

Stabilizator orbity

Definicja:

Stabilizatorem punktu $x_0 \in \Omega$ względem działania I grupy G na zbiorze Ω nazywamy następującą podgrupę grupy G:

$$St(x_0) = \{g \in G : \ I_g(x_0) = x_0\}$$

Fakt: Stabilizatory punktów z tej samej orbity są ze sobą izomorficzne

Dowód: Rozważmy dwa punkty tej samej orbity x_1, oraz $x_2 = gx_1$. Każdemu elementowi h stabilizatora elementu x_2 możemy przypisać element stabilizatora elementu x_1 wzorem $h \to g^{-1}hg$. Odwzorowanie to jest różnowartościowe i jest homomorfizmem grup. Co więcej konstrukcję możemy powtórzyć w przeciwnym kierunku, jest ono zatem odwracalne $\square$

Stabilizator orbity

Przykład: Dla działania grupy obrotów G wokół osi na globus, stablilizatorem bieguna jest całą grupa G, natomiast stabilizator pozostałych punktów jest trywialny ($\{e\}$).

Warstwy

Dla podgrupy H grupy G rozważmy jej działanie na grupie G poprzez mnożenie lewostronne:

$$I : H \times G \to G \qquad I_h(g) = hg$$

orbitę elementu g przy takim działaniu nazywamy **warstwą lewostronną** elementu g względem podgrupy H. Oznaczmy ją jako Hg

Analogicznie można zdefiniować **warstwę prawostronną** elementu g względem podgrupy H jako orbitę działania:

$$I : H \times G \to G \qquad I_h(g) = gh$$

Oznaczamy ją jako gH

Warstwy

Twierdzenie:

Warstwy względem tej samej podgrupy są równoliczne i równoliczne z tą podgrupą.

Dowód: Rozważmy odwzorowanie $f(x) = g_2 g_1^{-1} x$ działające z warstwy $g_1 H$ do warstwy $g_2 H$. odwzorowanie to jest:

- różnowartościowe: $f(g_1 h_1) = f(g_1 h_2) \implies g_2 h_1 = g_2 h_2 \implies h_1 = h_2 \implies g_1 h_1 = g_1 h_2$
- na: $g_2 h = f(g_1 h)$

zatem dwie warstwy prawostronne są ze sobą równoliczne. Analogicznie udowadniamy dla warstw lewostronnych

Ponieważ podgrupa H jest warstwą elementu e względem podgrupy H, to każda warstwa względem podgrupy elementów jest równoliczna z tą podgrupą $\square$

Dzielnik normalny

Definicja:

Podgrupę H grupy G dla której zachodzi warunek:

$$\forall h \in H \ \forall g \in G \ ghg^{-1} \in H$$

nazywamy **dzielnikiem normalnym** grupy G. Oznaczamy to jako $H \triangleleft G$

Fakt: Jądro homomorfizmu jest dzielnikiem normalnym.

Dowód: $\forall h \in \ker f \ \ f(ghg^{-1}) = f(g)f(h)f(g)^{-1}$
$= f(g)ef(g)^{-1} = f(g)f(g)^{-1} = e \implies ghg^{-1} \in \ker f.$

Fakt: Dowolna podgrupa grupy abelowej jest jej dzielnikiem normalnym.

Grupa ilorazowa

Fakt: Warstwa prawostronna i lewostrona elementu $g \in G$ względem dzielnika normalnego H są sobie równe.

Dzięki temu można zdefiniować działanie na warstwach względem dzielnika normalnego:

$$aH \cdot bH = a(Hb)H = a(bH)H = abH^2 = abH$$

Zbiór warstw z tak określonym działaniem ma strukturę grupy. Grupę tą oznaczamy jako G/H i nazywamy grupą ilorazową.

Przykłady

Przykład: Weźmy grupę $(\mathbb{R}, +)$ i jej podgrupę $(\mathbb{Z}, +)$. Ponieważ są to grupy abelowe, $\mathbb{Z} \triangleleft \mathbb{R}$.

Do tej samej orbity należą liczby rzeczywiste różniące się o liczbę całkowitą. Zbiór orbit jest grupą izomorficzną z grupą obrotów na płaszczyźnie.

Przykład: Weźmy grupę $(\mathbb{Z}, +)$ i jej podgrupę $(3\mathbb{Z}, +)$ (liczby podzielne przez trzy). Ponieważ są to grupy abelowe, $3\mathbb{Z} \triangleleft \mathbb{Z}$.

Orbitę tworzą liczby całkowite różniące się o wielokrotność trójki. Grupą ilorazową jest zbiór orbit czyli $\mathbb{Z}_3$.

Rząd grupy i indeks podgrupy

Definicja:

Ilość warstw podgrupy H w grupie G nazywamy **indeksem podgrupy** H w G i oznaczamy jako $(G : H)$

Definicja:

Ilość elementów grupy G nazywamy **rzędem grupy** G i oznaczamy jako $(G : e)$

(oznaczenie bierze się z obserwacji, że każdy element jest warstwą względem podgrupy $\{e\}$)

Uwaga: Jeżeli $H \triangleleft G$, to indeks H w G jest równy rzędowi grupy ilorazowej:

$$(G/H : e) = (G : H)$$

Twierdzenie Lagrange'a

Twierdzenie (Lagrange'a):

$$(G : e) = (G : H) \cdot (H : e)$$

Wniosek: Rząd grupy skończonej jest podzielny przez rząd każdej jej podgrupy

Fakt: Ilość elementów w orbicie elementu x pod działaniem grupy G jest równa liczbie warstw działającej grupy G względem stabilizatora elementu orbity (podgrupy G)

Z twierdzenia Lagrange'a mamy zatem:

$$\#G(x_0) = (G : St(x_0)) = \frac{(G : e)}{(St(x_0) : e)}$$