Kurs: Matematyka DYSKRETNA

Forma: Wykład

Typ: On-line

W.8

Temat. Kongruencja jako przykład relacji równoważności. Częściowy porządek.

Wiemy, że relacja $R \subset A \times A$ typu równoważność wyróżnia nam A na zbiory - klasy abstrakcji. I na odwrót, każdy podział zbioru A z klasy abstrakcji pewnej relacji równoważności.

Zad 1.

Niech $\mathcal{P} = \{A_t, t \in T\}$ będzie podziałem A. Zdefiniować r. równoważności generującą $\mathcal{P}$.

Zad 2. Przeczytać przykład 3.4.5 [ZR].

Zjawisko kongruencji

Niech $\mathbb{Z}$ oznacza zbiór l. całkowitych, $p > 1$ będzie z $\mathbb{Z}_+$.

Powiemy, że $n, m \in \mathbb{Z}$ przystają modulo p, będziemy pisali:

$n \equiv m \pmod p$, jeśli

$p \mid (n-m)$ (p dzieli $n-m$).

Mamy więc relację $R_p \subset \mathbb{Z} \times \mathbb{Z}$ $\left(= (\mathrm{mod}\, p)\right)$.

Zad.

Udowodnić, że R_p jest relacją równoważności.

Zbadamy bliżej własności tej relacji.

W tym celu zdefiniujmy funkcję

$$\nu_p : \mathbb{Z} \longrightarrow \mathbb{Z}_p,$$

gdzie $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ oraz

$\forall_{n \in \mathbb{Z}}$ $n = kp + \nu_p(n)$, gdzie zgodnie z zasadą podzielności, $0 \le \nu_p < p-1$

Oznaczmy reszty z dzielenia liczby n przez p.

FAKT 1.

$$\forall_{n,m\in\mathbb{Z}} \quad n \equiv m \pmod{p} \iff \nu_p(n) = \nu_p(m)$$

Dowód. Przeczytaj dowód F. 3.4.4 [RR].

Potrzebny jeszcze jeden ułamek.

Fakt 2.

$$\forall_{n,n',m,m'\in\mathbb{Z}} \quad \text{jeśli } n \equiv n' \pmod{p} \text{ i } m \equiv m' \pmod{p},$$

to

$$n+m \equiv n'+m' \pmod{p}$$
$$n \cdot m \equiv n' \cdot m' \pmod{p}$$

Dowód. Przeczytaj dowód Faktu 3.4.5 [RR].

Ponieważ $\forall_{n\in\mathbb{Z}} \; n \equiv \nu_p(n) \pmod{p}$, więc z Faktu 2 mamy:

Fakt 3

$$\forall_{n,m\in\mathbb{Z}} \quad \nu_p(n) + \nu_p(m) = n+m \pmod p$$
$$\nu_p(n)\cdot\nu_p(m) = n\cdot m \pmod p$$

Tezę Faktu 3 pokazuje się z pewnych uniwersalnych relacji modulo dodawanie i mnożenie l. całkowitych można opisać odpowiednimi działaniami na zbiorze skończonym $\mathbb{Z}_p$.

Zdefiniujmy te działania — oznaczmy je odpowiednio $\oplus_p$ i $\odot_p$ i nazwijmy: dodawaniem modulo p oraz mnożeniem modulo p, gdzie z def.

$$\forall_{n,m\in\mathbb{Z}_p} \quad n \oplus_p m = \nu_p(n+m)$$
$$n \odot_p m = \nu_p(n\cdot m).$$

No i wreszcie, jak mówiłem

$$\mathbb{Z} \ni n \longrightarrow \nu_p(n) \in \mathbb{Z}_p,$$

a pomysłem dowodzącym, że funkcja ν_p przenosi algebrę $(\mathbb{Z}, +, \cdot)$ na $(\mathbb{Z}_p, \oplus_p, \odot_p)$, bowiem

$$\forall_{n,m \in \mathbb{Z}} \quad \nu_p(n+m) = \nu_p(n) \oplus_p \nu_p(m)$$
$$\nu_p(n \cdot m) = \nu_p(n) \odot_p \nu_p(m)$$

Zad. 4 Udowodnić pomysł.

