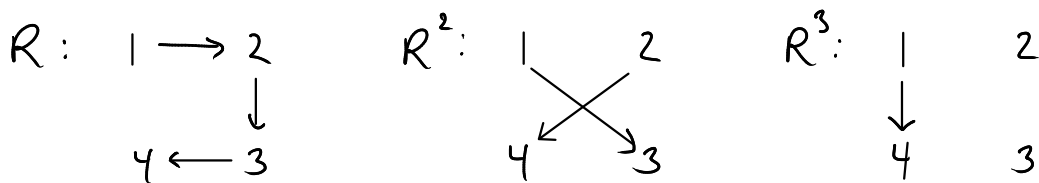


Sidste gang:

Transitiv lukning

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

$$\begin{aligned} t(R) &= R^* = R \cup R^2 \cup R^3 \cup R^4 \\ &= \{(1,2), (2,3), (3,4)\} \cup \{(1,3), (2,4)\} \cup \{(1,4)\} \cup \{\} \\ &= \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\} \end{aligned}$$



Ækvivalensrelation: (Afsnit 9.5)

Refleksiv, symmetrisk, transitiv

✓: $=$, samme paritet

✗: $\neq, <, \leq, |$

Ækvivalensklasse

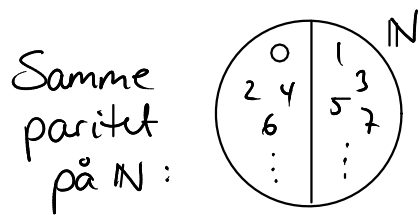
$$[a]_R = \{b \mid (a,b) \in R\} = \{b \mid (b,a) \in R\}$$

Ækvivalensklasserne for en ækvivalensrelation på en mængde A udgør en partitionering (disjunkt opdeling) af A .

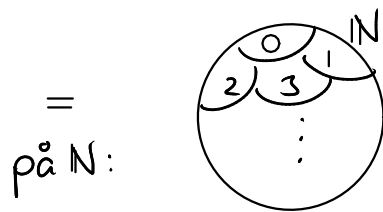
Og omvendt:

Enhver partitionering af A udgør ækv.klasserne for en ækv. relation.

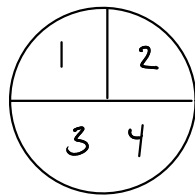
Eks:



$$\{(0,0), (0,2), (0,4), \dots, (2,0), (2,2), (2,4), \dots\}$$



$$\{(0,0), (1,1), (2,2), \dots\}$$



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

Partiel ordning: (Afsnit 9.6)

Refleksiv, **anti**symmetrisk, transitiv

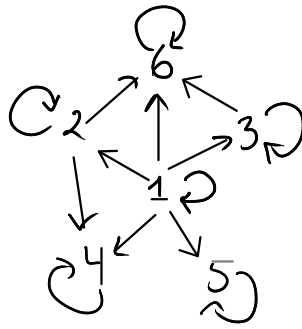
Eks:

✓: $=, |, \leq$

✗: $\neq, <, A \times A$

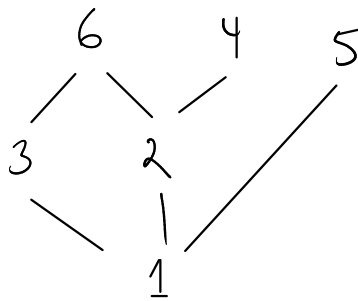
Hvis R er en partiel ordning på A ,
kaldes (A, R) en **partielt ordnet mængde** (poset).

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

! eks. overfor er 2 og 4 sammenlignelige, men 2 og 5 er ikke.

Def. 9.6.3

Lad $(A, \leq)$ være en partielt ordnet mængde.
Hvis a og b er sammenlignelige, for ethvert par $a, b \in A$,
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

$a_1 <_1 b_1$

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 december)

Hashing (DM534 uge 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) $3 \mid (15+24)$: $\frac{15+24}{3} = 5+8$
 $15+24 = 5 \cdot 3 + 8 \cdot 3 = (5+8) \cdot 3$

(ii) $3 \mid (7 \cdot 15)$: $\frac{7 \cdot 15}{3} = 7 \cdot 5 \Leftrightarrow 7 \cdot 15 = 7 \cdot 5 \cdot 3$

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

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):

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

□

Hvis en division ikke går op, bliver der en rest:

