O pewnych kratach testowych

Małgorzata JASTRZĘBSKA[*]

Teoria krat pojawiła się pod koniec XIX wieku, wyrastając z logiki i algebry. W logice kraty pojawiły się za sprawą George'a Boole'a, a w algebrze kraty pierwszy rozpatrywał Richard Dedekind. Kraty są przedmiotem badań algebraików, stanowią jednocześnie wygodny środek opisu znanych struktur matematycznych, których przykłady przedstawię w dalszej części artykułu. Można je opisać na dwa sposoby: algebraicznie lub przy użyciu częściowych porządków.

Czytelnikowi zainteresowanemu teorią krat oraz jej zastosowaniami w logice i algebrze polecamy szczególnie książki *Podstawy algebry ogólnej i teorii krat* Andrzeja Walendziaka (PWN, 2009), *The Mathematics of Metamathematics* Heleny Rasiowej i Romana Sikorskiego (PWN, 1963) oraz *Lattice Theory* Garretta Birkhoffa (AMS, 1967).

Definicja 1. *Krata w sensie algebraicznym* to struktura algebraiczna $(L, \wedge, \vee)$ spełniająca dla dowolnych elementów $a, b, c \in L$ następujące równości:

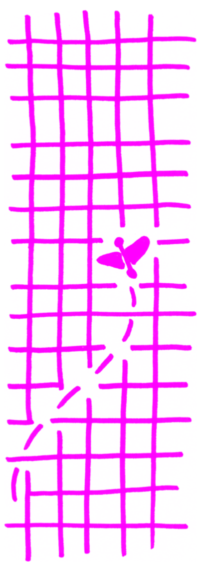
$$\begin{aligned} a \wedge b &= b \wedge a, & a \vee b &= b \vee a, \\ a \wedge a &= a, & a \vee a &= a, \\ a \wedge (b \wedge c) &= (a \wedge b) \wedge c, & a \vee (b \vee c) &= (a \vee b) \vee c, \\ a \wedge (a \vee b) &= a, & a \vee (a \wedge b) &= a. \end{aligned}$$

Krata w sensie częściowych porządków to niepusty częściowo uporządkowany zbiór $(L, \leqslant)$, w którym każdy dwuelementowy podzbiór ma oba kresy: górny i dolny.

Pojęcia krat w sensie algebraicznym i częściowych porządków są równoważne. Jeśli zdefiniujemy kratę jako zbiór algebraiczny z wymienionymi aksjomatami, to zadając porządek przez $a \leqslant b \Leftrightarrow a \vee b = b$, otrzymamy kratę w sensie porządku. Odwrotnie, jeśli w kracie w sensie porządku zdefiniujemy $a \vee b = \sup\{a, b\}$ oraz $a \wedge b = \inf\{a, b\}$, to dostaniemy kratę w sensie algebraicznym.

Zanim omówię wybrane przykłady krat, podam kilka użytecznych definicji. Kratę $(L, \leqslant)$ będziemy zwykle oznaczali literą L, identyfikując ją ze zbiorem jej elementów. Jeśli w kracie L istnieje element największy, to nazywamy go *jednością kraty* i oznaczamy przez 1. Podobnie, najmniejszy element w kracie (jeśli istnieje) oznaczamy symbolem 0 i nazywamy *zerem kraty*. Kratę z zerem i jednością nazywamy *kratą ograniczoną*. Podzbiór K kraty L nazwiemy jej *podkratą*, jeśli dla dowolnych $a, b \in K$ mamy $a \wedge b \in K$ oraz $a \vee b \in K$. Powiemy, że kraty L_1 i L_2 są izomorficzne wtedy i tylko wtedy, gdy istnieje bijekcja $\varphi : L_1 \to L_2$, taka że φ i φ^{-1} zachowują porządek, tj. $a \leqslant b \Leftrightarrow \varphi(a) \leqslant \varphi(b)$.