Przykład. $p = 2$, $\mathbb{Z}_2 = \{0, 1\}$

$\oplus_2$	0	1
0	0	1
1	1	0

$\odot_2$	0	1
0	0	0
1	0	1

Uwaga. To nie to samo, co $\oplus_6$, $\odot_6$ (!).

Przykład

$p=6$, $\mathbb{Z}_6=\{0,1,2,3,4,5\}$

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Zad 5. Skonstruować tabelę dla $\odot_6$.

Zad 6. Uzasadnić, że z tego, że $n \odot_p m = 0$ nie musi wynikać, że $n=0 \vee m=0$.

Zatem „$\cdot$" różni się od $\odot_p$!

Najwcześniejszy sygnał mamy wtedy, gdy p jest liczbą pierwszą.

Zad 7.

Niech p będzie l. pierwszą. Udowodnimy $\mathbb{Z}_p$ jest ciałem algebraicznym, czyli:

(i) w $\mathbb{Z}_p$ są dwa wyróżnione elementy
– 0 i 1

(ii) dwa działania: $\oplus_p$, $\odot_p$

(iii) oba są przemienne i łączne

(iv) 0 jest el. neutralnym dla $\oplus_p$
1 – " – dla $\odot_p$

(v) $\odot_p$ jest rozdzielne względem $\oplus_p$

(vi) $\forall n \in \mathbb{Z}_p \; \exists! \, m \in \mathbb{Z}_p$
$n \oplus_p m = 0$

(VII) $\forall_{n \in \mathbb{Z}_p, n \neq 0} \exists_{m \in \mathbb{Z}_p} \; n \odot_p m = 1$

Zad 8.

Opisać relację $\mathbb{Z}$ relacją $(\mod p)$.

II Częściowy porządek – drugi sposób porządkowania elementów zbioru.

Niech $R \subset A \times A$.

Każda relacja R, która jest co najmniej $(R\mathbb{Z}) \& (RA) \& (RP)$ nazywa się częściowym porządkiem, a (A, R) nazywa zbiorem częściowo uporządkowym.

Niech $\preceq$ będzie częściowym porządkiem na A.

Dalej będziemy pisać:

$\forall_{a,b \in A} \; a \preceq b$ zamiast $a R b$.

Uwaga.

1°. Jeśli $a \leq b$ i $a \neq b$, to

piszemy $a < b$.

2°. Widzimy podobieństwo pomiędzy „$\leq$" na $\mathbb{R}$

a „$\subseteq$" na A.

Przykłady.

1°. $(\mathbb{R}, \leq)$ jest tak.

2°. $(\mathcal{P}(X), \subseteq)$ p. tak.

Zauważmy, że nie prawdą jest, że

$\forall$ $A \subseteq B$ lub $B \subseteq A$.

$A, B \in \mathcal{P}(X)$

Definicja.

Niech $(A, \leqslant)$ będzie częściowym porządkiem. Jeśli dodatkowo

$$\forall_{a,b \in A} \quad a \leqslant b \vee b \leqslant a,$$

to porządek $\leqslant$ nazywamy porządkiem liniowym, a zbiór A zbiorem uporządkowanym.

Przykłady.

$(\mathcal{P}(X), \subseteq)$ NIE JEST PORZĄDKIEM LINIOWYM

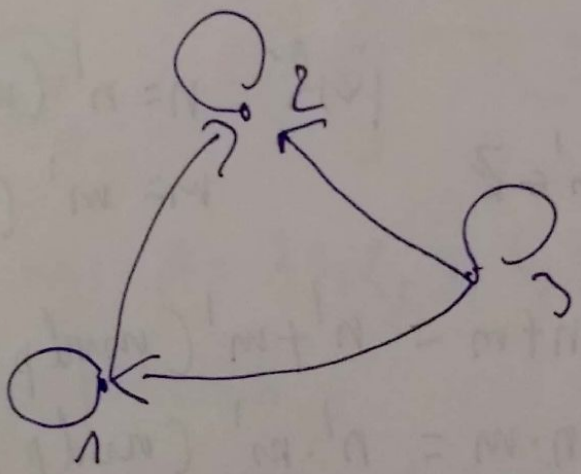
$(\mathbb{R}, \leq)$ JEST

→

Wyjaśnimy teraz na czym polega „porządkowanie" zbiorów relacją częściowego porządku.

