Kapittel 4

Relasjoner og funksjoner

4.1 Ordnede par og liknende

Når vi ga eksempler på mengder og på hvordan vi kunne definere mengder, brukte vi $\mathbb{R}^2$ og løsningsmengder til likninger i noen av eksemplene. Vi gjorde det som er helt vanlig i matematikken, vi problematiserte overhode ikke hva disse elementene i $\mathbb{R}^2$ egentlig er. I så godt som alle fremstillinger av matematikkens mengdeteoretiske grunnlag er *ordnede par* et matematisk grunnbegrep som vi mener å forstå like godt som for eksempel tallene 3 og 17, vi forklarer hva vi mener og vi bare godtar at disse objektene finnes.
Dette skal være vår tilnærming også i dette kurset. Hvis a og b er to objekter, lar vi (a, b) være det *ordnede paret* av a og b. Det vesentlige er at rekkefølgen spiller en rolle, slik at om a og b er forskjellige, så er $(a, b) \neq (b, a)$. Dette kan vi uttrykke ved en regel for når to ordnede par er like:

$$(a, b) = (c, d) \text{ hvis og bare hvis } a = c \text{ og } b = d.$$

I oppgave 4.1.1 skal vi se på hvordan ordnede par kan defineres i mengdelæren, men forsøk på å bringe denne typen definisjoner til elever uten helt spesielle interesser for matematikk resulterer trolig i ødsling av tid.

Når vi har sagt hva vi mener med ordnede par, kan vi også definere $\mathbb{R}^2$ som mengden av ordnede par av reelle tall, $\mathbb{N}^2$ som mengden av ordnede par av naturlige tall, $\mathbb{Z}^2$ og $\mathbb{Q}^2$. Vi kan også definere *Kartesiske produkter* generelt:

Definisjon 4.1 La A og B være to mengder.
Med produktet $A \times B$ mener vi $\{(a, b) \mid a \in A \wedge b \in B\}$, altså mengden av ordnede par hvor det første elementet er fra A og det andre fra B.

I endel anvendelser av matematikk opererer vi ikke bare med ordnede par, men med ordnede trippler, ordnede kvadrupler, kvintupler m.m. Noen har vært utsatt for regning i x, y, z-rommet. Lesere av fysikk vil ha hørt om det firedimensjonale tid-rommet hvor et punkt er bestemt av fire koordinater: Plassering i et tredimensjonalt rom samt tiden punktet befinner seg i.

Vi vil definere begrepet *ordnet sekvens* med den samme grad av presisjon som vi brukte da vi definerte ordnet par:

Definisjon 4.2 La n være et naturlig tall. Med et *ordnet n-tuppel* eller en *ordnet sekvens av lengde n* mener vi et objekt $(a_1, \ldots, a_n)$. To ordnede sekvenser er like hvis de har samme lengde og er like punkt for punkt.

Eksempler 4.1 a) $(1, 3, 4, 2)$ og $(1, 3, 2, 4)$ er to 4-tupler (det vi innledningsvis kalte kvadrupler) eller ordnede sekvenser av lengde 4. De er ikke like fordi vi har byttet om på de to siste leddene.

b) $(1, \frac{1}{2}, \frac{1}{3})$ og $(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4})$ er to ordnede sekvenser, men de er ikke like fordi de har forskjellig lengde.

c) Det å skulle løse to likninger med tre ukjente kan uttrykkes som å skulle finne alle ordnede trippler (x, y, z) slik at for eksempel

$$x^2 + y^2 = z^2$$
$$x + y = z$$

I oppgave 4.1.2 skal vi se på hvordan vi kan utvide Kartesisk produkt til å omfatte mer enn to mengder. I oppgave 4.1.3 ser vi på hvordan vi også kan tufte definisjonen av endelige sekvenser på et mengdeteoretisk grunnlag.

Oppgaver til avsnitt 4.1

Oppgave 4.1.1 Hvis a og b er to objekter, kan vi definere $(a, b) = \{\{a\}, \{a, b\}\}$. Vis at hvis vi bruker denne definisjonen, så gjelder det at

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

Oppgave 4.1.2 Hvis A, B og C er mengder, lar vi $A \times B \times C$ være mengden av alle ordnede trippler (a, b, c) slik at $a \in A$, $b \in B$ og $c \in C$.

a) Gi en direkte definisjon av $\mathbb{N} \times \mathbb{R} \times \mathbb{N}$.

b) Prøv å formuler en definisjon av $A_1 \times \cdots \times A_n$ generelt.

c) Se på definisjonene av $A \times B \times C$, $A \times (B \times C)$ og $(A \times B) \times C$.
Drøft hvorfor disse mengdene strengt tatt er forskjellige og hva sammenhengen mellom dem er.

Oppgave 4.1.3 I oppgave 4.1.1 så vi på hvordan vi kan betrakte et ordnet par som en mengde.
Vi kan definere $(a, b, c) = ((a, b), c)$, $(a, b, c, d) = ((a, b, c), d)$ og så videre.

a) Forklar hvordan disse definisjonene kan utvides til en definisjon av *ordnet sekvens av lengde n* for enhver n, slik at karakteriseringen av når to ordnede sekvenser av lengde n er like holder.

b) [u]Definisjonen av en ordnet sekvens av lengde n som vi la opp til i a) har en svakhet. Hvis vi ser på $(((a,b),c),d)$ kan dette oppfattes både som et ordnet par, en ordnet sekvens av lengde tre og som en ordnet sekvens av lengde fire. Diskuter hvordan vi kan endre definisjonen av en ordnet sekvens slik at to ordnede sekvenser er like hvis og bare hvis de har samme lengde og er punktvis like.

Oppgave 4.1.4 Bestem hvilke ordnede par som er like av $(1,1)$, $(4,1)$, $((-1)^2, 2^2)$, $(1^2, (-1)^2)$, $(1,-1)$ og $(2^2,1)$.

Oppgave 4.1.5 Undesøk om noen av disse ordnede sekvensene av lengde 3 er like: $(1,4,9)$, $(4,9,1)$, $(1,2+2,3+3+3)$, $(1+3,1+3+5,3-2)$, $(9,4,1)$ og $(3^2,2^2,1^2)$.

Oppgave 4.1.6 La (a,b,c) og (d,e,f) være to ordnede sekvenser av reelle tall av lengde 3 slik at

- $a+b=d+e$
- $a+c=d+f$
- $b+c=e+f$

Vis at de to sekvensene må være like.

4.2 Relasjoner

Ordet 'relasjon' er et fremmedord på norsk som kan bety noe slikt som 'forbindelse', 'sammenheng' og 'forhold til'. Vi kan snakke om mellomfolkelige relasjoner når vi diskuterer hvordan land og folkeslag trives sammen, og vi kan snakke om at 'utgiftene må sees i relasjon til nytteverdien' når vi skal argumentere for kjøp av en dyr bil. Vi bruker den samme ordstammen når vi sprer om oss med det intelektuelle 'alt er relativt', og engelsmennene bruker ordet 'relative' om en så vanlig forbindelse som en slektning.

I matematikken vil vi bruke ordet 'relasjon' om en matematisk størrelse som beskriver en sammenheng mellom to objekter.
La oss se på noen eksempler før vi gir den formelle definisjonen.

