

Første feedback på midtvejsevaluering:

Eksamen

Uafhængig af obl. opg. / tests

- Eksamenskaraktoren afhænger kun af tester i januar
- Obl. opg. / tests er ikke en forudsætningsprøve

Alle hjælpemidler, bortset fra Internet, tilladt

Ekstra opgaver

Gamle eksamensopgaver er altid relevante

Sidste gang:

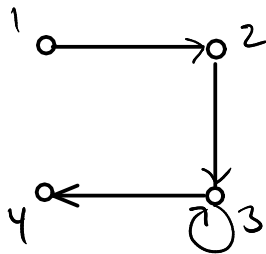
Kombinationer af relationer (Afsnit 9.1)

$$R_1 \cup R_2, R_1 \cap R_2, R_1 - R_2, R_1 \oplus R_2$$

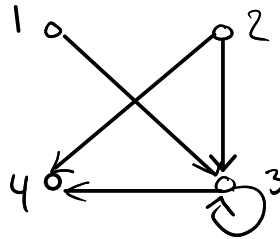
$$R_1 \circ R_2 = \{ (a, c) \mid \exists b : (a, b) \in R_2 \wedge (b, c) \in R_1 \}$$

$$\text{Eks: } R = \{ (1, 2), (2, 3), (3, 3), (3, 4) \}$$

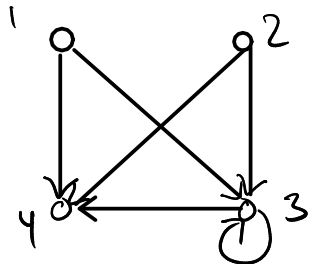
G_R :



G_{R^2} :



G_{R^3} :



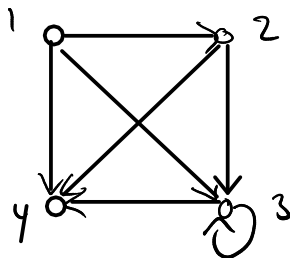
$$R^2 = R \circ R = \{ (1, 3), (2, 3), (2, 4), (3, 3), (3, 4) \}$$

$$R^3 = \{ (1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4) \}$$

$$t(R) = R^+ = R \cup R^2 \cup R^3$$

$$= \{ (1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4) \}$$

$G_{t(R)}$:



Ækvivalensrelationer (Afsnit 9.5)

Refleksiv, symmetrisk, transitiv

Eks:

✓: =, samme paritet, parallel

✗: $\neq$, $|$, $\leq$

$[a]_R = \{b \mid aRb\}$ kaldes a 's ækv.klasse

Eks:

$R = \{(a,b) \mid a \text{ har samme paritet som } b\}$ på $\mathbb{N}$

$[0]_R = \{0, 2, 4, \dots\} = [2]_R = [4]_R = \dots$

$[1]_R = \{1, 3, 5, 7, \dots\} = [3]_R = [5]_R = \dots$

Eks:

$S = \{(a,b) \mid a=b\}$ på $\mathbb{N}$

$[0]_S = \{0\}$

$[1]_S = \{1\}$

$[2]_S = \{2\}$

$\vdots$

Setning 9.5.1:

For enhver ækv.rel. R gælder

$\Updownarrow (a,b) \in R$

$\Updownarrow [a]_R = [b]_R$

$\Updownarrow [a]_R \cap [b]_R \neq \emptyset$

Sætning 1 kan bruges til at vise:

Sætning 9.5.2:

Lad A være en mængde. Da gælder

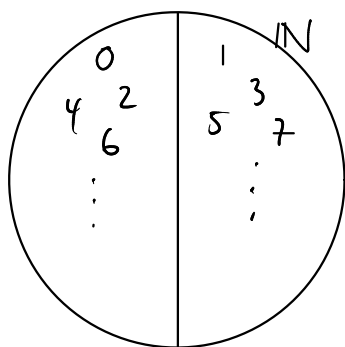
(1) R er en ækv.rel på $A \Rightarrow$

R 's ækv.klasser udgør en partitionering (disjunkt opdeling) af A .

