Disposition til

Diskret Matematik

Malthe Munk Karbo '14

11. juni 2017

INDHOLD

KAPITEL 1

HELE TAL

Taleplan

1. Definer de hele tal
2. Definer en divisor
3. DFP
4. GDFP
5. AFS

Beviser

Definition 1.1 (5)
*Et helt tal d kaldes en **divisor** i et andet helt tal a, hvis det findes et helt tal q så $dq = a$. Vi skriver $d|a$ og med det menes der at d går op i a og af er et **multiplum** af d.*

Definition 1.2 (11)
*Et helt tal $a \geq 2$ kaldes et **primtal** såfremt det ikke har andre divisorer end de trvielle divisorer $\pm a$ og ± 1.*

Definition 1.3 (13)
*Hvis $d|a$ og $d|b$ siges d at være en **fælles divisor** for a, b. Den største fælles divisor for $a, b \in \mathbb{Z}$ betegnes (a, b). Hvis $(a, b) = 1$ siges a og b at være **indbyrdes primiske**.*

Proposition 1.4 (26, **Det fundamentale primtalslemma**)
Hvis a og b er hele tal og p er et primtal, da gælder

$$p|ab \iff p|a \text{ eller } p|b.$$

Bevis.
Først vises $\Leftarrow$: Antag af $p|a$. Da findes $q \in \mathbb{Z}$ sådan at

$$a = pq$$

Og vi ser at $ab = pqb \iff \frac{pqb}{p} = qb \in \mathbb{Z}$ □

Proposition 1.5 (108, **Generelle fundamentale primtalslemma**)
Hvis $a_1, \ldots, a_n \in Z$ og p er et primtal, da gælder

$$p|a_1 \cdots a_n \implies p|a_i \text{ for et} 1 \leq i \leq n$$

Bevis.
For $n = 1$ gælder det. antag det gælder for n, altså hvis $a_1, \ldots, a_n \in \mathbb{Z}$ så gælder

$$p|a_1 \cdots a_n \implies p|a_i \text{ for et} 1 \leq i \leq n.$$

Antag nu at $a_1, \ldots, a_{n+1} \in Z$ og $p|a_1 \cdots a_{n+1} = (a_1 \ldots a_n)a_{n+1}$. Pr. DFP har vi at

$$p|(a_1 \ldots a_n) \text{ eller } p|a_{n+1}$$

Men per antagelse har vi

$$p|a_1 \text{ eller } p|a_2 \text{ eller } \ldots \text{ eller } p|a_n$$

og vi har da at

$$p|a_i$$

for eller andet $1 \leq i \leq n+1$ □

Proposition 1.6 (30, **Aritmetikkens fundamentalsætning**)
Ethvert naturligt tal $n > 1$ har en entydig primtalsopløsning, i.e. $\exists! p_1 \ldots p_s$ s.t.

$$n = p_1 p_2 \cdots p_s$$

KAPITEL 2

INDUKTION

Taleliste

1. Peanos axiomsystem
2. simpel induktion
3. fuldstændig induktion

Beviser

Definition 2.1 (**Peanos axiomsystem**)
De naturlige tal er en mængde $\mathbb{N}$ *med en funktion* $S\colon \mathbb{N} \to \mathbb{N}$ *s.t.*

1. $1 \in \mathbb{N}$.
2. *For* $n \in \mathbb{N}$ *gælder der* $1 \neq S(n)$.
3. *For* $m, n \in \mathbb{N}$ *gælder der* $m \neq n \implies S(n) \neq S(m)$.
4. ***INDUKTIONSAKSIOMET*** *Hvis* $A \subseteq \mathbb{N}$ *har egenskaberne* $1 \in A$ *og* $m \in A \implies S(m) \in A$ *så gælder* $A = \mathbb{N}$.