Zauważmy, że jeśli $(L, \leqslant)$ jest kratą, to para $(L, \geqslant)$, gdzie relacja $\geqslant$ zdefiniowana jest wzorem $a \geqslant b \Leftrightarrow b \leqslant a$ również jest kratą. Kratę $(L, \geqslant)$ będziemy nazywać kratą dualną do kraty L i oznaczać symbolem L^{∂}. Łatwo sprawdzić, że jeśli $a \wedge b = c$ w kracie L, to $a \vee b = c$ w kracie L^{∂}, oraz analogicznie jeśli $a \vee b = d$ w kracie L, to $a \wedge b = d$ w kracie L^{∂}.



Przykład 1. Niech X będzie dowolnym zbiorem. Rodzina $\mathcal{P}(X)$ wszystkich podzbiorów zbioru X wraz z porządkiem zadanym przez inkluzję $\subseteq$ jest kratą. Mianowicie, jeśli $A, B \in \mathcal{P}(X)$, to $A \wedge B = A \cap B$ oraz $A \vee B = A \cup B$. Jest to krata ograniczona. Zerem tej kraty jest zbiór pusty, a jednością zbiór X.

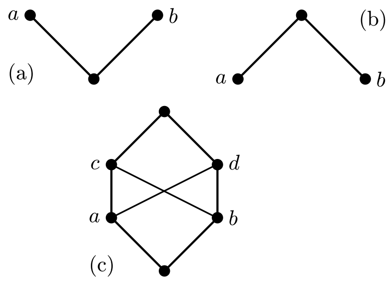
Przykład 2. Niech $|$ oznacza relację podzielności w zbiorze $\mathbb{N}$ dodatnich liczb całkowitych. Niech $\mathrm{NWD}(a, b)$ tradycyjnie oznacza największy wspólny dzielnik liczb a i b oraz $\mathrm{NWW}(a, b)$ ich najmniejszą wspólną wielokrotność. Zbiór uporządkowany $(\mathbb{N}, |)$ jest kratą z działaniami $a \wedge b = \mathrm{NWD}(a, b)$ oraz $a \vee b = \mathrm{NWW}(a, b)$. Krata ta ma element najmniejszy równy 1 i nie ma elementu największego.

Przykład 3. Niech V będzie przestrzenią liniową nad ciałem K i niech $\mathrm{Sub}(V)$ oznacza rodzinę wszystkich jej podprzestrzeni. Zbiór $(\mathrm{Sub}(V), \subseteq)$ jest kratą. Jeśli $A, B \in \mathrm{Sub}(V)$, to $A \wedge B = A \cap B$ oraz $A \vee B = A + B$, gdzie $A + B = \{a + b : a \in A \text{ i } b \in B\}$. Zerem w tej kracie jest wektor zerowy, a jedynką cała przestrzeń V. Podobnie, kratami są również: rodzina podgrup zadanej grupy, rodzina jej dzielników normalnych oraz rodzina podpierścieni danego pierścienia, wszystko z relacją inkluzji.

Przykład 4. Niech S będzie rodziną podzbiorów przestrzeni $\mathbb{R}^2$ złożoną ze zbioru pustego, całej przestrzeni $\mathbb{R}^2$ oraz wszystkich punktów i wszystkich prostych w $\mathbb{R}^2$. Zbiór ten z relacją zawierania stanowi kratę ograniczoną. Zerem tej kraty jest zbiór pusty, a jednością $\mathbb{R}^2$.

[*] Instytut Matematyki i Fizyki, Wydział Nauk Ścisłych, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

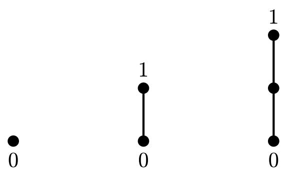
Kraty, tak jak wszystkie porządki, możemy ilustrować za pomocą diagramów, które tworzymy w następujący sposób: elementy kraty L zaznaczamy na płaszczyźnie jako punkty. Jeśli a, b są elementami kraty L oraz $a \leqslant b$, to punkt odpowiadający elementowi a rysujemy poniżej punktu odpowiadającego elementowi b. Jeśli b jest następnikiem a, czyli $a < b$ oraz nie istnieje $z \in L$, taki że $a < z < b$, to punkty a i b łączymy odcinkiem.



