MAT2400

Funksjoner

Formelt er en funksjon $f: A \to B$ en delmengde f av $A \times B$ slik at hvert element $a \in A$ forekommer i nøyaktig ett par (a,b) i f. Den tilhørende b'en betegnes med $f(a)$.

I praksis bruker man heller på en funksjon som en regel eller en tilordning som til hvert element $a \in A$ gir oss et element $f(a)$ i B. Noen ganger lønner det seg likevel å holde seg til definisjonen - det kan f.eks. være nyttig å si om funksjonen at $a \in f$.

Noen vanlige betingelser på funksjoner:

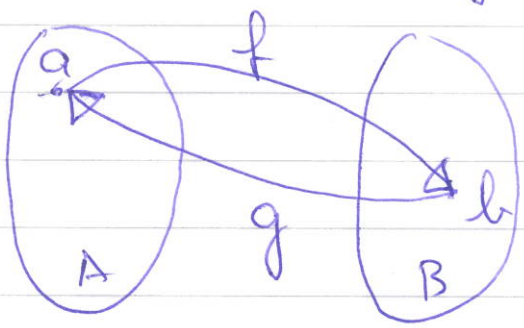
1) f er injektiv dersom $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

2) f er surjektiv dersom det for hver $y \in B$ finnes (minst) én $x \in A$ slik at $f(x) = y$

3) f er bijektiv dersom den er både injektiv og surjektiv.

Hvis f er bijektiv, gir den en entydig korespondanse mellom elementer i A og B. Det finnes derfor en omvendt/invers funksjon

$g: B \to A$ definert ved $g(b) = a$ dersom $f(a) = b$.



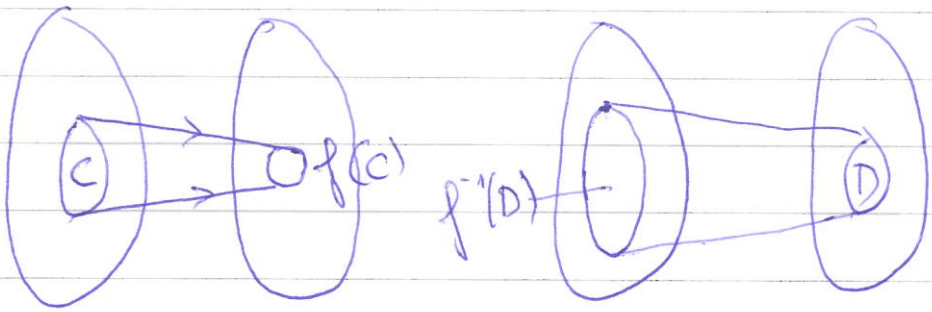
Vi har $f(g(y)) = y$ og $g(f(x)) = x$ for alle $y \in B$ og alle $x \in X$.

Direkte og inverse bilder: Dersom $C \subseteq A$, er bildet $f(C)$ av C under f definert ved

$$f(C) = \{f(c) : c \in C\}$$

Dersom $D \subseteq B$, er det inverse bildet av D under f definert ved

$$f^{-1}(D) = \{c \in C : f(c) \in D\}$$



Setning: Hvis $D, D_1, D_2, \ldots$ er delmengder av B, er

a) $f^{-1}(\bigcup_{n \in \mathbb{N}} D_n) = \bigcup_{n \in \mathbb{N}} f^{-1}(D_n)$

b) $f^{-1}(\bigcap_{n \in \mathbb{N}} D_n) = \bigcap_{n \in \mathbb{N}} f^{-1}(D_n)$

c) $f^{-1}(D^c) = (f^{-1}(D))^c$

Direkte bilder er litt verre:

Setning: Hvis $\{C_n\}$ er en familie av delmengder av A, er

a) $f(\bigcup_{n\in\mathbb{N}} C_n) = \bigcup_{n\in\mathbb{N}} f(C_n)$

b) $f(\bigcap_{n\in\mathbb{N}} C_n) \subseteq \bigcap f(C_n)$

Hvis f er injektiv, har vi likhet også i b)

Isomorfier er bijektive avbildninger som bevarer den strukturen vi er interessert i. Isomorfi mellom grupper bevarer gruppeoperasjonen, isomorfi mellom grafer bevarer kantstrukturen osv. La oss se nærmere på isomorfi mellom partielle ordninger.

Definisjon: Anta at $(X, \leq_X)$ og $(Y, \leq_Y)$ er to partielle ordninger. En isomorfi mellom de to ordningene er en bijeksjon $f: X \to Y$ slik at

$$x \leq_X y \iff f(x) \leq_Y f(y).$$

To partielle ordninger er isomorfe hvis det finnes en isomorfi mellom dem.