Proposition 2.2 (Simpel induktion)
Lad $p(x)$ *være et prædikat i* x *som løber over* $\mathbb{N}$. *Hvis der gælder for* $p(x)$ *at*

1. $p(1)$ *er sand,*
2. *for alle* $m \in \mathbb{N}$ *kan man af* $p(m)$ *slutte* $p(m+1)$*,*

da gælder $p(n)$ *for alle* $n \in \mathbb{N}$

Bevis.
Lad $p(x)$ være et prædikat i x over $\mathbb{N}$. Antag $p(1)$ er sand samt $p(m) \implies p(m+1)$ for alle $m \in \mathbb{N}$. Hvis

$$A = \{n \in \mathbb{N} | p(n) \text{ er sand}\}$$

opfylder $A \subseteq \mathbb{N}$ induktionsaksiomet:

$$1 \in A, \quad m \in A \implies S(m) = m + 1 \in A$$

så $A = \mathbb{N}$ og $p(n)$ er sand for alle $n \in \mathbb{N}$. □

Proposition 2.3 (**Fuldstændig induktion**)
Hvis $p(x)$ er et prædikat i x over $\mathbb{N}$ og

1. *$p(1)$ er sand*
2. *for alle $m \in \mathbb{N}$ kan man af $p(1), \ldots, p(m)$ slutte $p(m+1)$.*

Da er $p(n)$ sand for alle $n \in \mathbb{N}$.

Bevis.
lad $p(x)$ være et prædikat i $x \in \mathbb{N}$ og antag at $p(1)$ er sand og at man af $p(1), \ldots, p(m)$ kan slutte $p(m+1)$. Betragt

$$q(n) = (\forall k \in \mathbb{N} \colon k \leq n \implies p(k)).$$

Hvis $q(n)$ er sand for $n \in \mathbb{N}$ har vi at $k \leq n$ medfører $p(k)$ er sand for alle $k \in \mathbb{N}$, og da $n \leq n$ er $p(n)$ da sand. $q(1)$ er sand da $\forall k \leq 1 \implies p(k)$ er sand da $k \leq 1 \implies k = 1$ og $p(1)$ er sand. Antag nu er $q(m)$ er sand for m. Da $k \leq m$ er sandt for $k = 1, 2, \ldots, m$ har vi $p(k)$ for $k = 1, 2, \ldots, m$. pr. antagelse kan vi nu slutte $p(m+1)$. Men så har vi

$$k \leq m + 1 \implies p(k)$$

og så har vi $q(m+1)$ □

KAPITEL 3

MÆNGDELÆRER

Taleliste

1. Definition af ens mængder
2. Eksistens og entydighed af den tomme mængde $\emptyset$
3. Distributive love
4. De Morgan's love

Beviser

Definition 3.1
Lad A, B være mængder. Da er $A = B$ hvis

$$x \in A \iff x \in B.$$

Proposition 3.2 (Eksistens og entydighed af den tomme mængde)
Der eksisterer præcist én mængde uden nogen elementer

Bevis.
Lad A, B være tomme mængder. Da er $A = B$ for udsagnene

$$x \in A, \quad x \in B$$

er begge falske for alle x. □

Definition 3.3
For delmængder $A, B \subseteq X$ har vi følgende notationer

$$\begin{aligned} A \cap B &:= \{x \in X : x \in A \text{ and } x \in B\} \\ A \cup B &:= \{x \in X : x \in A \text{ or } x \in B\} \\ A \subseteq B &\text{ hvis } x \in A \implies x \in B \\ A \backslash B &:= \{x \in X : x \in A \text{ and } x \ni B\} \\ A^c &:= X \backslash A \end{aligned}$$

Proposition 3.4 (Distributive love)
For A, B, C mængder gælder

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Proposition 3.5 (Distributive lovea)
For en mængde A og end familie af mængder $\{B_i\}_{i \in I}$ gælder

$$A \cap \left(\bigcup_{i \in I} B_i \right) = \bigcup_{i \in I} (A \cap B_i)$$
$$A \cup \left(\bigcap_{i \in I} B_i \right) = \bigcap_{i \in I} (A \cup B_i)$$