Eksempler 4.2 a) Når vi regner med tall og ulikheter bruker vi symboler som $<$ og $\leq$. Disse uttrykker en sammenheng mellom to tall, nemlig at det ene er mindre enn det andre, eller at det er mindre eller lik det andre.

b) I tallteori er det at et tall er en faktor i et annet tall en viktig egenskap. Vi skriver ofte $a|b$ for å uttrykke at a er en faktor i b.

c) I et slektsregister er det viktig å markere hvem som er far eller mor til hvem, hvem som er gift med hvem, hvilket kjønn den enkelte har og muligens andre relasjoner.

Hvis vi kjenner til 'barn-foreldre'-relasjonen i slekten, kan vi også finne ut av hvem vi er etterkommere av. Dette er et eksempel på en relasjon hvorfra vi kan utlede andre relasjoner. Dette kommer vi tilbake til i Kapittel 5

d) I utsagnslogikken definerte vi hva vi mener med at et sammensatt uttrykk impliserer et annet eller at det er ekvivalent med et annet. Den presise definisjonen gjør $\Rightarrow$ og $\Leftrightarrow$ til relasjoner på mengden av sammensatte utsagn i utsagnslogikk.

d) Det er fullt mulig å snakke om relasjoner mellom objekter av vidt forskjellig karakter. På de fleste skoler er mengden av lærere disjunkt fra mengden av elever, men fortsatt kan vi snakke om lærer-elev-relasjonen i betydningen A er læreren til B i minst et fag.
Et annet eksempel på en relasjon som er av interesse for eiendomsregisteret, men hvor de to "aktørene" er vidt forskjellige er

Person A er eier av eiendom B.

Når vi skal lage en matematisk modell for relasjonsbegrepet er det viktig å få med seg de viktige aspektene, men ellers gjøre begrepet så generelt som mulig. Det er ingen grunn til å tro at vi kan begrense oss til å studere de relasjonene som er eller vil bli av interesse for noen. Det som er viktig er at en relasjon representerer en mulig sammenheng mellom to objekter, og at sammenhengen kan være asymmetrisk og mellom forskjellige sorter objekter. (Symmetri ville betydd, for eksempel i d) over, at huset og tomten min eier meg, og det er ikke tilfelle.

Definisjon 4.3 La A og B være mengder. En (binær) relasjon fra A til B er en delmengde $R \subseteq A \times B$.
Vi sier at R er en relasjon *på* A dersom R er en relasjon fra A til A.

Vi skrev ordet 'binær' i parentes for å antyde at definisjonen kan utvides til å omfatte at flere enn to objekter kan stå i et forhold til hverandre.
Hvis R er en relasjon fra A til B vil vi kalle A for *argumentområdet* til R og B for *verdiområdet* til R. Denne språkbruken vil falle oss mer naturlig etter at vi har lest avsnitt 4.3, men den antyder også at det kan være forskjell i viktighetsgrad mellom objektene i argumentområdet og objektene i verdiområdet. For en lærer er det av interesse hvilke elever hun/han har, så lærerne vil nok oppfatte seg som argumentområdet i lærer-elev-relasjonen. For elevene er det nok mere viktig å ha oversikt over hvilke lærere de har, og de vil nok heller se på elev-lærer-relasjonen.
I et personregister kan det være aktuelt å liste opp hvilke eiendommer den enkelte personen besitter, mens i et eiendomsregister vil det være viktig å liste opp den (eller de) som står som eier(e).
Det at det ofte er naturlig å se en relasjon fra to kanter, har ledet til at vi definerer den *inverse* relasjonen:

Definisjon 4.4 La R være en relasjon fra en mengde A til en mengde B. Med den *inverse* relasjonen mener vi relasjonen R^{-1} fra B til A definert ved

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

Eksempler 4.3 Vi så hvordan vi kan konstruere den inverse til en relasjon. Nå skal vi se på noen eksempler hvor vi konstruerer nye relasjoner fra gamle på andre interessante måter:

a) Hvis vi har gitt relasjonene 'mor til' og 'far til' har vi også indirekte gitt de fire relasjonene 'mormor til', 'morfar til', 'farmor til' og 'farfar til'.

b) Vi har tidligere antydet at 'lærer-elev'-relasjonen er av interesse. Det er ganske opplagt at for elevene er 'barn-foresatt'-relasjonen av interesse. Det innebærer imidlertid at lærerne også vil ha en gruppe foresatte de må forholde seg til. 'Lærer-foresatt'-relasjonen er avledet av de to foregående.

Vi skal nå gi en definisjon som fanger opp denne typen konstruksjoner:

Definisjon 4.5 La R være en relasjon fra A til B og S en relasjon fra B til C. Vi definerer *sammensetningen*

$$T = S \circ R$$

av R og S som en relasjon fra A til C ved

$$(a, c) \in T \text{ hvis det finnes } b \in B \text{ slik at } (a, b) \in R \text{ og } (b, c) \in S.$$

Hvis vi i eksemplet over lar M være 'mor til'-relasjonen og F være 'far-til'-relasjonen, vil $M \circ F$ være 'farmor', $M \circ M$ være 'mormor'. For å få Lærer-foresatt-relasjonen må vi se på $L \circ B$, hvol L er 'lærer til' og B er 'barn av'.

Oppgaver til avsnitt 4.2

Oppgave 4.2.1 La $A = \{1, 2\}$ og $B = \{1, 2, 3, 4\}$.
Forklar hvorfor det finnes 256 relasjoner fra A til B.

Oppgave 4.2.2 La $A = \{1, 2\}$, $B = \{3, 4\}$ og $C = \{5, 6\}$.
La $R = \{(1, 3), (2, 4)\}$ og $S = \{(3, 6), (4, 6), (3, 5)\}$.
Bestem argumentområdene og verdiområdene til S og T.
Finn S^{-1}, R^{-1} og $S \circ R$.
Kan du finne en relasjon som kan kalles $S^{-1} \circ R^{-1}$?
Vis at $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.
Tror du dette er en tilfeldighet?

Oppgave 4.2.3 Relasjonen $<$ på $\mathbb{N}$ er definert som

$$\{(n, m) \in \mathbb{N}^2 \mid n < m\}.$$

Vis at $(<)^2 \subset <$, det vil si at det er en ekte delmengde, hvor $(<)^2 =< \circ <$.
Er $\leq^2 = \leq$?

Oppgave 4.2.4 La R være relasjonen på $\mathbb{N}$ definert ved at $(n, m) \in R$ hvis $\frac{m}{n} \in \mathbb{N}$. Dette er den samme relasjonen som relasjonen | vi har sett på tidligere.

a) Forklar hvorfor $R^{-1} \circ R$ består av alle par av naturlige tall.

b) Beskriv $R \circ R^{-1}$ og forklar hvorfor du mener den er slik den er.

Oppgave 4.2.5 Finn et eksempel på en relasjon R på en mengde A slik at $R^{-1} \circ R \neq R \circ R^{-1}$.
Forklar hva som er sammenhengen mellom de to sammensatte relasjonene.