Rys. 1. Diagramy nieprzedstawiające krat.

Przyjrzyjmy się diagramom z rysunku 1. Widzimy, że na diagramie (a) elementy a i b nie mają kresu górnego, a w przypadku diagramu (b) elementy a i b nie mają kresu dolnego. Na diagramie (c) elementy a i b mają dwa ograniczenia górne c i d, ale nie mają kresu górnego. Zatem diagramy te nie przedstawiają krat.

Wskażemy teraz diagramy porządków będących kratami. Oczywiście, każdy liniowo uporządkowany zbiór (często nazywany łańcuchem) jest kratą. Łatwo można sprawdzić, że kraty o co najwyżej trzech elementach muszą być łańcuchami.



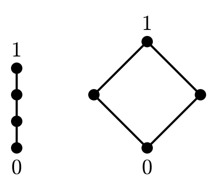
Rys. 2. Kraty o co najwyżej trzech elementach.

Kraty o czterech elementach są tylko dwie (z dokładnością do izomorfizmu), a krat pięcioelementowych jest dokładnie pięć (rys. 3 i 4).

W matematyce ważną rolę spełniają kraty rozdzielne i modularne.

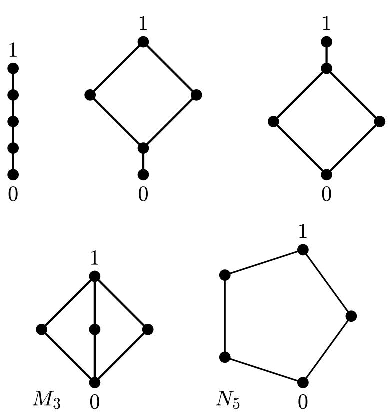
Definicja 2. Kratę L nazywamy *modularną*, gdy dla dowolnych jej elementów $a, b, c \in L$, takich że $c \leqslant a$, zachodzi $(a \wedge b) \vee c = a \wedge (b \vee c)$.

Definicja 3. Kratę L nazywamy *rozdzielną* (*dystrybutywną*), gdy dla dowolnych jej elementów $a, b, c \in L$ spełniona jest równość $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.



Rys. 3. Kraty czteroelementowe.

Wprost z definicji wynika, iż każda krata rozdzielna jest modularna. Zwróćmy uwagę, że wszystkie łańcuchy są kratami rozdzielnymi. Rozważmy kratę z przykładu 1 – równość z definicji kraty rozdzielnej w przypadku kraty $\mathcal{P}(X)$ ma postać dobrze znanego prawa rozdzielności przecięcia zbiorów względem dodawania $(A \cap (B \cup C) = (A \cap B) \cup (A \cap C))$, zatem krata $\mathcal{P}(X)$ jest rozdzielna. W tym przypadku nie napotkaliśmy problemów z wykazaniem tej własności, często jednak sprawdzenie wprost z definicji, czy dana krata jest dystrybutywna bądź modularna, jest dość kłopotliwe. Na szczęście istnieją niezwykle obrazowe i przydatne twierdzenia sprowadzające problem do pytania, czy wśród jej podkrat znajdują się pewne wymienione wcześniej kraty.



Rys. 4. Kraty pięcioelementowe.

Twierdzenie 1. *Krata L jest modularna wtedy i tylko wtedy, gdy nie ma podkraty izomorficznej z N_5* (rys. 4).