Bevis.
Viser $A \cap \left(\bigcup_{i \in I} B_i \right) = \bigcup_{i \in I} (A \cap B_i)$:

$$\begin{aligned} x \in A \cap \left(\bigcup_{i \in I} B_i \right) &\iff (x \in A) \text{ and } (x \in \bigcup_{i \in I} B_i) \\ &\iff (x \in A) \text{ and } (\exists i \in I : x \in B_i) \\ &\iff \exists i \in I : (x \in A) \text{ and } (x \in B_i) \\ &\iff \exists i \in I : x \in A \cap B_i \\ &\iff x \in \bigcup_{i \in I} (A \cap B_i). \end{aligned}$$

Bevises for den anden identitet forløber analogt. □

Proposition 3.6 (De morgan's love)
Lad X være en mængde og $\{B_i\}_{i \in I} \subseteq X$ være en familie af delmængder af X. da gælder:

$$X \setminus \left(\bigcup_{i \in I} B_i \right) = \bigcap_{i \in I} (X \setminus B_i)$$
$$X \setminus \left(\bigcap_{i \in I} B_i \right) = \bigcup_{i \in I} (X \setminus B_i).$$

Bevis.

For den første, lad X og $\{B_i\}_{i\in I} \subseteq X$ som antaget. og vi ser

$$\begin{aligned} x \in X\setminus\left(\bigcup_{i\in I} B_i\right) &\iff x \in X \text{ and } x \notin \bigcup_{i\in I} B_i \\ &\iff x \in X \text{ and } \forall i \in I\colon x \notin B_i \\ &\iff \forall i \in I\colon x \in X \text{ and } x \notin B_I \\ &\iff \forall i \in I\colon x \in X\setminus B_i \\ &\iff x \in \bigcap_{i\in I}(X\setminus B_i) \end{aligned}$$

Beviset for den anden identitet forløber analogt. □

KAPITEL 4

ÆKVIVALENSRELTATIONER

Taleliste

1. En relation som delmængde
2. Definition på ækvivalensreltation
3. Definition på ækvivalensklasser
4. Sætning om entydighed af ækvivalensklasser
5. Definition på en klassedeling
6. Sætning: $M/_\sim$ er en klassedeling for alle $\sim$ ækvivalensrelationer

Beviser

Definition 4.1 (Relation som delmængde af kartesisk produkt)
For to mængde A, B er en relation $R \subseteq A \times B$. Den kan have forskellige egenskaber.

Definition 4.2 (**Ækvivalensrelationer**)
*En relation $\sim \subseteq A \times A$ er en ækvivalensrelation hvis den er **refleksiv, symmestrisk og transitiv**, i.e. hvis:*

1. *Refleksiv: $\forall x \in A \colon x \sim x$.*
2. *Symmetri: $x \sim y \implies y \sim x$.*
3. *Transitivitet: $(x \sim y)$ og $(y \sim z)$ medfører $x \sim z$*

Definition 4.3 (**Ækvivalensklasser**)
Hvis $\sim$ er en ækvivalensrelation på A. For $a \in A$ definerer vi mængden

$$[a] = \{x \in A \colon x \sim a\},$$

som vi betegner med ækvivalensklassen for a. Dette giver mening, da $\forall a \in A$ gælder der $a \sim a$ så $\forall a \in A \colon [a] \neq \emptyset$.

Proposition 4.4
Lad $\sim$ være en ækvivalensrelation på en mængde A. For $a, b \in A$ gælder der

$$[a] = [b] \iff a \sim b$$

Bevis.
" $\Rightarrow$ ": Antag $[a] = [b]$. Da $a \in [b]$ gælder der $a \sim b$. " $\Leftarrow$ ": Lad $a, b \in A$ med $a \sim b$. Da $a \in [a]$ samt $a \sim b$ gælder $a \in [b]$. □

Definition 4.5 (Klassedeling (**Partitioning**))
*En familie Ω af ikke tomme delmængder af en mængde M kaldes en **klassedeling** af M hvis elementerne i Ω er parvist disjunkte og foreningen er lig M, i.e.*

1. $\forall A \in \Omega \colon A \neq \emptyset$
2. $\forall A, B \in \Omega \colon A = B$ *eller* $A \cap B = \emptyset$
3. $\bigcup_{A \in \Omega} A = M$

Proposition 4.6 (Ækvivalensklasser udgør klassedeling)
Lad $\sim$ være en ækvivalensrelation på M. Da udgør ækvivalensklasserne $(M/_\sim)$ en klassedeling af M.