4.3 Funksjoner

Funksjonsbegrepet er viktig i matematikken, og egentlig mer fundamentalt enn relasjonsbegrepet. På barnetrinnet møter elevene funksjonene $+$, $-$, $\cdot$ og $:$ og lærer å regne med dem. I Grunnskolen lærer også elevene formler for arealet av en sirkel, volumet av en pyramide, overflaten av en kule og andre formler for areal og overflater. Alle disse formlene beskriver egentlig funksjoner.
På matematikk-intensive retninger på Videregående Skole blir elevene utsatt for en mer systematisk funksjonslære, gjennom kjennskap til trigonometriske funksjoner, logaritmefunksjonen og eksponensialfunksjonen, og sammenhengen mellom disse funksjonene er en viktig del av det de skal lære.
Det er naturlig å forestille seg at hvis man skal lage en matematisk modell for funksjonsbegrepet, så bør man prøve å fange opp hva slags sammenheng det kan være mellom det vi putter inn i funksjonen og det vi får ut. De fleste vil ha en forestilling av at det foregår en prosess fra argument til verdi. Denne forestillingen har mye for seg, og når man prøver å lage matematiske modeller for hvordan datamaskiner behandler inngangsdata og kommer med et svar, er det nettopp de viktigste aspektene ved en slik prosess man prøver å fange opp.

Når vi nå skal gi en mengdeteoretisk tolkning av hva vi mener med en funksjon, skal vi legge oss på et lavere ambisjonsnivå. Vi skal nevne to grunner til det:

1. Vi bør begrense oss til det ene grunnleggende aspektet ved funksjoner, nemlig at hvis vi putter noe inn får vi en og bare en ting ut. Hvis vi får bruk for å modellere flere aspekter får vi heller gjøre det ved å legge på tillegsinformasjon, ikke endre grunnbegrepet.

2. Det finnes mange situasjoner hvor vi med rimelighet kan snakke om funksjoner, men hvor det ikke er noen påtakelig sammenheng mellom inngangsdata og utgangsdata.

Definisjon 4.6 La A og B være mengder.
Med en *funksjon* $f : A \to B$ mener vi en relasjon f fra A til B slik at

For alle $a \in A$ finnes det en og bare en $b \in B$ slik at $(a, b) \in f$.

Når $f : A \to B$ er en funksjon fra A til B, skriver vi $f(a)$ for den ene b som er slik at $(a, b) \in f$.

Det vi her har gjort er å identifisere en funksjon med sin *graf*, nemlig relasjonen $f(a) = b$ som vi får ut fra vanlig språkbruk.

Eksempel 4.4 La $A = \{0, 1\}$ og $B = \{0, 1, 2, 3\}$. Da finnes det nøyaktig 16 forskjellige funksjoner $f : A \to B$, vi har fire valg for $f(0)$ og fire valg for $f(1)$. Disse valgene kan gjøres uavhengige av hverandre, så det totale antall friheter er $4 \cdot 4 = 16$.

Eksempel 4.5 Vi kan definere en funksjon $f : \mathbb{R} \to \mathbb{R}$ ved at $f(x) = x^3 - 17$ om x er et rasjonalt tall, mens $f(x) = 0$ ellers.
Poenget her er at f ikke er særlig kontinuerlig, og det kan bli svært vanskelig å tegne grafen til f. Likefullt er f en funksjon.

Eksempel 4.6 La $X = \{P_1, \ldots, P_n\}$ være en mengde utsagnsvariable.
La

$$V = \{f \mid f : X \to \{\top, \bot\}\}$$

og la

$$TAB = \{F \mid F : V \to \{\top, \bot\}\}.$$

V er mengden av fordelinger av sannhetsverdier til de gitte utsagnsvariablene, og det svarer til alle linjene i en sannhetsverditabell. TAB svarer da til alle mulige sannhetsverditabeller for de gitte utsagnsvariablene, når vi ikke tar hensyn til mellomregningene, men bare til sluttsøylen.
Dette illustrerer at vi kan fange opp mye mer enn funksjoner på tallmengder ved det generelle funksjonsbegrepet.

Da vi så på relasjoner generelt, definerte vi sammensetning av relasjoner. Den som er vant til å arbeide med funksjoner har trolig også sett på sammensetning av funksjoner:

$$(g \circ f)(x) = g(f(x)).$$

Hvis vi nå ser på vår definisjon av en funksjon som en relasjon, skal vi ha at $(x, z) \in g \circ f$ hvis og bare hvis det finnes en y slik at $(x, y) \in f$ og $(y, z) \in g$.
Skriver vi dette på den vanlige måten, er dette det samme som at det finnes en y slik at $y = f(x)$ og $z = g(y)$. Siden vi arbeider men funksjoner finnes det en og bare en y slik at $y = f(x)$, så $(x, z) \in g \circ f$ betyr det samme som at $z = g(f(x))$.

Hvis R er en relasjon fra A til B definerte vi R^{-1} som en relasjon fra B til A. Det betyr at hvis $f : A \to B$ er en funksjon har vi hjemmel for å snakke om f^{-1} som en relasjon fra B til A. Det er imidlertid en betenkelighet med den språkbruken, og det er at f^{-1} ikke alltid er en funksjon. Det kan være to grunner til at en relasjon S fra B til A ikke er en funksjon:

1. Det finnes en $b \in B$ slik at vi ikke har $(b, a) \in S$ for noen $a \in A$.

2. Det finnes en $b \in B$ slik at det finnes forskjellige a og c i A hvor vi har både $(b, a) \in S$ og $(b, c) \in S$.

Vi skal se på eksempler på funksjoner f hvor disse problemene oppstår for f^{-1}. La oss starte med problem 1:

Eksempel 4.7 La $f : \mathbb{N} \to \mathbb{N}$ være definert ved $f(x) = 2x$. Da er

$$f^{-1} = \{(2x, x) \mid x \in \mathbb{N}\}.$$

Hvis vi setter $x = 1$ er ikke $\frac{x}{2} \in \mathbb{N}$, så det finnes ingen $y \in \mathbb{N}$ slik at $(x, y) \in f^{-1}$.

Vi ser at vi får dette problemet hver gang $f : A \to B$ og det finnes en $b \in B$ som ikke er på formen $f(a)$ for noen $a \in A$.

Definisjon 4.7 La $f : A \to B$.
Vi sier at f avbilder A *på* B, eller at f er *surjektiv* dersom vi for alle $b \in B$ har en $a \in A$ slik at $f(a) = b$.

Eksempler 4.8 Følgende er eksempler på surjektive funksjoner:

a) La $\mathbb{R}^+$ være mengden av positive reelle tall. La $f : \mathbb{R} \to \mathbb{R}^+$ være definert ved
$$f(x) = 2^x.$$

b) La $f : \mathbb{N} \to \{0, 1, 2\}$ være definert ved at $f(x)$ er resten vi får når vi deler x på 3.

c) La $f : (\mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}) \to \mathbb{N}$ være definert ved $f(A)$ er det minste tallet i A.

Følgende funksjoner er eksempler på funksjoner som ikke er surjektive:

d) $f : \mathbb{R} \to \mathbb{R}$ definert ved $f(x) = 2^x$.

e) $f : \mathbb{N} \to \mathbb{N}$ definert ved $f(n) = n + 1$.

Ser vi på eksemplene a) og d) ser vi at vi kan gjøre en funksjon som ikke er surjektiv om til en funksjon som er surjektiv ved å endre på verdimengden, men egentlig ikke forandre funksjonen selv.

Det er ikke vanskelig å vise at sammensetningen av surjektive funksjoner er surjektiv. Dette overlates leseren som oppgave 4.3.2.

