Kurs: Matematyka DYSKRETNA

Forma: Ćwiczenia

Tryb: Online 8.04.2021

Temat: Relacja równoważności, kongruencje, częściowy porządek.

Przykład 1

Każda partycja wyznacza relację równoważności, której klasami abstrakcji są wszystkie jej zbiory.

Niech $X \neq \emptyset$ i weźmy rodzinę

$$P = \{A_t,\ t \in T\},\ \text{taką że}$$

(i) $\forall_{t,t'}\ t \neq t' \Rightarrow A_t \cap A_{t'} = \emptyset$

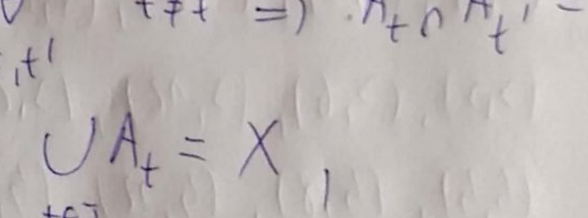
(ii) $\bigcup_{t \in T} A_t = X$,

czyli partycję zb. X.

Definiujemy $R \subset X \times X$:

$$\forall_{a,b \in X}\ aRb \equiv \exists_{t \in T}\ a, b \in A_t$$

aRb $\quad \neg aRc$



Pomocniczo: dla $a \in X = \bigcup_{t \in T} A_t \equiv \exists_t\, a \in A_t$, tak

aRa, czyli R jest (R2).

dla $a, b \in X$, $a, b \in A_t \equiv b, a \in A_t$, to

$aRb \Rightarrow bRa$ (RS)

dla $a, b, c \in X$

$a, b \in A_t \wedge b, c \in A_t \Rightarrow a, c \in A_t$, to

R jest (RP).

Niech $a \in X$. Oznaczmy $[a]_R$.

$b \in [a]_R \equiv aRb \equiv \exists_t\, a, b \in A_t$,

co dowodzi, że $[a]_R \subset A_t$

Na odwrót, ponieważ $a \in A_t$, to dla $b \in A_t$

mamy aRb, skąd $b \in [a]_R$, co dowodzi, że

$[a]_R = A_t$.

P2. Niech $p \geq 2$ całkowita,

$$\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$$

Dla $n \in \mathbb{Z}$, niech $r_p(n)$ oznacza resztę z dzielenia n przez p, czyli z zasady podzielności

$$n = kp + r_p(n), \quad k \in \mathbb{Z}$$

$$r_p(n) \in \mathbb{Z}_p.$$

Na $\mathbb{Z}_p$ definiujemy dwa działania $\oplus_p$, $\odot_p$, gdzie

$$n \oplus_p m \overset{df}{=} r_p(n+m)$$

$$n \odot_p m \overset{df}{=} r_p(n \cdot m), \quad n, m \in \mathbb{Z}_p$$

Zbudujmy tabele dla tych działań dla $p=4$, $p=7$.

$p=4$

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

„Efekt przemienności"

Zauważ, że.

Dla działania $\oplus_p$, $\forall_{a\in\mathbb{Z}_p}\ \exists!_{b\in\mathbb{Z}_p}\ a \oplus_p b = 0$,

$\downarrow$

„element przeciwny do a"

bowiem $a \oplus_p b = r_p(a+b)$,

Zatem $b = p-a$, $a \geq 1$

$b = a = 0$, $a = 0$ (patrz tabela).

Problem. Czy dla działania $\odot_p$ prawdą jest, że

(*) $\forall_{a\in\mathbb{Z}_p}\ \exists!_{b\in\mathbb{Z}_p}\ a \odot_p b = 1$, $a \neq 0$

$\downarrow$

„element odwrotny" do a

Tabela dla $p=4$ pokazuje, że tak nie jest!

(np. „2" nie ma elementu odwrotnego!).

W takim razie kiedy (*) jest prawdziwe.

Wróćmy teraz do $\odot_7$.

$\odot_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tutaj

$1 \odot_7 1 = 1$

$2 \odot_7 4 = 1$

$3 \odot_7 5 = 1$

$4 \odot_7 2 = 1$

$5 \odot_7 3 = 1$

$6 \odot_7 6 = 1$

Dlaczego teraz jest dobrze?