Bevis.
For $a \in M$ gælder der $a \in [a]$ $(a \sim a)$, så elementerne i $(M/_\sim)$ er ikke tomme. Pr. tidligere bevis har vi at $[a] = [b]$ eller $[a] \cap [b] = \emptyset$ for alle $a, b \in M$. For at vise $\bigcup_{a \in M} [a] = M$ viser vi inklusion to veje.

$$\forall a \in M \colon [a] \subset M \implies \bigcup_{a \in M} [a] \subset M.$$

$$a \in M \implies a \in [a] \implies a \in \bigcup_{a \in M} [a]$$

Som ønsket. □

KAPITEL 5

AFBILDNINGER

Taleliste

1. Definition på en relation
2. surjektivitet og injektivitet
3. billedmængde
4. sætning om billede af forening og billede af fællesmængde
5. evt modbeviser til sætningen ovenover

Beviser

Definition 5.1 (Afbildning)
Givet to mængder A, B sige en relation $f \subseteq A \times B$ at være en afbildning hvis

1. *Hvis $a \in A$ så eksisterer $b \in B$ sådan at afb.*
2. *Hvis $a \in A$ og $b_1, b_2 \in B$ sådan at afb_1 og afb_2 må $b_1 = b_2$.*

En relation som opfylder disse skrives $f \colon A \to B$.

Definition 5.2 (Surjektivitet)
*En afbildning $f \colon A \to B$ siges at være **surjektiv** hvis givet $b \in B$ så eksisterer et $a \in A$ sådan at*

$$f(a) = b.$$

Definition 5.3 (injektivitet)
*En afbildning $f \colon A \to B$ siges at være **injektiv** hvis givet der gælder for alle $x, y \in A$ at*

$$f(x) = f(y) \implies x = y$$

Definition 5.4 (Bijektivitet)
En afbildning $f \colon A \to B$ siges at være bijektiv hvis den både er injektiv og surjektiv

Definition 5.5 (Billedmængde)
For en afbildning $f\colon A \to B$ defineres billedmængden for f af en delmængde $M \subseteq A$ ved

$$f(M) := \{y \in B \colon \exists x \in M \ f(x) = y\}$$

Proposition 5.6 (Billedmængde inklusioner)
For en funktion $f\colon X \to Y$ og en familie af delmængder $\{T_i\}_{i\in I} \subseteq X$ gælder der

1. $f(\bigcup_{i\in I} T_i) = \bigcup_{i\in I} f(T_i)$.
2. $f(\bigcap_{i\in I} T_i) \subseteq \bigcap_{i\in I} f(T_i)$.

Bevis.
(1):

$$\begin{aligned} y \in f(\bigcup_{i\in I} T_i) &\iff \exists x \in X \colon x \in \bigcup_{i\in I} T_i \text{ and } f(x) = y \\ &\iff \exists x \in X \exists i \in I \colon x \in T_i \text{ and } f(x) = y \\ &\iff \exists i \in I \exists x \in X \colon x \in T_i \text{ and } f(x) = y \\ &\iff \exists i \in I \colon y \in f(T_i) \\ &\iff y \in \bigcup_{i\in I} f(T_i) : \end{aligned}$$

(2):

$$\begin{aligned} y \in f(\bigcap_{i\in I} T_i) &\iff \exists x \in X \colon x \in \bigcap_{i\in I} T_i \text{ and } f(x) = y \\ &\iff \exists x \in X \forall i \in I \colon x \in T_i \text{ and } f(x) = y \\ &\implies \forall i \in I \exists x \in X \colon x \in T_i \text{ and } f(x) = y \\ &\iff \forall i \in I \colon y \in f(T_i) \\ &\iff y \in \bigcap_{i\in I} f(T_i). \end{aligned}$$

□

\+ evt. modbevis til (2)

KAPITEL 6

KOMBINATORIK OG TÆLLEMETODER

Taleliste

1. Definer kardinalitet
2. Sætning om kardinalitet af disjunkte mængder A, B
3. Sætning om kardinalitet af $A \times B$ (modificeret bevis)
4. Sætning ovenover for $A_1 \times A_2 \times \cdots \times A_n$.