Potrzebujemy pojęcia ŁAŃCUCHA — jest to każdy podzbiór zbioru cz. uporządk., który jest porządkiem.

Przykład.



Niech $\mathcal{R}$ będzie relacją przedstawioną grafem jak wyżej. Zauważ, że

$$(A, \mathcal{R}) = (A, \leq), \quad A = \{1, 2, 3\}$$

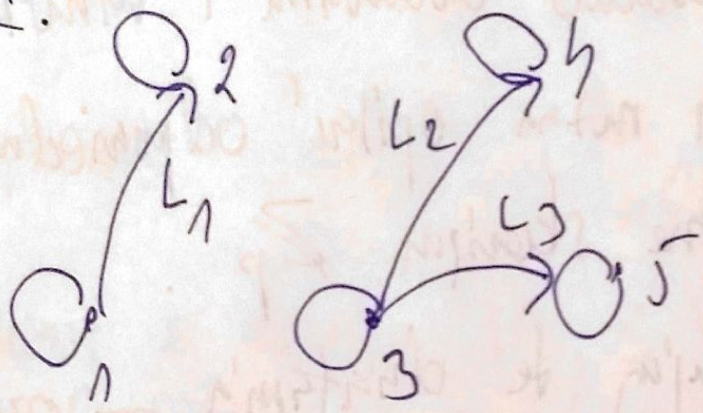
jest częściowym porządkiem.

Ponadto mamy:

$1 < 2$, $3 < 1 < 2$

Zatem $(A, \leqslant)$ ma ponadto, co oznacza że wszystkie elementy A sklasyfikowane są na tańcach.

Przykład.



Tutaj na $A = \{1, 2, 3, 4, 5\}$ mamy cztery ponadto.

Mamy 3 tańce: L_1, L_2, L_3

$(A, \leqslant)$ nie ma ponadto.

Mówi się, że $L \subset A$ jest łańcuchem w zbiorze częściowo uporządkowanym $(A, \leq)$ gdy $|L| = k$, to wszystkie elementy L można uporządkować „liniowo", tj.

$$l_1 < l_2 < \ldots < l_k.$$

Natomiast w dowolnym $(A, \leq)$ tak być nie musi (p. pomysłowe wyżej!).

Dlatego potrzebne kolejne pojęcia.

Niech $(A, \leq)$ cz. uporządk.

1° $b \in A$ jest maksymalny, jeśli

$$\forall_{c \in A} \; b \leq c \Rightarrow c = b$$

2° $a \in A$ jest minimalny, gdy jest maksymalny dla relacji odwrotnej.

3°. $b \in A$ jest największy, jeśli

$$\forall_{c \in A} \; c \leqslant b$$

4°. $a \in A$ jest najmniejszy, jeśli jest największy dla relacji przeciwnej.

Zad. Dla relacji ze str. 12 wskazać: ~~najmniejsze, największe~~ minimalne maksymalne.

Czy istnieją: największy i najmniejszy.

Można udowodnić (p. TU. 3.5.2 LRRT), że jeśli $(A, \leqslant)$ częściowy uporządkowany, A-skończony, to można z A wybrać takich L, że jego element pierwszy = min, ostatni = maksymalny.

Zad

Pokazać, że najmniej jeden obraz p zawiera maksymalny, ale nie na odwrót.

Na kolejnym wykładzie pokazemy własne pewniki (IT) relacji częściowego porządku.