Odp. bo $p=7$ jest liczbą pierwszą.

P.3. Wiadomo, że dla $\mathbb{Z}$ z działaniami „$\cdot$"

$$m \cdot n = 0 \Rightarrow m = 0 \vee n = 0.$$

Czy tak jest dla $\mathbb{Z}_p$ z $\odot_p$.

Wsk. Porównać tabele dla $\odot_4$ i $\odot_7$.

P.4. Opisać rozbicie $\mathbb{Z}$ relacją $(\mathrm{mod}\ p)$.

Wiemy, że mod p jest relacją równoważności na $\mathbb{Z}$, dlatego z zasady abstrakcji generuje rozbicie $\mathbb{Z}$.

Pokażmy, że

$$\mathbb{Z} = A_0 \,\dot\cup\, A_1 \,\dot\cup \ldots \dot\cup\, A_{p-1},$$

gdzie $A_j = [j]_{\mathrm{mod}\, p}$, $j \in \mathbb{Z}_p$.

Weźmy $n \in \mathbb{Z}$. Wiemy z zasady podzielności

$$n = kp + r_p(n) \quad (k \in \mathbb{Z}).$$

Zatem $n \equiv r_p(n) \pmod{p}$, co dowodzi, że $n \in A_{r_p(n)}$, gdzie $r_p(n) = j$.

Pozostaje wyjaśnić z jakich liczb składają się zbiory A_j (już było!).

P5. Na A definuj relację R, taką że
co najmniej: R2, RA, RP.
Oznacz ją $\leq_A$ i mówimy (A, $\leq_A$) -
„A jest zbiorem częściowo uporządkowanym"

Niech A: {1, 2, 3, 4, 6, 8, 12, 24}

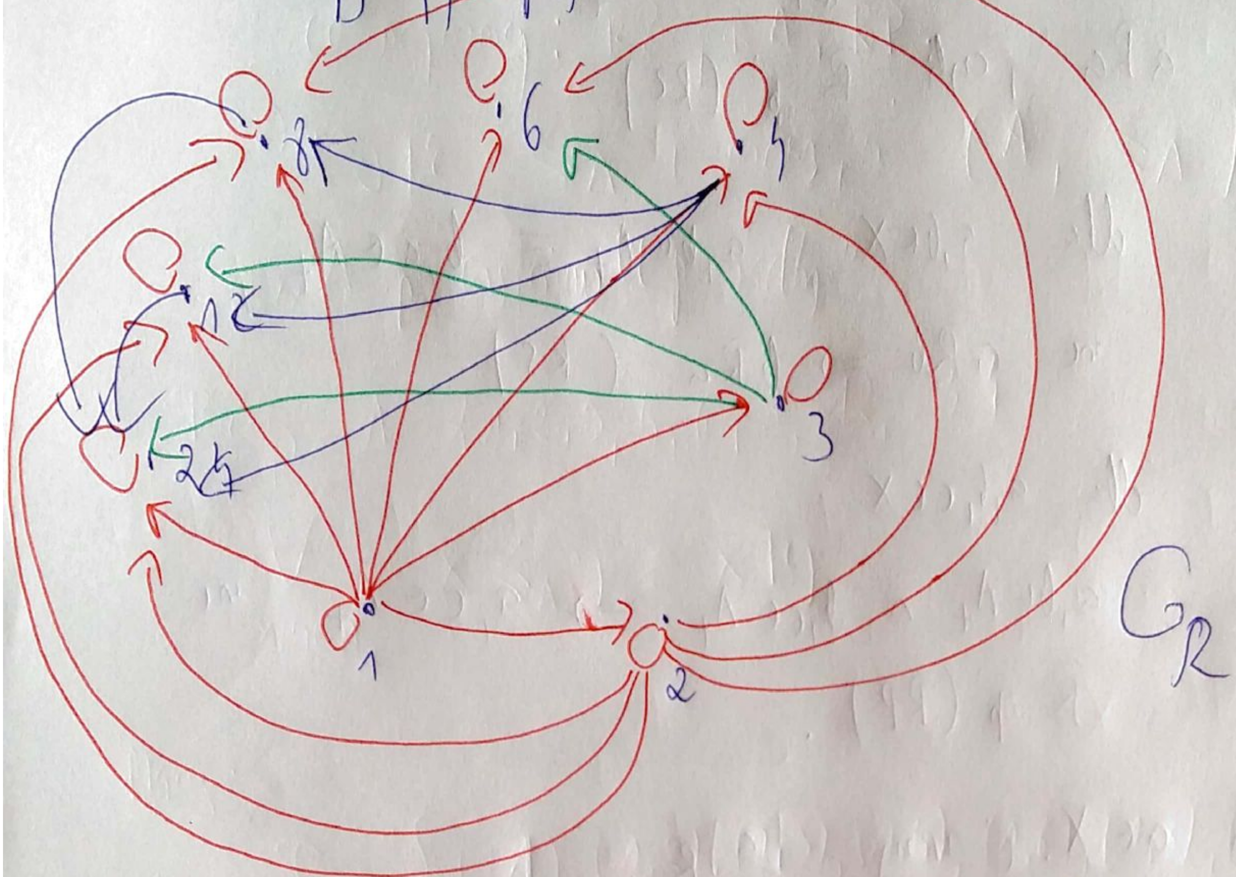
$$\forall_{x,y \in A} \quad x \leq_A y \equiv x \mid y$$

