

Struktury na \mathbb{Q} - przydatne pojęcia

Skrypt ma na celu wprowadzenie kilku pojęć, które będą użyteczne na warsztatach i których dotyczą zadania kwalifikacyjne.

1 Grupy

Definicja 1 (Grupy). *Grupą nazywamy dowolny niepusty zbiór G , na którym określono działanie dwuargumentowe $\otimes : G \times G \rightarrow G$ (tzn. dla dowolnych $a, b \in G$ mamy określone pewne $a \otimes b \in G$), dla którego istnieje wyróżniony element $e \in G$, zwany elementem neutralnym, taki, że spełnione są warunki:*

- (a) $\forall a, b, c \in G \quad a \otimes (b \otimes c) = (a \otimes b) \otimes c$ (działanie jest łączne)
- (b) $\forall a \in G \quad a \otimes e = e \otimes a = a$ (e jest neutralny dla działania)
- (c) $\forall a \in G \quad \exists b \in G \quad a \otimes b = b \otimes a = e$ (każdy element a ma pewną odwrotność b).

Przykłady grup:

- $G = \mathbb{Z}$ z działaniem dodawania $\otimes = +$. Wtedy rolę elementu neutralnego spełnia $e = 0$, zaś elementem odwrotnym do a jest $-a$. Zamiast dodawania liczb całkowitych, moglibyśmy rozpatrywać dodawanie liczb wymiernych, bądź rzeczywistych, w obydwu przypadkach otrzymując grupy w analogiczny sposób.
- $G = \mathbb{Q} \setminus \{0\}$ z działaniem mnożenia $\otimes = \cdot$. Wtedy $e = 1$ i widać, że elementem odwrotnym ustalonego a jest $\frac{1}{a}$. Tak samo będzie, jeśli $G = \mathbb{R} \setminus \{0\}$.
- $G = S_n$ - zbiór permutacji zbioru $\{1, \dots, n\}$, tzn. bijekcji $f : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$, w którym działaniem jest operacja składania funkcji $\otimes = \circ$, elementem neutralnym funkcja identycznościowa, zaś istnienie odwrotności można potraktować jako część definicji funkcji będącej bijekcją. W odróżnieniu od wcześniej przedstawionych grup, w tej grupie na ogół będzie $f \otimes g \neq g \otimes f$, tzn. działanie nie będzie przemienne, a więc grupy w ogólności nie muszą być przemienne.
- Grupa złożona z izometrii płaszczyzny \mathbb{R}^2 , z działaniem składania funkcji.
- Grupa $G = Z_n$ złożona z elementów $\{0, \dots, n-1\}$ z działaniem dodawania modulo n , tj. dodawania i brania z wyniku reszty modulo n : $a \otimes b = (a + b) \bmod n$. Grupy tego typu i grupę z pierwszego przykładu nazywamy grupami cyklicznymi. Ogólniej,

grupę G nazwiemy cykliczną, jeśli istnieje taki jej element $g \in G$, że każdy inny element G daje się zapisać jako g^k dla pewnej liczby całkowitej k (ujemne k oznacza potęgę odwrotności g).

Dla pierwszych dwóch przykładów grup łatwo zauważyć, że element neutralny spełniający warunek (b) definicji może być tylko jeden, a następnie, że żaden element grupy nie może mieć dwóch różnych odwrotności. Jest to prawdą dla każdej grupy i nietrudno te wnioski wyciągnąć z definicji (polecam się o tym przekonać!). Ów jedyny element odwrotny do danego $a \in G$ będziemy oznaczać przez a^{-1} lub $(-a)$ w zależności od tego, czy działanie będziemy nazywać "mnożeniem", czy "dodawaniem" (jest to tylko kwestia czysto językowa). W przypadku "mnożenia" na ogół opuszcza się znak działania ($ab = a \otimes b$), odtąd będziemy mówić tylko o "mnożeniu".

Czasem w grupie można wyróżnić mniejszą grupę:

Definicja 2 (Podgrupy). *Podgrupą grupy G z elementem neutralnym e nazwiemy każdy podzbiór $H \subset G$ zawierający e oraz zamknięty na mnożenie i branie odwrotności w G , tzn. jeśli $h_1, h_2 \in H$, to $h_1 h_2 \in H$ oraz $h_1^{-1} \in H$. Podgrupa jest w szczególności grupą z tym samym działaniem (rozumianym jako zdefiniowane tylko dla elementów H) i tym samym elementem neutralnym.*

Przykład: W grupie izometrii płaszczyzny wyróżnić możemy podzbiór złożony z obrotów wokół początku układu współrzędnych. Widać łatwo, że te obroty tworzą podgrupę grupy izometrii, gdyż złożenie dwóch obrotów jest obrotem, zaś przekształceniem odwrotnym jest obrót o kąt przeciwny.

2 Działania grup na zbiorach

Nas będą interesowały głównie grupy, które umiemy traktować jako złożone z pewnych przekształceń, takie jak S_n , czy grupa izometrii płaszczyzny. Weźmy $G = S_n$ i oznaczmy $X = \{1, \dots, n\}$. Elementy G są w szczególności funkcjami z X do X , więc dla $g \in G$ i $x \in X$ możemy napisać wyrażenie $g(x)$ oznaczające pewien element X . Jeśli będziemy pisać w takich sytuacjach gx zamiast $g(x)$, to mamy jakby mnożenie elementów X przez elementy G z lewej strony, które spełnia warunki $(gh)x = g(hx)$ i $ex = x$ dla $g, h \in G$ i e będącego elementem neutralnym (tutaj używamy też notacji $gh = g \otimes h$). Mówimy tutaj, że grupa G działa na zbiorze X .

Definicja 3 (Działania grupy na zbiorze). *Działaniem grupy G , z elementem neutralnym e , na zbiorze X nazwiemy dowolną operacją dwuargumentową $G \times X \rightarrow X$ (wynik tej operacji na argumentach $g \in G$, $x \in X$ zapisujemy jako gx), która spełnia dwa warunki:*

$$(a) \quad \forall_{g,h \in G} \quad \forall_{x \in X} \quad (gh)x = g(hx)$$

$$(b) \quad \forall_{x \in X} \quad ex = x$$

Przykłady:

- Grupa $G = S_n$ działa na $X = \{1, \dots, n\}$ tak, jak określono powyżej.
- Grupa $G = S_n$ działa też na $X = S_n$ w taki sposób, że dla $g \in G$, $x \in X$ określamy $gx = gxg^{-1}$, gdzie lewą stronę należy czytać jako "wynik działania g na x ", zaś prawą jako "złożenie permutacji g , x i g^{-1} " (po prawej stronie x traktujemy jako permutację w S_n).

Zadanie działania grupy na zbiorze pozwala traktować elementy grupy jako przekształcenia danego zbioru. Jeśli mamy działanie grupy G na zbiorze X , to dla każdego $g \in G$ mamy też funkcję $f_g : X \rightarrow X$ określoną w ten sposób, że $f_g(x) = gx$. Korzystając z własności (a) i (b) widzimy, że dla wszelkich $g \in G$ oraz $x \in X$ zachodzi $f_g(f_{g^{-1}}(x)) = g(g^{-1}x) = (gg^{-1})x = ex = x$ i analogicznie $f_{g^{-1}}(f_g(x)) = x$ czyli funkcje f_g i $f_{g^{-1}}$ są wzajemnie odwrotne. A więc przekształcenia odpowiadające elementom G są w istocie bijekcjami. Patrzenie na własności tych przekształceń pozwala wyciągać interesujące wnioski o strukturze samej grupy.