Talleori

Anta at $a, b \in \mathbb{Z}$. Et tall $c \in \mathbb{Z}$ er en <u>lineærkombinasjon</u> av a, b dersom det finnes tall $x, y \in \mathbb{Z}$ slik at

$$c = xa + yb.$$

<u>Setning</u>: c er en lineærkombinasjon av a og b hvis og bare hvis c er delelig med største felles divisor for a og b.

Man finner lineærkombinasjonen ved å bruke Euklids algoritme på a og b - først forlengs og så baklengs.

<u>Aritmetikkens fundamentalteorem</u>: Ethvert naturlig tall $n \geq 2$ kan skrives som et produkt $n = p_1 p_2 \cdots p_r$ på nøyaktig én måte.

<u>Korsetsregel</u>: Dersom et primtall p deler ab, deler det enten a eller b.

Kongruensregning

Anta $n > 1$. Vi definerer en ekvivalensrelasjon $\equiv \pmod n$ på $\mathbb{Z}$ ved

$$a \equiv b \pmod n \Leftrightarrow n \mid (a-b).$$

Ekvivalensklassene er: $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$.

$\mathbb{Z}/(n)$ er mengden av restklasser.

Algebraiske operasjoner: $\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} \cdot \bar{b} = \overline{ab}$

Nulldivisor: $\bar{a} \cdot \bar{b} = \bar{0}$ selv om $\bar{a}, \bar{b} \neq \bar{0}$.

p primtall: Ingen nulldivisorer, alle elementer har inverser.

n sammensatt: Nulldivisorer, elementer uten inverser.

Lineære kongruenser: $\bar{a}\bar{x} = \bar{b}$ i $\mathbb{Z}/(n)$

Alltid løsninger i $\mathbb{Z}/(p)$: $\bar{x} = \bar{a}^{-1}\bar{b}$.

Løsninger i $\mathbb{Z}/(n)$: Dersom b er delelig med (a, n).

Løsningsmetode: Finn linearkombinasjon

$b = ax + ny$. Da er $\bar{a}$ en løsning.

Tre sentrale teoremer

Fermats lille teorem: Hvis p er et primtall og $\bar{a} = \bar{0}$, er

$$\bar{a}^{p-1} = \bar{1} \quad i \quad \mathbb{Z}/(p)$$

Eulers teorem: Hvis a er innbyrdes primisk med n, er

$$\bar{a}^{\varphi(n)} = \bar{1} \quad i \quad \mathbb{Z}/(n)$$

$\varphi(n)$ = tall mindre enn n innbyrdes primisk med n

Wilsons teorem: For alle primtall er

$$\overline{(p-1)!} = -\bar{1} \quad i \quad \mathbb{Z}/(p)$$

Kvadratiske rester

$\bar{a} \in \mathbb{Z}/(p)$ er en kvadratisk rest dersom det finnes en $\bar{x} \in \mathbb{Z}/(p)$ slik at $\bar{a} = \bar{x}^2$.

Halvparten av de ikke-null elementene i $\mathbb{Z}/(p)$ er kvadratiske rester.

Eulers kriterium: $\bar{a} \neq \bar{0}$ i $\mathbb{Z}/(p)$ er en kvadratisk rest hvis og bare hvis $\bar{a}^{\frac{p-1}{2}} = 1$

Kardinalitet

Definisjon: En mengde A er **tellbar** dersom det finnes en følge $a_1, a_2, a_3, \ldots$ som inneholder alle elementene i A.

Setning: A er tellbar nøyaktig dersom det finnes en injeksjon $f: \mathbb{N} \to A$.

Setning: Hvis A, B er tellbare, er $A \times B$ tellbar.

Setning: Hvis $\{A_n\}$ er en følge av tellbare mengder, er $\bigcup_{n \in \mathbb{N}} A_n$ tellbar.

Setning: Hvis A er tellbar, er $f(A)$ tellbar.

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ er tellbare, $\mathbb{R}$ er ikke tellbar.

Eksempel: Vis at mengden av alle åpne intervaller $[a,b]$ med rasjonale endepunkter er tellbar.

Løsning: Siden $\mathbb{Q} \times \mathbb{Q}$ er tellbar, er delmengden

$R = \{[a,b) : a, b \in \mathbb{Q}, a \leq b\}$

tellbar. Siden funksjonen $f((a,b)) = [a,b]$ er en injeksjon, er mengden av tellbar.

Kardinalitet

Hvis A og B er to mengder, skriver vi $\text{card}\, A = \text{card}\, B$ dersom det finnes en bijeksjon $f: A \to B$

Vi skriver $\text{card}\, A \leq \text{card}\, B$ dersom det finnes en injektiv funksjon $f: A \to B$

Schröder-Bernsteins teorem: Hvis $\text{card}\, A \leq \text{card}\, B$, og $\text{card}\, B \leq \text{card}\, A$, så er $\text{card}\, A = \text{card}\, B$