Szkic dowodu: Łatwo zauważyć, że jeśli L ma podkratę izomorficzną z N_5, to nie jest modularna. Załóżmy teraz, że L nie jest modularna, tzn. istnieją $a, b, c \in L$, $c \leqslant a$, takie że $d \neq e$, gdzie $d = (a \wedge b) \vee c$ i $e = a \wedge (b \vee c)$. Z założenia $c \leqslant a$ oraz oczywistych relacji $c \leqslant b \vee c$, $a \wedge b \leqslant a$ i $a \wedge b \leqslant b \vee c$ w prosty sposób wynika $d \leqslant e$, więc $d < e$. Wykażemy, że b, d, e wraz z $a \wedge b$ i $b \vee c$ tworzą kratę izomorficzną z N_5. Najpierw upewnimy się, że $a \wedge b$ i $b \vee c$ są różne od reszty wyszczególnionych elementów – istotnie, gdyby było $b = a \wedge b$, to mielibyśmy $b \vee c = d < e = a \wedge (b \vee c)$, co jest niemożliwe; podobnie dowodzimy, że $b \neq b \vee c$. Ponadto $e = b \vee c$ byłoby równoznaczne z $b \vee c \leqslant a$, skąd $b \leqslant a$, czyli $b = a \wedge b$, co jak już wiemy, jest niemożliwe; analogicznie $d \neq a \wedge b$. Korzystając z własności działań kratowych, otrzymujemy

$$b \vee d = b \vee ((a \wedge b) \vee c) = (b \vee (a \wedge b)) \vee c = b \vee c$$

i analogicznie $b \wedge e = a \wedge b$. Ponadto, skoro zachodzi $a \wedge b \leqslant d \leqslant e$, to

$$a \wedge b = a \wedge b \wedge b \leqslant d \wedge b \leqslant e \wedge b = a \wedge b,$$

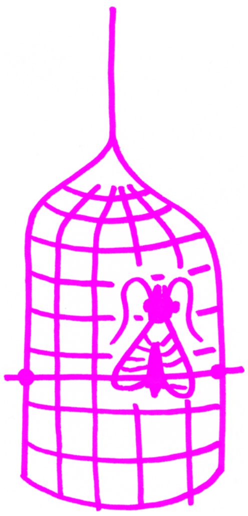
tak więc $d \wedge b = a \wedge b$. Podobnie dowodzimy $e \vee b = b \vee c$, co w połączeniu z wykazanymi wcześniej zależnościami prowadzi nas już do wniosku, że wskazane elementy faktycznie tworzą podkratę izomorficzną z N_5.

W analogiczny, choć nieco bardziej skomplikowany sposób, otrzymujemy podobny wynik dla krat rozdzielnych.

Czytelnik Oczytany dostrzeże podobieństwo przytoczonych twierdzeń do twierdzenia Kuratowskiego, które orzeka, że graf skończony jest planarny wtedy i tylko wtedy, gdy nie ma podgrafu homeomorficznego z K_5 lub $K_{3,3}$.

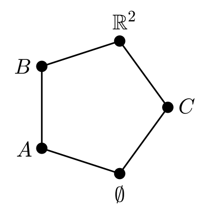
Twierdzenie 2. *Krata L jest rozdzielna wtedy i tylko wtedy, gdy nie ma podkraty izomorficznej z M_3 lub N_5* (patrz rys. 4).

Z podanych twierdzeń w prosty sposób wynika, że jeśli krata L jest modularna (rozdzielna), to krata L^∂ również jest modularna (rozdzielna).