La oss nå se på et eksempel hvor problem 2 oppstår:

Eksempel 4.9 La $f : \mathbb{R} \to \mathbb{R}$ være definert ved

$$f(x) = x^2.$$

f er ikke surjektiv, men det er ikke noen stor hindring for å studere den inverse, det er bare å begrense den til ikke-negative tall (eller å utvide tallområdet til de komplekse tallene hvis man er fortrolig med dem). Det er et større problem at hvis $y > 0$ finnes det to tall x slik at $f(x) = y$.
Alle som har lært å løse 2. gradslikninger vet at vi bruker $\sqrt{x}$ som den inverse, og at vi bruker $\pm\sqrt{x}$ i formelen for løsningen til en 2.gradslikning.

Definisjon 4.8 La $f : A \to B$ være en funksjon. Vi sier at f er *enentydig* eller *injektiv* hvis vi for alle a og b i A har at om $f(a) = f(b)$, så er $a = b$.

Teorem 4.1 *La $f : A \to B$ være en funksjon som både er surjektiv og injektiv. Da er f^{-1} en funksjon fra B til A.*

Vi har allerede kommenter at det at f er surjektiv og injektiv svarer til de to betingelsene for at f^{-1} er en funksjon, så det er egentlig ikke noe å vise.

Selv om uttrykket f^{-1} gir mening for alle funksjoner f fordi de er relasjoner, skal man være forsiktig med å bruke det i andre tilfeller enn der f^{-1} faktisk er en funksjon, i alle fall bør man presisere at man fraviker denne anstendighetsregelen når man gjør det. I oppgave 4.3.4 skal vi se på en situasjon hvor en generell bruk av inverse funksjoner gir mening.

Et viktig aspekt ved inversdannelser i matematikken er at hvis man gjør noe og så gjør det motsatte (bruker den inverse) så skal man komme tilbake til utgangspunktet. Hvis man legger til et tall og så trekker det fra igjen er man tilbake til utgangspunktet og hvis man først multipliserer med et tall forskjellig fra null og så dividerer med det samme tallet er man også tilbake til utgangspunktet. Dette gjelder generelt for sammensetningen av en funksjon som har en invers med sin inverse, vi har alltid at $f^{-1}(f(x)) = x$.

Oppgaver til avsnitt 4.3

Oppgave 4.3.1 Undersøk hvilke av disse funksjonene som er surjektive, injektive og bestem f^{-1} der f har en invers:

a) $A = B = \mathbb{N}$ og $f(n) = n^2$.

b) $A = \mathbb{R}$, $B = \mathbb{R}^+$ og $f(x) = e^x$.

c) $A = B = \{1, 2, 3, 4, 5\}$ og $f(x) = 6 - x$.

d) $A = \{0, 1, 2, 3\}$, $B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ og $f(x) = x^2$.

e) $A = \mathbb{R}$, $B = [-1, 1]$ og $f(x) = \sin x$.

Oppgave 4.3.2 Vis at hvis $f : A \to B$ og $g : B \to C$ er surjektive funksjoner så er $(g \circ f) : A \to C$ også surjektiv.

Oppgave 4.3.3 Vis at hvis $f : A \to B$ og $g : B \to C$ er injektive funksjoner så er $(g \circ f) : A \to C$ også injektiv.

Oppgave 4.3.4 La $f : A \to B$ være en vilkårlig funksjon.
Hvis $C \subseteq B$ definerer vi det *inverse bildet* $f^{-1}[C]$ av C under f ved

$$f^{-1}[C] = \{a \in A \mid f(a) \in C\}.$$

Vis at det inverse bildet respekterer mengdealgebraen på B ved å vise

a) Hvis $C \subseteq B$ og $D \subseteq B$ er

$$f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]$$

og

$$f^{-1}[C \cup D] = f^{-1}[C] \cup f^{-1}[D].$$

b) Hvis $C \subseteq B$ er

$$f^{-1}[B \setminus C] = A \setminus f^{-1}[C].$$

Vi har brukt uttrykket $f^{-1}[\cdot]$ for å markere at dette er noe annet enn f^{-1} selv om det er et visst slektskap.
Drøft hva som er argumentområdet og verdiområdet til $f^{-1}[\cdot]$.

Oppgave 4.3.5 I lys av Oppgave 4.3.4 er det naturlig å definere det *direkte bildet* av en mengde under en funksjon som

$$f[C] = \{f(a) \mid a \in C\}.$$

a) Vis at hvis $f : A \to B$ $C \subseteq A$ og $D \subseteq A$, såvil

$$f[C \cup D] = f[C] \cup f[D].$$

b) La $A = \{1, 2, 3, 4\}$ og $B = \{1, 2\}$. La $f(1) = f(2) = 1$ og $f(3) = f(4) = 2$. La $C \subset A$ være mengden $\{1, 3\}$ og $D \subset A$ være mengden $\{2, 4\}$. Vis at $f[C \cap D] \neq f[C] \cap f[D]$ og at $f[A \setminus C] \neq B \setminus f[C]$.

c) Vis at vi for alle funksjoner $f : A \to B$, $C \subseteq A$ og $D \subseteq A$ har at

$$f[C \cap D] \subseteq f[C] \cap f[D].$$

d) [u] Finn naturlige egenskaper som sikrer at det direkte bildet respekterer snitt og komplement.

Oppgave 4.3.6 [u] La $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.
La $P : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ være definert ved

$$P(n, m) = \frac{1}{2}((n + m)^2 + 3m + n).$$

Vis at P er både injektiv og surjektiv.
[Hint: Regn ut $P(0, 0)$, $P(1, 0)$, $P(0, 1)$, $P(2, 0)$, $P(1, 1)$ og $P(0, 2)$ og se om du finner et mønster. Prøv å argumenter for at det mønsteret du finner fortsetter.]
Eksistensen av P viser at det i en viss forstand finnes like mange par av tall som tall. Cantor definerte to mengder A og B som like store hvis det finnes en $F : A \to B$ som er både injektiv of surjektiv. Hvis noen synes at dette strider mot sunn fornuft, så må man huske at dette bare er en teknisk definisjon av et matematisk begrep. Den stemmer overens med hva vi mener med 'like mange' for endelige mengder og viderfører noe (men ikke alt) av intuisjonen omkring 'like stor' til uendelige mengder.

4.4 Algoritmer

Da vi innførte funksjonsbegrepet innrømmet vi at det finnes mange sider ved vår intuitive oppfatning av hva en funksjon er som ikke blir fanget opp av definisjonen vår. Den viktigste intuisjonen er at en funksjon faktisk **gjør** noe med de argumentene vi gir den før den gir oss en verdi. I endel lærebøker blir funksjonsbegrepet forklart ved hjelp av en boks hvor vi putter x inn på den ene siden og så kommer $f(x)$ ut på den andre siden. Vi hevdet imidlertid også at det finnes så mange tilfeller hvor det kan være greit å snakke om funksjoner, men hvor det ikke er noen slik underliggende "prosess".

I dette avsnittet skal vi snakke om noen slike prosesser, om det vi kaller *algoritmer*. Det vil føre for langt å gå inn på noen systematisk behandling av algoritmebegrepet, dette er noe som hører inn under et dypere studium av informatikkens og matematikkens grunnlag. Siktemålet er gjennom noen eksempler å gi en intuisjon om hva en algoritme er og hvorfor det kan være interesssant å studere fenomenet mer systematisk.
Vi skal definere hva vi mener med en algoritme, men definisjonen er så upresis at algoritmebegrepet vårt ikke kan brukes til å formulere matematiske teoremer.