Eks: $16 = 3 \cdot 5 + 1$

Der bliver en rest på 1, når man dividerer 16 med 3.

$$16 \text{ div } 3 = 5$$

$$16 \bmod 3 = 1$$

$$-16 = 3 \cdot (-6) + 2$$

Der bliver en rest på 2, når man dividerer 16 med 3.

$$-16 \text{ div } 3 = -6$$

$$-16 \bmod 3 = 2$$

Sætning 4.1.2 (Divisionsalgoritmen):

For $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$ gælder

$$\exists! q, r : (a = d \cdot q + r \wedge 0 \leq r < d)$$

dividend

divisor

kvotient

rest

Def. 4.1.2

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

$$r = a \bmod d \quad \text{„a modulo d“}$$

Def. 4.1.3:

For $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ gælder

$$a \equiv b \pmod{m} \quad (\Leftrightarrow) \quad m \mid (a-b)$$

„a og b er kongruente modulo m”

Eks: $7 \equiv 16 \pmod{3}$, da $3 \mid (16-7)$
 $11 \equiv 11 \pmod{4}$, da $4 \mid 0$

Kongruens kan defineres på mange måder:

Def. 4.1.3

$$\begin{aligned} & a \equiv b \pmod{m} \\ & \Updownarrow \\ & m \mid (a-b) \quad (*) \end{aligned}$$

Sætning 4.1.3

$$\Updownarrow \\ a \bmod m = b \bmod m$$

Sætning 4.1.4

$$\Updownarrow \\ \exists k \in \mathbb{Z}: a = b + km \quad (**)$$

Bevis for Sætning 4.1.3: Opgave 21-22

Bevis for Sætning 4.1.4:

(**) er en simpel omskrivning af (*):

$$\begin{aligned} & m \mid (a-b) \\ & \Updownarrow \\ & a-b = km, \quad k \in \mathbb{Z}, \quad \text{ifølge Def. 4.1.3} \\ & \Updownarrow \\ & a = b + km, \quad k \in \mathbb{Z} \end{aligned}$$

□

For = må man addere og multiplicere med det samme tal på begge sider.

For $\equiv$ må man også *addere* og *multiplicere* med det "samme" tal på begge sider:

Sætning 4.1.5:

For $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ gælder

$$\begin{aligned} & \begin{cases} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{cases} \\ \Downarrow & \\ & \begin{cases} a+c \equiv b+d \pmod{m} \\ a \cdot c \equiv b \cdot d \pmod{m} \end{cases} \end{aligned}$$

Eks:

$$\begin{aligned} & \begin{cases} 5 \equiv 8 \pmod{3} \\ 4 \equiv 10 \pmod{3} \end{cases} \\ \Downarrow & \\ & \begin{cases} 9 \equiv 18 \pmod{3} \\ 20 \equiv 80 \pmod{3} \end{cases} \end{aligned}$$

Bevis for Sætning 4.1.5:

Bogen bruger Sætning 4.1.4.

Man kan også bruge Def. 4.1.3 og Sætning 4.1.1:

$$\begin{aligned} & a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \\ \Downarrow & m \mid (a-b) \wedge m \mid (c-d), \text{ ifølge Def. 4.1.3} \\ \Downarrow & m \mid (a-b+c-d), \text{ ifølge Sætning 4.1.1 (i)} \\ \Downarrow & m \mid (a+c-(b+d)) \\ \Downarrow & a+c \equiv b+d \pmod{m}, \text{ ifølge Def. 4.1.3} \end{aligned}$$

$$\begin{aligned} & a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \\ \Downarrow & a = b + km \wedge c = d + lm, \quad k, l \in \mathbb{Z}, \text{ ifølge Sætning 4.1.4} \\ \Downarrow & ac = (b+km)(d+lm), \quad k, l \in \mathbb{Z} \\ \Downarrow & ac = bd + bkm + kdm + klm, \quad k, l \in \mathbb{Z} \\ \Downarrow & ac = bd + (bl + kd + klm) \cdot m, \quad bl + kd + klm \in \mathbb{Z} \\ \Downarrow & ac \equiv bd \pmod{m}, \text{ ifølge Sætning 4.1.4} \quad \square \end{aligned}$$

Må man også subtrahere „samme“ tal på begge sider?

Må man dividere med samme tal på begge sider?