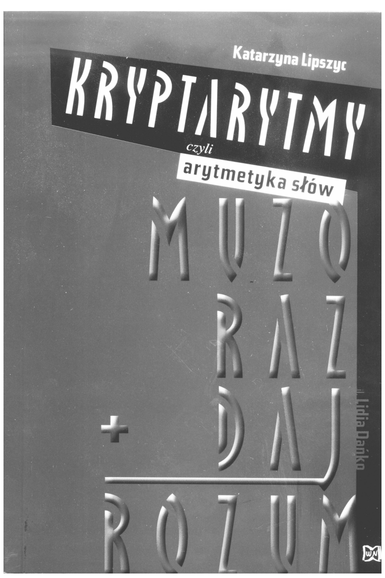
Weźmy teraz kratę z przykładu 3. Gdyby $\mathrm{Sub}(V)$ nie była modularna, to w kracie tej istniałaby podkrata izomorficzna z N_5. Istniałyby zatem parami różne podprzestrzenie $A, B, C, E, F \subseteq V$, takie że $A \subset B$, $A \cap C = B \cap C = E$, oraz $A + C = B + C = F$. Nie jest to jednak możliwe, co pozostawiam Czytelnikowi Podejrzliwemu jako nietrudne zadanie z algebry liniowej. Krata $\mathrm{Sub}(V)$ jest zatem kratą modularną, jednocześnie łatwo wykazać, że nie jest to krata rozdzielna. Weźmy przestrzeń $W \subseteq V$ wymiaru dwa i trzy jej różne jednowymiarowe podprzestrzenie A, B, C. Podprzestrzenie A, B, C przecinają się w wektorze zerowym i każde dwie z nich generują W. Dostajemy zatem podkratę izomorficzną z M_3.

Wykażemy teraz, że krata z przykładu 4 nie jest nawet modularna. Zauważmy, że jeżeli A oznacza punkt leżący na prostej B, a przez C oznaczymy prostą nieprzecinającą prostej B, to otrzymujemy podkratę:



Kraty modularne i rozdzielne są dokładnie opisane w literaturze i znamy wiele ich własności. Poza nimi rozważa się, oczywiście, wiele innych rodzajów tych struktur. Niektóre z nich dają się scharakteryzować poprzez zawieranie pewnej podkraty lub podkrat. Te charakterystyczne obiekty (np. M_3 oraz N_5) to właśnie tytułowe *kraty testowe.*

Kryptarytmy, czyli arytmetyka słów



Wydawnictwo Nowik Sp.j., Opole 2013

Kryptarytm (gr. *kryptós* = ukryty; *arythmos* = liczba) to zadanie szaradziarskie w postaci działania arytmetycznego, w którym cyfry zastąpiono literami. Zadaniem rozwiązującego jest odtworzenie owego działania. Takim samym literom powinny odpowiadać takie same cyfry, a różnym literom – różne cyfry. Żadna z liczb wielocyfrowych nie może zaczynać się zerem. Po zastąpieniu liter cyframi powinno otrzymać się poprawne działanie. Z kolei alfametyk to kryptarytm, w którym cyfry zaszyfrowane są literami tworzącymi wyrazy powiązane znaczeniowo bądź też słowa składające się w sensowne frazy lub zdania.

W książeczce (zdrobnienie podyktowane jest wygodnym, małym formatem) znajdziemy wiele alfametyków podzielonych przez autorkę, Katarzynę Lipszyc, na kilka działów: „Łatwe", jak np.

BOK + BOK + BOK + BOK = ROMB,

„Trochę trudniejsze", „Kryptarytmy – zdania" i „Układy równań" (a raczej układy kryptarytmów, gwarantujące jedyność rozwiązania). Niektóre z nich zostały zainspirowane konkretnymi wydarzeniami, jak np.

MYŚL + LECA + ŚMIGA = CELNIE,

ułożony przez autorkę z okazji stulecia urodzin Stanisława Jerzego Leca w 2009 roku, czy

TSUNAMI − ZMIATA = MIASTA,

powstały w 2011 roku po trzęsieniu ziemi w Japonii.

Niewątpliwym walorem książeczki jest jej szata graficzna. Świetne i zabawne rysunki autorstwa Lidii Dańko, ozdabiające kryptarytmy, zachęcają do zmierzenia się z nimi. Książeczka ucieszy miłośników matematyki rekreacyjnej (kryptarytmy od czasu do czasu pojawiają się w polskiej prasie szaradziarskiej, ale nie ma ich zbyt wiele), przyda się też nauczycielom, którzy chcą przekonać swoich uczniów, że matematyką można się wspaniale bawić, ćwicząc przy okazji logiczne myślenie i wytrwałość.

Renata JURASIŃSKA

PS. Czytelniku, zanim zajrzysz do tej książki, rozwiąż alfametyk z jej okładki!

Redakcja