Beviser

Definition 6.1 (Kardinalitet)
For en mængde A skriver vi $|A|$ om $A's$ kardinalitet.

Proposition 6.2 (kardinalitet af disjunkte mængder)
For to endelige mængder A, B som er disjunkte gælder der

$$|A \cup B| = |A| + |B|.$$

Bevis.
For A, B med $|A| = n, |B| = m$ er der bijektive afbildninger $f\colon A \to \{1, \ldots, n\}$ og $g\colon B \to \{1, \ldots, m\}$. Sæt

$$h(x) = \begin{cases} f(x) & x \in A \\ m + g(x) & x \in B \end{cases}$$

. $h\colon A \cup B \to \{1, \ldots, n+m\}$ bijektivt. □

Proposition 6.3
For to endelige mængder $A \times B$ gælder der

$$|A \times B| = |A||B|$$

Bevis.
Lad $|A| = n$ og $|B| = m$. Vi ser at

$$A \times B = \bigcup_{1 \le i \le n} \{(a_i, b_k)\}_{1 \le k \le m}$$

Samt at for $k \neq s$ gælder der $\{(a_k, b_j\}_{1 \leq j \leq m} \cap \{(a_s, b_j)\}_{1 \leq j \leq m} = \emptyset$. Mængderne er oplagt ikke tomme, da A, B har kardinalitet > 0. Derfor har vi pr. den additive tællemetode for parvist disjunkte mængder, at

$$|A \times B| = \sum_{j=1}^{n} |\{(a_j, b_k)\}_{1 \leq k \leq m}| = \sum_{j=1}^{n} m = nm = |A||B|$$

□

KAPITEL 7

PERMUTATIONER

Taleliste

1. Definition på en permutation $\sigma\colon A \to A$
2. Sætning injektiv iff surjektiv *
3. Definition på flytpunkter og fixpunkter
4. Definition på en cykel
5. Definition på en Bane
6. sætning 412 - klassedeling baner
7. Cykelsætningen*

Beviser

Definition 7.1 (Definition på en permutation)
En bijektiv afbildning $\sigma\colon A \to A$ kaldes en permutation af mængden A

Definition 7.2 (Fix- og flyttepunkter)
For en permutation $\sigma\colon A \to A$ defineres mængderne

$$\mathit{fix}(\sigma) := \{a \in A\colon a = \sigma(a)\} \quad \mathit{flyt}(\sigma) := \{a \in A\colon a \neq \sigma(a)\}$$

Definition 7.3 (Definition på en cykel)
En p-cykel er en permutation σ af længde p hvor

$$\begin{aligned} \sigma(a_1) &= a_2 \\ \sigma(a_2) &= a_3 \\ &\vdots \\ \sigma(a_p) &= a_1 \end{aligned}$$

og den noteres med cykelnotation $\sigma = (a_1\ a_2 \dots a_p)$. Hvis $|A| = n > p$ er $\sigma(a_i) = a_i$ for $p < i \leq n$. (TEGNING)

Definition 7.4 (bane)
Lad σ være en permutation på en endelig mængde A. Da defineres banen for a under σ ved

$$B_a = \{a, \sigma(a), \sigma^2(a), \dots\}$$

dvs hvis vi sætter $a := a_1$ så udgør B_a en følge af p, nemlig $a_1, a_2, a_3, \dots, a_p$ elementer hvor p er længden af banen. Dertil ses det at en bane B svarer til en cykel γ, nemlig $(a_1\ a_2\ \dots\ a_p)$ med

$$\gamma(a) = \sigma(a)\ hvis\ a \in B$$
$$\gamma(b) = b\ ellers$$

Og vi får ydermere at

$$a \in B_b \iff B_a = B_b$$

Proposition 7.5 (banerne for en permutation udgør en klassedeling på en endelig mængde A)
Lad σ være en permutation på en endelig mængde A. Da udgør banerne for σ en klassedeling af A. Med andre ord