Definisjon 4.9 En *algoritme* er et sett regler som forteller oss hvordan vi mekanisk skal kunne finne en verdi $F(x)$ fra et argument x.

Eksempel 4.10 Når vi skal multiplisere to store tall, for eksempel $328 \cdot 542$ har vi lært at vi først multipliserer 2 med 328. På linjen under, og forskjøvet en plass til venstre, skriver vi 4 multiplisert med 328. Slik fortsetter vi til alle sifrene i tallet til høyre er multiplisert med tallet til venstre og svarene er skrevet under hverandre forskjøvet en plass for hver linje. Til slutt legger vi sammen alle linjene slik de står og får svaret.
Alle som kan multiplisere ensifrede tall med flersifrede tall og legge sammen flere flersifrede tall kan greie å multiplisere flersifrede tall med hverandre uten å forstå hvorfor det de gjør er riktig. de kan følge algoritmen mekanisk.
Det finnes selvfølgelig underliggende algoritmer for å multiplisere ensifrede og flersifrede tall med hverandre og for å summere flersifrede tall, og det eneste elevene virkelig må kunne er den lille multiplikasjonstabellen samt hvordan ensifrede og flersifrede tall legges sammen.

Eksempel 4.11 Elevene lærer også en algoritme for hvordan man deler et flersifret tall med et annet. Leseren vil kjenne denne algoritmen like godt som multiplikasjonsalgoritmen, så poenget her er bare at vi erkjenner at også divisjon er noe man lære å utføre mekanisk. Man trenger ikke å tenke seg om for å dividere riktig.

Eksempel 4.12 En kjent klassisk algoritme for å finne største felles faktor til to (store) tall er Euklids algoritme.
Den benytter seg av to observasjoner:

1. Hvis $n < m$ er to naturlige tall og n er en faktor til m, så er n den største felles faktoren til n og m.

2. Hvis $n < m$, n ikke er en faktor til m og k er resten vi får når vi deler m med n, så er den største felles faktoren til n og m den samme som den største felles faktoren til k og n.

Den første observasjonen er helt triviell, mens den andre trenger litt tankevirksomhet. Vi overlater observasjonen til leseren i ubevist tilstand, men leseren bør ikke oppfatte det som en avskrekking; det er lett.
Dette gir oss en algoritme for å finne den største felles faktoren til to tall, en algoritme som vi illustrerer med et eksempel, vi vil finne største felles faktor til 2331 og 171.
Ideen er at vi deler det største tallet på det minste, og fortsetter deretter med det minste og med resten, inntil divisjonen går opp. Da har vi funnet største felles faktor:

1. $2331 = 13 \cdot 171 + 108$
2. $171 = 1 \cdot 108 + 63$
3. $108 = 1 \cdot 63 + 45$
4. $63 = 1 \cdot 45 + 18$
5. $45 = 2 \cdot 18 + 9$
6. $18 = 2 \cdot 9$

Vi har på en helt mekanisk måte bestemt at den største felles faktoren til 2331 og 171 er 9.

Eksempel 4.13 Når jeg skriver dette kompendiet, bruker jeg et tekstbehandlingsystem som heter *Latex*. Den teksten jeg skriver på skjermen ser ganske anderledes ut enn den som kommer på trykk. For eksempel vil jeg skrive '\alpha' hvis jeg ønsker at det skal stå 'α'.
Poenget her er at det finnes en underliggende algoritme, et *program* som omformer det jeg skriver p{\aa} skjermen til det jeg ønsker at leseren skal se.
Programmer må oppfattes som algoritmer fordi de egentlig er instruksjoner som forteller en datamaskin hvordan den skal finne utgangsdata fra inngangsdata

Eksempel 4.14 En algoritme som begynnende datastudenter ofte får i oppdrag å skrive et program for er algoritmen for *Hanois Tårn*.
Hanois tårn består av tre pinner. På den ene pinnen ligger det n ringer i forskjellig størelse slik at det aldri ligger en større ring over en mindre. Poenget er å flytte alle ringene over til en av de andre pinnene ved bare å flytte én og én ring, og slik at vi aldri har en stor ring oppå en mindre.
Hvis $n = 1$ er det bare å flytte ringen.
Hvis $n > 1$ sier algoritmen at vi først må bruke den til å flytte de $n - 1$ øverste ringene til den tredje pinnen. Deretter flytter vi den største ringen dit den skal og til sist bruker vi algoritmen til å flytte de $n - 1$ mindre ringene fra den tredje pinnen til dit de skal.

Her har vi beskrevet algoritmen ved å henvise til at vi skal bruke algoritmen på en mindre mengde ringer. Siden vi vet hva vi skal gjøre når det bare er én ring, fungerer dette. Prøv selv med tre eller fire spillkort med forskjellige valører, 'puttebokser' eller liknende, og se at det virker.

Eksempel 4.15 Et annet eksempel på en selvkallende algoritme kan være følgende sorteringsalgoritme. Anta at vi har gitt en lang liste av navn og vi ønsker å sortere den alfabetisk. Hvis listen ikke var lang likevel, for eksempel bare inneholdt ett navn, så var den ferdigsortert. Algoritmen for å sortere en liste med ett navn er altså kjent, vi sier "i orden". Hvis listen er lenger, tar vi utgangspunkt i det øverste navnet på listen. Vi søker nedover i listen, og alle navn som kommer foran det første i alfabetet flyttes oppover. Samtidig sjekker vi om listen er ferdig sortert. Hvis listen er ferdig sortert, skriver vi "i orden" og avslutter. Hvis listen ikke er ferdig sortert bruker vi algoritmen på den delen av listen som nå er kommet over det navnet som opprinnelig sto øverst og vi bruker algoritmen på de navnene som ble stående igjen under. Når dette er gjort er listen ferdig sortert.

Sorteringsalgoritmen beskrevet i dette siste eksemplet er ikke den mest effektive og er mere egnet til å illustrere algoritmebegrepet enn til teknologiske anvendelser.

Det finnes prosesser som følger faste mønstre, men som ikke kan regnes som utførelse av algoritmer:

Eksempel 4.16

- Man putter 34 nummererte kuler i en beholder.
- Man blander kulene godt.
- Man trekker ut 7 av kulene, mens man blander mellom hver gang.
- Man deler et betydelig beløp på de som har krysset av syv nummererte ruter på et ark, og nummerne som er krysset av svarer til nummerene på de kulene som blir trukket ut.

Erfaring tilsier at resultatet av denne prosessen varierer fra gang til gang, selv om den blir riktig utført hver lørdag. Resultatet av en algoritme skal ikke være situasjonsavhengig så lenge utgangspunktet er det samme.

Oppgaver til avsnitt 4.4

Oppgave 4.4.1 Et populært eksempel blant matematikere som besøker grunnskolen er et spill hvor to spillere sitter med en felles bunke fyrstikker. Etter tur kan spillerne trekke en, to eller tre fyrstikker, og den som forsyner seg med den siste fyrstikken har vunnet.
Beskriv en algoritme som du kan benytte deg av slik at du i tre av fire spill er sikker på å vinne hvis du får lov til å begynne og som alltid sikrer at du vinner hvis motstanderen minst en gang ikke følger algoritmen.