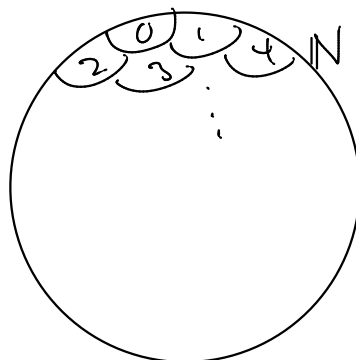
Det omvendte gælder også:

(2) For enhver partitionering af A findes der en ækv.rel., hvis ækv.klasser netop er mængderne i partitioneringen.

Eks: $R = \{(a,b) \mid a \text{ og } b \text{ har samme paritet}\}$ på $\mathbb{N}$



$S = \{(a,b) \mid a=b\}$ på $\mathbb{N}$



Beris for Sætning 9.5.2:

(1): Ækv.rel. $\Rightarrow$ partitionering: dvs. hvert element er indeholdt i præcis én mængde.

Ækv.klasserne dækker hele A , dvs. $\bigcup_{a \in A} [a] = A$:

$a \in [a]$ for alle $a \in A$, da R er refleksiv

D.v.s. ethvert element i A er indeholdt i en ækv.klasse.

Ækv.klasserne er disjunkte, dvs. $[a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset$

Kontraposition: $[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$

↑
Sætning 1

(2): Partitionering $\Rightarrow$ ækv.rel.:

Lad $R = \{(a,b) \mid a \text{ og } b \text{ tilhører samme mængde i part.}\}$

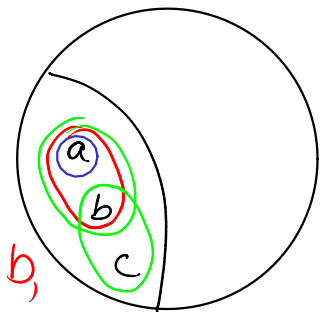
R er en ækv. rel.:

Refleksiv: for alle $a \in A$ gælder:

a tilhører samme mængde som a .

Symmetrisk: for alle $a, b \in A$ gælder:

Hvis a tilhører samme mængde som b ,
så tilhører b samme mængde som a .



Transitiv: for alle $a, b, c \in A$ gælder:

Hvis a tilhører samme mængde som b ,
og b tilhører samme mængde som c ,
så tilhører a samme mængde som c .

Mængdene i partitioneringen udgør R 's ækv.klasser, da hvert element er i samme mængde som præcis de elementer, det er relateret til.

D.v.s. hver mængde er ækv.klasse for hvert af de elementer, som den indeholder.

Partielle ordninger

(Afsnit 9.6)

Def 9.6.1

Hvis en relation R på en mængde A er
refleksiv, **antisymmetrisk** og transitiv,
kaldes den en **partiel ordening**.

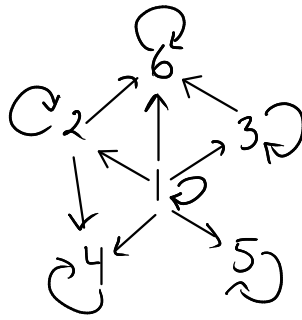
(A, R) kaldes en **partielt ordnet mængde** (poset)

Eks:

✓ : $\leq, =, |, \subseteq$

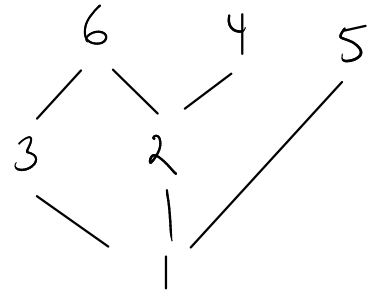
✗ : $<, \neq, \equiv, \subset$
refl. anti-sym. trans. refl.

Eks: $R = \{(a,b) \mid a|b\}$ på $\{1,2,3,4,5,6\}$



Hasse-diagram:

- Udelad alle kanter, som kan udledes af egenskaberne refleksiv og transitiv.
- Tegn a under b , hvis aRb .