Mamy:

$$R = \{(1,1), (1,2), (1,3), (1,4), (1,6), (1,8), (1,12), (1,24),$$
$$(2,2), (2,4), (2,6), (2,8), (2,12), (2,24),$$
$$(3,3), (3,6), (3,12), (3,24),$$
$$(4,4), (4,8), (4,12), (4,24),$$
$$(8,8), (8,24),$$
$$(12,12), (12,24),$$
$$(24,24)\}.$$

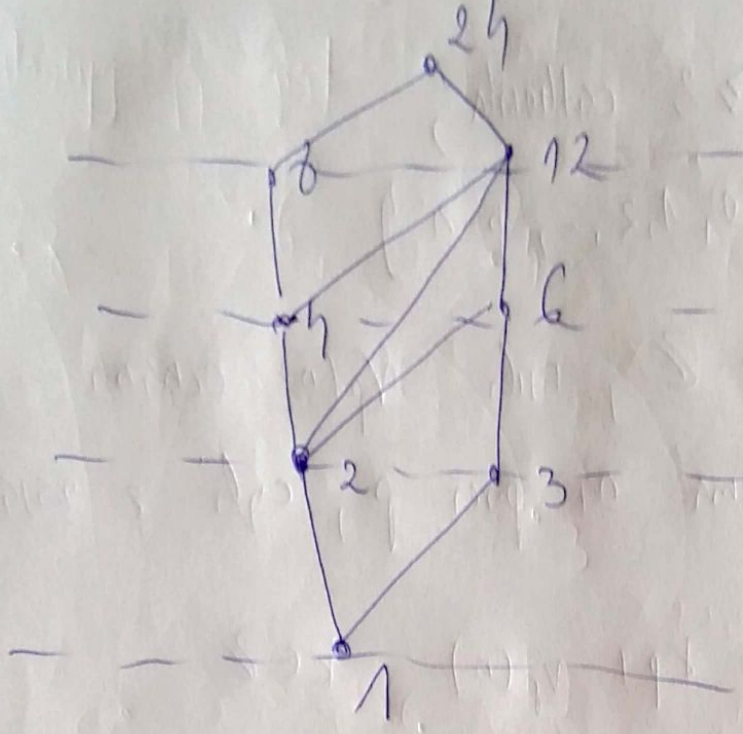
Niech R jest: (R2), (RA), (RP).

Skonstruujmy jej graf



Jak widać wygląda to „niezbyt czytelnie" .. Spróbujmy wyzyskując własności R „uproszczając" G_R : pomijamy pętle, i „efekt przechodniości" oraz nie będziemy rysowali krawędzi skierowanych, a uwzględnimy „hierarchię" wierzchołków.

Otrzymujemy tzw. diagram Hassego :



Mamy $3 < 6 < 12 < 24$

Ale „6" p' nashpmiki „3"

„12" „6"

„24" „8"