Oppgave 4.4.2 La $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ være en funksjon, hvor vi antar at vi har en algoritme for å beregne f.
Definer h ved hjelp av følgende algoritme:

- $h(x, y) = x$ hvis $f(x, y) = 0$
- $h(x, y) = h(x, y + 1) + 1$ hvis $f(x, y) \neq 0$.

La $g(x) = h(x, 0)$.
Vis at $g(x)$ er den minste y slik at $f(x, y) = 0$ hvis det finnes en slik y, mens algoritmen for $g(x)$ aldri vil lede til noe svar hvis det ikke finnes noen slik y.
[Hint: h er slik at hvis $h(x, y)$ er definert, vil $f(x, y + h(x, y)) = 0$.]

4.5 Noen relasjonstyper

I dette avsnittet skal vi se på noen av de vanlige fremmedordene som brukes i tilknytning til binære relasjoner, og på noen av de viktigste relasjonstypene.

Definisjon 4.10 La R være en relasjon på en mengde A. Vi sier at R er

1. *refleksiv* hvis aRa for alle $a \in A$
2. *irrefleksiv* hvis ikke aRa for noen $a \in A$
3. *symmetrisk* hvis aRb medfører bRa for alle a og b i A
4. *antisymmetrisk* hvis aRb og bRa medfører at $a = b$ for alle a og b i A
5. *transitiv* hvis aRb og bRc medfører at aRc for alle a, b og c i A
6. *total* hvis vi for alle a og b i A har at aRb, bRa eller $a = b$

Alt i alt skulle vi ha 64 mulige kombinasjoner av disse egenskapene. Vi ser imidlertid at hvis R er både refleksiv og irrefleksiv vil $A = \emptyset$ og hvis R er både symmetrisk og antisymmetrisk kan A ha høyst ett element. Det er også anndre kombinasjoner som ikke vil oppstå eller som bare oppstår i trivielle og uinteressante tilfeller. Vi skal først se på noen lett gjenkjennelige relasjoner og se på hvilke egenskaper de har. Deretter vil vi definere noen klasser av relasjoner som er av spesiell interesse i matematikken og i den teoretiske informatikken.

Eksempler 4.17 a) La $A = \mathbb{N}$ og $R =<$. Da er R irrefleksiv, antisymmetrisk, transitiv og total. Dette vil også være tilfelle i mange andre situasjoner hvor vi snakker om 'mindre enn'.

b) La $A = \mathbb{N}$ og $R =\leq$. Da er R refleksiv, antisymmetrisk, transitiv og total. Dette vil også være tilfelle i mange andre situasjoner hvor vi snakker om 'mindre eller lik'.

c) La $A = \mathcal{P}(\{1, 2, 3\})$ og $R =\subseteq$. Da er R refleksiv, antisymmetrisk og transitiv. R vil ikke være total, for det finnes par av mengder slik at ingen av dem er inneholdt i den andre, eksempelvis $\{1, 2\}$ og $\{2, 3\}$.

d) La $A = \mathbb{Z}$ og aRb hvis vi får samme rest når vi deler a og b på 17. R er refleksiv, symmetrisk og transitiv. Dette er en relasjonstype vi ofte får når vi vil uttrykke at elementene deler noen egenskaper.

e) La $A = \mathbb{R}^2$ og la $(x, y)R(u, v)$ hvis $(x - u)^2 + (y - v)^2 < 1$, det vil si hvis avstanden mellom punktene er mindre enn 1.
R vil være refleksiv, symmetrisk men ikke transitiv.

f) La $A = \mathbb{R}^2$ og la $(x, y)R(u, v)$ hvis $(x - u)^2 + (y - v)^2 = 1$. Da er R symmetrisk og irrefleksiv.

Vi skal nå se på noen relasjonstyper.

Definisjon 4.11 La R være en relasjon på en mengde A.

a) Vi kaller R en *ordning* om R er transitiv, refleksiv og antisymmetrisk.

b) Vi kaller R en *strikt ordning* hvis R er transitiv og irrefleksiv.

c) En ordning eller strikt ordning kalles *total* hvis den er total som relasjon.

Noen ganger kan vi bruke betegnelsen *partiell ordning* hvis vi vil understreke at den ikke trenger å være total.

Lemma 4.1 *En strikt ordning er også antisymmetrisk.*

Bevis
Anta at R er en strikt ordning, og la aRb og bRa. Ved transitivitet vil aRa, noe som er i konflikt med at R er irrefleksiv. Vi kan derfor ikke ha at aRb og bRa samtidig.

I kapittel 6 vil vi se på bevisformer generelt, og da vil vi gjenkjenne dette som et kontrapositivt bevis.
I avsnittet om utfordringer skal vi se på en situasjon hvor det er naturlig å utvide en relasjon til en som er refleksiv og transitiv.

Definisjon 4.12 La R være en binær relasjon på en mengde A.
Vi definerer den *refleksive og transitive tillukningen* R^* av R som følger:
aR^*b hvis $a = b$ eller hvis det finnes $c_1, \ldots, c_n$ i A slik at $a = c_1$, $b = c_n$ og $c_i R c_{i+1}$ for alle $i < n$.

Vi har at aR^*b hvis $a = b$ eller hvis vi kan komme fra a til b ved endelig mange skritt slik at vi beveger oss langs relasjonen R i hvert skritt.

Lemma 4.2 *a) Hvis R er en binær relasjon på en mengde A, er R^* en refleksiv og transitiv relasjon på A.*

b) Hvis $R \subseteq S$ er binære relasjoner på en mengde A og S er refleksiv og transitiv, så vil $\mathbb{R}^* \subseteq S$.

Bevis
For å gi et formelt bevis trenger vi å ha lest Kapittel 8 om induksjonsbevis. Her vil vi basere oss på den intuisjonen som ligger til grunn for induksjonsbevis.

a) R^* er refleksiv fordi vi pr. definisjon har at aR^*a for alle $a \in A$.
Hvis aR^*b og bR^*c har vi at $a = b$, $b = c$ eller at vi kan komme fra a til b og videre fra b til c ved endelig mange R-hopp. I de to første tilfellene har vi opplagt aR^*c, og i det siste tilfellet setter vi sammen de to seriene av endelig mange R-hopp fra a til b og fra b til c til en endelig serie R-hopp fra a til c.

b) Hvis aR^*b fordi $a = b$ vil aSb fordi S er refleksiv.
Hvis aR^*b på grunn av rekken $c_1, \ldots, c_n$ av R-hopp, har vi at c_iSc_{i+1} for alle $i < n$ fordi $R \subseteq S$. Ettersom S er transitiv vil c_iSc_j hver gang $1 \leq i < j \leq n$ (det er her vi egentlig trenger induksjon) så vi har spesielt $a = c_1Sc_n = b$.