Def 9.6.2

Lad $\preceq$ være en partiel ordning.
Hvis $a \preceq b$ eller $b \preceq a$, kaldes a og b
sammenlignelige.

Def. 9.6.3

Lad $(A, \preceq)$ være en partielt ordnet mængde.
Hvis alle par $a, b \in A$ er sammenlignelige,
kaldes $\preceq$ en total ordning

Ex:

$\sqrt{\cdot} : \preceq$

$\% : =, |, \subseteq, <$

6
|
5
|
4
|
3
|
2
|
1

Leksikografisk ordning $\leq$

$\leq_1, \leq_2$: partielle ordninger

$a <_1 b$ betyder $a \leq_1 b \wedge a \neq b$

Tilsvarende for $\leq_2$.

$(a_1, a_2) \leq (b_1, b_2)$, hvis

$a_1 <_1 b_1$

eller

$a_1 = b_1$ og $a_2 \leq_2 b_2$

Eks: Ordbog

Her er $\leq_1, \leq_2, \leq_3, \dots$ alfabetrækkefølge

Talteori (Afsnit 4.1)

Anvendelser:

Kryptologi (DM534 november)

Hashing (DM534 uge 39-40, DM507)

Pseudo-tillfældige tal

⋮

Def. 4.1.1:

For $a, b \in \mathbb{Z}$, $a \neq 0$, gælder:

$$a \mid b \Leftrightarrow \frac{b}{a} \in \mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z}: b = k \cdot a$$

"a går op i b" "a er en faktor i b"
"b er et multiplum af a"

Eks: $3 \mid 15$: $\frac{15}{3} = 5 \Leftrightarrow 15 = 5 \cdot 3$

$3 \mid 24$: $\frac{24}{3} = 8 \Leftrightarrow 24 = 8 \cdot 3$

(i) $3 \mid (15+24)$: $\frac{15+24}{3} = \frac{15}{3} + \frac{24}{3} = 5+8$
 $15+24 = 5 \cdot 3 + 8 \cdot 3 = (5+8) \cdot 3$

(ii) $3 \mid 75$: $\frac{75}{3} = \frac{5 \cdot 15}{3} = 5 \cdot 5 \Leftrightarrow 5 \cdot 15 = 5 \cdot 5 \cdot 3$

Kor. 1 $3 \mid 270$: $\frac{270}{3} = \frac{2 \cdot 15 + 10 \cdot 24}{3} = 2 \cdot 5 + 10 \cdot 8 \Leftrightarrow$
 $2 \cdot 15 + 10 \cdot 24 = (2 \cdot 5 + 10 \cdot 8) \cdot 3$

Mer generelt:

Sætning 4.1.1:

For $a, b, c \in \mathbb{Z}$, $a \neq 0$, gælder

$$(i) \quad a|b \wedge a|c \Rightarrow a|(b+c)$$

$$(ii) \quad a|b \Rightarrow \forall k \in \mathbb{Z}: a|kb$$

$$(iii) \quad a|b \wedge b|c \Rightarrow a|c$$

Korollar 4.1.1:

$$a|b \wedge a|c \Rightarrow \forall m, n \in \mathbb{Z}: a|(mb+nc)$$

Eks:

$$\begin{aligned} & \begin{cases} 3|15: & \frac{15}{3} = 5 \\ 15|60: & \frac{60}{15} = 4 \end{cases} \\ (iii) \Downarrow & \quad 3|60: \quad \frac{60}{3} = 5 \cdot 4 \end{aligned}$$

Bewis for Sætning 4.1.1 (i):

$$\begin{aligned} a|b \wedge a|c & \Rightarrow b=ka \wedge c=la, \quad k, l \in \mathbb{Z} \\ & \Rightarrow b+c = ka+la = (k+l)a, \quad k+l \in \mathbb{Z} \\ & \Rightarrow a|(b+c) \end{aligned}$$

□