

Ækvivalensrelationer (afsnit 9.5)

Def. 9.5.1:

En relation, som er

- refleksiv
- symmetrisk
- transitiv

kaldes en ækvivalensrelation.

Eks:

$$\sqrt{}: =, \equiv$$

$$\forall: \leq, |, \neq$$

Def. 8.5.2:

Hvis R er en ækv. rel., og $(a, b) \in R$,
da er a og b ækvivalente.

D.v.s. hvis R er en ækv. rel., og $(b, a) \in R$,
da er a og b ækvivalente (R er symmetrisk).

Def. 9.5.3:

Lad R være en ækv. rel. på A og
lad $a \in A$.

Da er a 's ækvivalensklasse

$$[a]_R = \{ b \mid (a, b) \in R \} = \{ b \mid (b, a) \in R \}$$

Eks: $R = \{(a,b) \mid a \equiv b \pmod{3}\}$ på $\mathbb{N}$

$$[0]_R = \{0, 3, 6, 9, \dots\}$$

$$[1]_R = \{1, 4, 7, 10, \dots\}$$

$$[2]_R = \{2, 5, 8, 11, \dots\}$$

$$[3]_R = \{0, 3, 6, 9, \dots\} = [0]$$

O.S.U.

Bemærk: $[0] \dot{\cup} [1] \dot{\cup} [2] = \mathbb{N}$ ($\dot{\cup}$: „disjunkt forening“)

Eks: $R = \{(a,b) \mid a=b\}$ på $\mathbb{N}$

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

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

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

$\vdots$

$$\text{Igen: } \mathbb{N} = [0] \dot{\cup} [1] \dot{\cup} [2] \dot{\cup} \dots$$

Ætning 9.5.1:

Lad R være en ækv.rel. på A .

Da gælder

$$aRb \quad (i)$$

$$\Updownarrow [a] = [b] \quad (ii)$$

$$\Updownarrow [a] \cap [b] \neq \emptyset \quad (iii)$$

Bevis:

Vil bevise $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$

$$\underline{aRb \Rightarrow [a] = [b] : \quad ((i) \Rightarrow (ii))}$$

Antag, aRb

Da er bRa , da R er symmetrisk

$$\underline{[a] \subseteq [b] :}$$

$$\uparrow c \in [a]$$



$$cRa$$

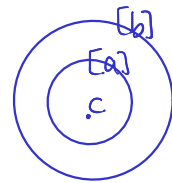


$$cRa \wedge aRb \quad (\text{vores antagelse})$$

$$\Downarrow cRb, \text{ da } R \text{ transitiv}$$



$$c \in [b]$$



D.v.s. alt, hvad der er i $[a]$, er også i $[b]$.

$$\underline{[b] \subseteq [a] :}$$

$$\uparrow c \in [b]$$



$$cRb$$



$$cRb \wedge bRa \quad (\text{vores antagelse})$$

$$\Downarrow cRa, \text{ da } R \text{ er transitiv}$$



$$c \in [a]$$

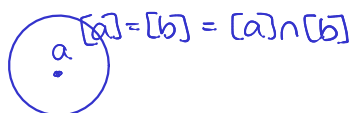


D.v.s. alt, hvad der er i $[b]$, er også i $[a]$.

$$\underline{[a] = [b] \Rightarrow [a] \cap [b] \neq \emptyset : \quad ((ii) \Rightarrow (iii))}$$

Skal blot vise $[a] \neq \emptyset$:

$a \in [a]$, da R er refleksiv

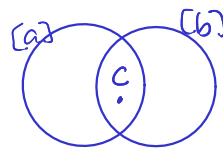


$$\underline{[a] \cap [b] \neq \emptyset \Rightarrow aRb : ((ii) \Rightarrow (i))}$$

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

$$\Updownarrow \exists c : aRc \wedge cRb$$

$$\Updownarrow aRb, \text{ da } R \text{ er transitiv}$$



Sætning 9.5.1 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.

Beris:

(1): Äkv.rel. $\Rightarrow$ partitionering:

Äkv.klasserna dölker hele A, dus $\bigcup_{a \in A} [a] = A$:

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

$$A = \bigcup_{a \in A} \{a\} = \bigcup_{a \in A} [a]$$

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

Kontraposition:

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

Gælder iflg. Sætning 9.5.1.

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

Lad R være relationen defineret ved, at aRb , hvis og kun hvis a og b tilhører samme mængde i partitioneringen.

Vi skal vise, at 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 .

Partielle ordninger (afsnit 9.6)

Def. 9.6.1:

En relation R på en mængde A , som er

- refleksiv,
- antisymmetrisk og
- transitiv

kaldes en partiel ordning.

(A, R) kaldes en partielt ordnet mængde.