Eksempler 4.18 Vi skal se på følgende eksempler på den refleksive, transitive tillukningen:

a) La $A = \mathcal{P}(\mathbb{N})$ og la XRY hvis $X \subset Y$ og Y har ett element mer enn X.
Da vil XR^*Y hvis $X \subseteq Y$ og $Y \setminus X$ er endelig.

b) La A være en gjeng soldater stilt opp i en rad og la aRb hvis b står bak a i en armlengdes avstand og uten noen mellom dem. Da vil aR^*b hvis b ikke står foran a og alle soldatene mellom er stilt opp slik at alle har armlengdes avstand til soldaten foran.

c) La A være en samling dominobrikker som er stilt på høykant. Vi er interesserte i å vite hvilke brikker som vil falle dersom vi dytter på en av dem. Hvis vi lar aRb bety at b blir dyttet over ende i det a faller, vil R^* være den relasjonen vi egentlig er interessert i.

Definisjon 4.13 La R være en relasjon på en mengde A. Vi kaller R en *ekvivalensrelasjon* hvis R er refleksiv, symmetrisk og transitiv.

Vi så på et eksempel på en ekvivalensrelasjon, nemlig at vi får samme rest når vi deler på 17. Det er ikke noe spesielt med tallet 17, så vi har allerede uendelig mange eksempler her. La oss se på noen andre

Eksempler 4.19 a) La A være mengden av sammensatte utsagn i utsagnsvariablene P_1, P_2, P_3. Vi lar $\phi R\psi$ hvis $\phi \Leftrightarrow \psi$, det vil si hvis $\phi \leftrightarrow \psi$ er en tautologi.
Da er R en ekvivalensrelasjon.

b) En *vektor* er et par (x, y) av punkter i planet eller rommet. x kalles *roten* til vektoren og y kalles *spissen* til vektoren.
Det er vanlig å si at to vektorer er like hvis de har samme lengde og retning. Det uttrykker vi ved

$$(x, y)R(u, v) \Leftrightarrow y - x = v - u.$$

Dette er en ekvivalensrelasjon.

c) La A og B være mengder, $f : A \to B$ være surjektiv.
Da kan vi definere R på A ved $aRb \Leftrightarrow f(a) = f(b)$. Da er R en ekvivalensrelasjon.

Vi skal nå se at det siste eksemplet egentlig dekker alle ekvivalensrelasjoner. Hvis vi derfor tenker oss at f er en funksjon som avbilder a på mengden av egenskaper vi synes er interessante for øyeblikket, vil den tilhørende ekvivalensrelasjonen uttrykke at to objekter i A har de samme interessante egenskapene.

Definisjon 4.14 La R være en ekvivalensrelasjon på en mengde A og la $a \in A$. Vi lar *ekvivalensklassen* til a være

$$[a] = \{b \in A \mid aRb\}.$$

Teorem 4.2 *La R og A være som over.*

a) For alle $a \in A$ vil $a \in [a]$.

b) Hvis aRb vil $[a] = [b]$.

c) Hvis $\neg(aRb)$ vil $[a] \cap [b] = \emptyset$

Dette teoremet sier at hvis R er en ekvivalensrelasjon på A, så kan vi dele A opp i disjunkte klasser av parvis ekvivalente elementer.

Bevis
Siden aRa vil $a \in [a]$. Dette viser a).
La aRb. Siden vi da også har at bRa er det nok å vise at $[b] \subseteq [a]$ for å vise b). Så la $c \in [b]$. Da vil $aRb \wedge bRc$ så aRc. Det betyr at $c \in [a]$.
Til sist, anta at $c \in [a] \cap [b]$. Da vil $aRc \wedge bRc$. Ved symmetri og transitivitet for R følger det at aRb. Snur vi dette argumentet på hodet, får vi at $\neg(aRb) \Rightarrow [a] \cap [b] = \emptyset$. Dette viser c), og teoremet er bevist.

Oppgaver til avsnitt 4.5

Oppgave 4.5.1 La R være en relasjon på en mengde A slik at R er antisymmetrisk og irrefleksiv. Forklar hvorfor vi ikke kan finne a og b i A slik at aRb og bRa.

Oppgave 4.5.2 La $A = \{1, 2, 3, 4, 5\}$ og la R være relasjonen som består av tallparene $(1, 3)$, $(3, 2)$, $(3, 5)$ og $(5, 4)$.
Bestem hvilke av de 25 parene i A^2 som er i R^*.

Oppgave 4.5.3 La R være ekvivalenrelasjonen på $\mathbb{Z}$ definert i Eksempel 4.17 d).

a) Vis at om aRb og cRd så vil $(a + c)R(b + d)$.

b) Vi definerer addisjon mellom ekvivalensklasser ved $[a] + [b] = [a + b]$. Bruk a) til å forklare hvorfor dette er en lovlig definisjon.

c) Forklar hvorfor vi kan gi en tilsvarende definisjon av produktet av to ekvivalensklasser.

d) Vis at $[4] \cdot [11] = [1]$.

Ved å bruke at 17 er et primtall er det mulig å vise at hvis $0 < a < 17$ så finnes det et tall b slik at $[a] \cdot [b] = [1]$. Ta utfordringen og prøv å vis dette. Stikkord: Euklids algoritme. 1 er største felles faktor til a og 17. Regn bakover.

Oppgave 4.5.4 Vi definerer en relasjon R på $\mathbb{R}^2$ ved $(x, y)R(u, v)$ hvis $x + y = u + v$.
Vis at R er en ekvivalensrelasjon.
Beskriv ekvivalensklassene til R.
Finn en naturlig funksjon f som avbilder $\mathbb{R}$ injektivt og surjektivt på mengden av ekvivalensklasser.

Oppgave 4.5.5 [u] La R være en binær relasjon på en mengde A. Vis at

$$(R \cup R^{-1})^*$$

er en ekvivalensrelasjon og at den er den minste ekvivalensrelasjonen som utvider R.

4.6 Utfordringer

En modell for programmering.

Vi skal se på et veldig enkelt programmeringsspråk for regning med ikke-negative hele tall.
I en viss forstand snakker vi om programmering for regning med tallerkenstabler, hvor vi kan legge til en tallerken i en stabel, fjerne en tallerken fra en ikke-tom stabel og bestemme oss for hva vi vil gjøre avhengig av om en stabel er tom eller ikke.

Vi vil ha et programmeringsspråk med variable x_1, x_2, ... og uttrykk for alle tall $a \in \mathbb{N}_0$.
Et *program* skal være en instruksjon for hvordan vi kan endre verdiene på variablene. Grunnprogrammene vil være

- $x := a$ hvor $a \in \mathbb{N}_0$
- $x := x + 1$ hvor vi øker verdien av variabelen x med 1.
- $x := x \dot{-} 1$ hvor vi trekker fra 1 hvis mulig, men ellers lar verdien fortsatt være 0.
- Hvis P og Q er programmer lar vi $P; Q$ være et program. Ideen er at vi først kjører P og så kjører Q.

- Hvis P og Q er programmer og x er en variabel, er

  $$if\ x > 0\ then\ P\ else\ Q\ fi$$

  et program.
  Intuisjonen her er at dersom verdien på variabelen x er positiv, så skal vi bruke programbiten P, ellers skal vi bruke programbiten Q.

- Hvis x er en variabel og P er et program, er

  $$while\ x > 0\ do\ P\ od$$

  et program.
  Intuisjonen er at vi skal gjenta P, som vil endre verdiene på de variable, inntil variabelen x får verdien 0, og så er vi ferdige.