1. *Banerne er ikke tomme*
2. *Hvis to baner har et element tilfælles er de ens*
3. *foreningsmængden af alle banerne er hele A*

Bevis.
(1) og (3) følger direkte fra definitionen af banerne, da $\forall a \in A$: $a \in B_a$. **(2)**: hvis $c \in B_a$ og $c \in B_b$ da findes $m, n \in \mathbb{N}$ s.t. $c = \sigma^n(a)$ og $c = \sigma^m(b)$. for $m = n$ er vi færdige (injektivitet). Antag uden tab af generelitet at $m > n$. Da er

$$\sigma^n(a) = \sigma^m(a) = \sigma^{m-n+n}(a) = \sigma^n(\sigma^{m-n}(b))$$

og per injektivitet fås $a = \sigma^{m-n}(b)$ så $a \in B_b$ så $B_a = B_b$ □

KAPITEL 8

ORDNINGSRELATIONER

Taleliste

1. Definition på en ordningsrelation
2. Definition på en total ordningsrelation
3. Definition på en majorant
4. definition på supremum
5. Sætning om supremum

Beviser

Definition 8.1 (Partiel ordning)
En reltation $\leq \subseteq M \times M$ siges at være en partiel ordningsrelation hvis den er refleksiv, antisymmetrisk og transitiv, i.e.,

1. $\forall a \in M$ *gælder* $a \leq a$
2. $\forall a, b \in M$ *gælder* $a \leq b$ *og* $b \leq a$ *medfører* $a = b$
3. $\forall a, b, c \in M$ *gælder* $a \leq b$ *og* $b \leq c$ *medfører* $a \leq c$

Definition 8.2 (Totalordning)
Hvis $\leq$ er en partiel ordningsrelation på M som opfylder

$$\forall a, b \in M \colon a \leq b \quad \text{eller} \quad b \leq a$$

siges $\leq$ at være en total ordning på M.

Definition 8.3 (Majorant)
Lad $A \subseteq (M, \leq)$ være en delmængde, da er $x \in M$ en majorant for A hvis

$$\forall a \in A \colon a \leq x$$

Definition 8.4 (Supremum)
Lad $A \subseteq (M, \leq)$. Et element $b \in M$ er et supremum for A hvis

1. *b er en majorant for A*

2. b er den mindste majorant for A. (x majorant for A medfører $b \leq x$)

Proposition 8.5 (tilstrækkelige betingelser for supremum)
Lad $A \subseteq (M, \leq)$ hvor $(M, \leq)$ er totalordnet. Da er $b = \sup A$ hvis og kun hvis

1. *b er en majorant for A*
2. *$\forall x < b \; \exists a \in A \colon a > x$*

Bevis.
(1) følger af antagelse. **(2)**. Vi har

$$\begin{aligned} B = \sup A &\iff (x \text{ er en majorant for } A \implies b \leq x) \\ &\iff (x \text{ er en majorant for } A \implies \neg(x < b) \\ &\iff (x < b) \implies x \text{ ikke en majorant for A} \\ &\iff \forall x < b \exists a \in A \colon a > x \end{aligned}$$

som ønsket. □

hvor der er brugt totalordning samt kontraposition

KAPITEL 9

GRUPPER OG MODULÆR ARITMETIK

Taleliste

1. Definer komposition
2. Associativitet og kommutivitet for komposition
3. Definition gruppe
4. $a \equiv b \ (mod \ n)$ ækvivalens relation på $\mathbb{Z}$
5. $\mathbb{Z}/n\mathbb{Z}$ er en gruppe