Eks:

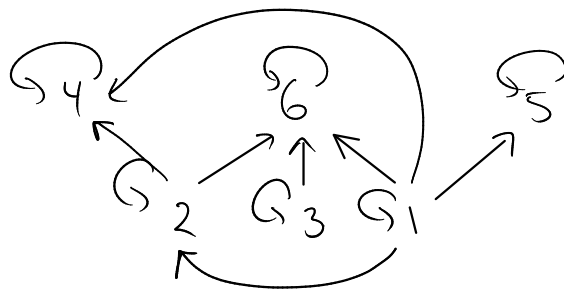
$\vee : \leq, =, |, \subseteq$

$\wedge : <, \neq, \equiv, \subset$

Eks:

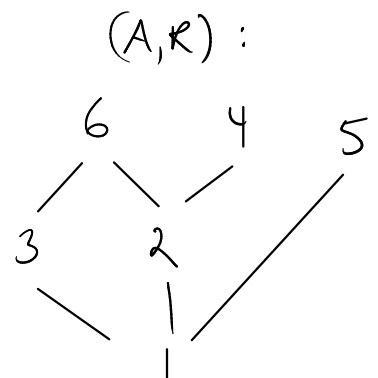
$A = \{1, 2, \dots, 6\}$, $R = \{(a, b) \in A \times A \mid a \mid b\}$

(A, R) :



Hasse-diagram:

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



Def. 9.6.2 :

Lad $\leq$ være en partiel ordning

Hvis $a \leq b$ eller $b \leq a$, kaldes a og b sammenlignelige.

Def. 9.6.3 :

Lad $(A, \leq)$ være en partielt ordnet mængde.

Hvis alle $a, b \in A$ er sammenlignelige,

kaldes $\leq$ en total ordning

Eks:

$\sqrt{} : \leq$

$\% : =, |, \subseteq$

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

$$a_1 <_1 a_2$$

eller

$$a_1 = a_2 \quad \text{og} \quad a_2 \leq_2 b_2$$

Eks: Ordbog

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

Talteori (afsnit 4.1)

Anvendelser: Kryptologi, hash-funktioner,
pseudo-tilfældige tal, ...

Def 4.1.1:

Lad $a, b \in \mathbb{Z}$ og $a \neq 0$.

$$\Leftrightarrow a \mid b \quad (a \text{ går op i } b)$$

$$\Leftrightarrow \frac{b}{a} \in \mathbb{Z}$$

$$\Leftrightarrow \exists c \in \mathbb{Z} : b = c \cdot a$$

$$(\Leftrightarrow b \bmod a = 0)$$

Hvis $a \mid b$, siger man også, at
 a er en **faktor i** b , eller
 b er et **multiplum af** a .

$a \nmid b$: a går ikke op i b .

Sætning 4.1.1:

Lad $a, b, c \in \mathbb{Z}$. Da gælder

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

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

$$(iii) \quad a|b \wedge b|c \Rightarrow a|c \quad (\text{d.v.s. transitiv relation})$$

Beweis:

$$(i): \quad a|b \wedge a|c$$

$$\Downarrow \exists m, n \in \mathbb{Z}: b=ma \wedge c=na, \text{ ifølge Def. 4.1.1}$$

$$\Downarrow \exists m, n \in \mathbb{Z}: b+c = ma+na = (m+n)a$$

$$\Downarrow \exists t \in \mathbb{Z}: b+c = ta \quad (t=m+n)$$

$$\Uparrow a|(b+c)$$

$$(ii): \quad \text{Opgave 4.1.3}$$

$$(iii): \quad \text{Opgave 4.1.4}$$

Sætning 4.1.2 (Divisions-algoritmen)

Lad $a \in \mathbb{Z}$ og $d \in \mathbb{Z}^+$. Da gælder

$$\exists! q, r \in \mathbb{Z} : 0 \leq r < d \wedge a = dq + r$$

dividend
divisor
kvotient
rest

Def. 4.1.2

$$q = a \text{ div } d$$

$$r = a \text{ mod } d \quad (\text{"a modulo b"})$$

↑ skrives som % i mange prog.sprog

Eks: $47 = 5 \cdot 9 + 2$ — divisionen går ikke op

$$47 \text{ div } 5 = 9 \quad (\text{kvotient})$$

$$47 \text{ mod } 5 = 2 \quad (\text{rest})$$

når vi dividerer 47 med 5

$$42 = 7 \cdot 6 + 0 \quad \text{— divisionen går op}$$

$$42 \text{ div } 7 = 6$$

$$42 \text{ mod } 7 = 0$$

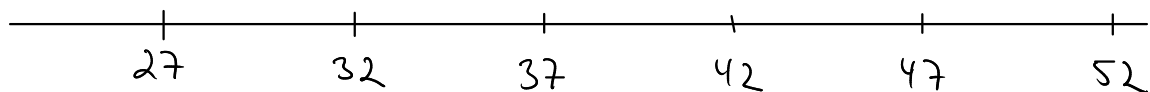
$$-47 = 5 \cdot (-10) + 3$$

$$-47 \text{ div } 5 = -10$$

$$-47 \text{ mod } 5 = 3$$

$$32 = 5 \cdot 6 + 2$$

$$\Rightarrow 47 \equiv 32 \pmod{5}$$



Alle disse tal er kongruente med hinanden modulo 5.

Def. 4.1.3 :

Lad $a, b \in \mathbb{Z}$ og $m \in \mathbb{Z}^+$. Da gælder

$$a \equiv b \pmod{m} \quad (a \text{ og } b \text{ er kongruente modulo } m)$$
$$\iff m \mid (a-b)$$

$a \not\equiv b \pmod{m}$: a og b er ikke kongruente modulo m

Kongruens kan defineres på mange måder:

$$\text{Def. 4.1.3} \iff \begin{aligned} &a \equiv b \pmod{m} \\ &m \mid (a-b) \end{aligned}$$

$$\text{Sætn. 4.1.3} \iff a \bmod m = b \bmod m$$

$$\text{Sætn. 4.1.4} \iff \exists k \in \mathbb{Z} : a = b + km$$