Det er to måter vi kan gi en presis matematisk mening til hva et slikt program 'gjør'. La oss for enkelthets skyld anta at vi bare har tre varible. En *valuasjon* vil da være et sett verdier $v(x_1)$, $v(x_2)$ og $v(x_3)$ på de tre variablene. En *situasjon* vil bestå av et par (v, P) hvor v er en valuasjon og P er et program. Vi lar $\emptyset$ betegne det tomme programmet, som vi tillater oss å regne som et program. En situasjon på formen $(v, \emptyset)$ kaller vi da et *svar*, ettersom det er den type situasjon vi skal stå igjen med når programmet er ferdig kjørt.
Vi definerer relasjonen $\vdash$ mellom situasjoner som følger:

- $(v, x_i := a; P) \vdash (v', P)$ hvor $v'(x_i) = a$ og $v'(x_j) = v(x_j)$ for $j \neq i$.
- $(v, x_i := x_i{+}1; P) \vdash (v', P)$ hvor v' kommer fra v ved å la $v'(x_i) = v(x_i){+}1$, men ellers ikke gjøre noen endringer.
- $(v, x_i := x_i \dot{-} 1; P) \vdash (v', P)$ hvor v' kommer fra v ved å redusere $v'(x_i)$ med 1 om mulig, men ellers ikke gjøre noen endringer.
- $(v,\ if\ x_i > 0\ do\ \mathrm{P}\ else\ Q\ fi\ ; R) \vdash (v, P; R)$ om $v(x_i) > 0$
- $(v,\ if\ x_i > 0\ do\ \mathrm{P}\ else\ Q\ fi\ ; R) \vdash (v, Q; R)$ om $v(x_i) = 0$
- $(v,\ while\ x_i > 0\ do\ P\ od\ ; Q) \vdash (v, Q)$ om $v(x_i) = 0$.
- $(v,\ while\ x_i > 0\ do\ P\ od\ ; Q) \vdash (v, P;\ while\ x_i >\ do\ P\ od\ ; Q)$ ellers.

Hvis vi i tillegg setter $\emptyset; P = P$, så får vi her regler for hvordan vi fra en valuasjon og et program får en ny valuasjon og et restprogram etter ett regnetrinn.

Dette kalles den *operasjonelle tolkningen* av programmeringsspråket, den forteller oss hvordan 'regningen' foregår skritt for skritt. Hvis vi bruker den refleksive og trasitive tillukningen $\vdash^*$ får vi en presis definisjon av hva vi mener med at vi vil komme fra en situasjon (u, P) til en annen situasjon (v, Q) ved å regne ingen, ett eller flere skritt.

Dette kan igjen brukes til å definere den *denotasjonelle tolkningen*. Hvis u og v er valuasjoner sier vi at

$$v\langle P\rangle u$$

hvis $(v, P) \vdash^* (u, \emptyset)$.
På denne måten bruker vi relasjoner og begreper knyttet til relasjoner til å gi en matematisk definisjon av hvilken funksjon et program definerer.

Bemerkning 4.1 Det er svært bevisst at dette avsnittet står under overskriften *Utfordringer*. Det er ingen grunn til fortvilelse hvis man synes at dette var vanskelig eller sågar umulig å forstå. En lærebokfremstilling av dette stoffet ville nok krevd en 4-5 sider med forklarende tekst. Hensikten med å ta med dette eksemplet er å illustrere at den typen matematikk vi tar opp i EVU 6 faktisk blir brukt for å legge det teoretiske grunnlaget for informasjonsteknologien.
Hvis man arbeider med mer kompliserte programmeringsspråk, så vil en matematisk behandling av hva disse programmene virkelig betyr innebære en operasjonell og en denotasjonell tolkning som minner mye om det vi har gjort her.

Vi sier at en funksjon $f : \mathbb{N}_0 \to \mathbb{N}_0$ er *beregnbar* hvis det finnes et program P slik at vi for alle a har at $v_a\langle P\rangle v_{f(a)}$ hvor $v_b(x_1) = b$ og $v_b(x_j) = 0$ når $i \neq j$.
Dette virker som en beskjeden definisjon av når en funksjon er beregnbar, men faktum er at ingen har greid å komme opp med en funksjon som er beregnbar i en eller annen form, men som ikke faller inn under vår definisjon.

Kvotienter

En viktig bruk av ekvivalensrelasjoner og ekvivalensklasser er at hvis vi tar utgangspunkt i en matematisk modell med en ekvivalensrelasjon, så vil vi ofte få en nedarvet struktur på mengden av ekvivalensklasser. I oppgave 4.5.3 så vi et eksempel på dette. Der definerte vi addisjon og multiplikasjon mellom ekvivalensklasser av hele tall. Noe av poenget med den konstruksjonen er at vi får en rikere matematisk modell, ved at vi også kan utføre divisjon mellom visse ekvivalensklasser.

Her skal vi se hvordan vi kan konstruere en partiell ordning fra en binær relasjon som er transitiv og refleksiv:
La R være en binær relasjon på en mengde A slik at R er refleksiv og transitiv.
La $\hat{R}$ være definert ved

$$a\hat{R}b \Leftrightarrow aRb \wedge bRa.$$

Vi skal se at $\hat{R}$ er en ekvivalensrelasjon. Det er tre egenskaper vi må vise:

1. $\hat{R}$ er refleksiv:
   Dette følger direkte ved at R er refleksiv siden vi for alle $a \in A$ har at $aRa \wedge aRa$.

2. $\hat{R}$ er symmetrisk:
   Hvis $a\hat{R}b$ har vi $aRb \wedge bRa$, så vi har at $bRa \wedge aRb$, hvilket betyr at $b\hat{R}a$.

3. $\hat{R}$ er transitiv:
   Anta $a\hat{R}b \wedge b\hat{R}c$. Da har vi på den ene siden at $aRb \wedge bRc$, så aRc siden R er transitiv.
   På den andre siden har vi at $cRb \wedge bRa$, så cRa.
   Til sammen gir dette oss at $a\hat{R}c$.

La $B = A/\hat{R}$ være mengden ac $\hat{R}$-ekvivalensklasser $[a]$. Vi definerer $S = R/\hat{R}$ på B ved

$$[a]S[b] \Leftrightarrow aRb.$$

Vi må strengt tatt vise at hvis $[a]S[b]$, $[a] = [c]$ og $[b] = [d]$, så vil $[c]S[d]$.
Dette er en konsekvens av transitiviteten til R, og overlates leseren.
S er antisymmetrisk, for hvis $[a]S[b]$ og $[b]S[a]$, vil aRb og bRa, så $a\hat{R}b$, dvs $[a] = [b]$.
Det at S er transitiv følger fra definisjonen og fra at R er transitiv, så S er en partiell ordning på B.

Det vi har gjort er å slå samen par av objekter i A hvis de utgjør et moteksempel til antisymmetri .
La oss knytte denne konstruksjonen til studiet av programmer, og la oss bruke det eksemplet vi så på i forrige avsnitt. Et problem med å forstå det eksemplet er at det ikke er hver gang at et gitt program med en gitt valuasjon som utgangspunkt gir oss et svar, noen av disse programmene vil 'regne' uendelig lenge uten å komme til noe svar.Vi kan derfor ikke bruke mengden av funksjoner fra $\mathbb{N}_0$ til $\mathbb{N}_0$ som tolkningsområde for slike programmer.

Definisjon 4.15 La P og Q være programmer. Vi sier at $P \preceq Q$ hvis vi for alle valuasjoner u og v har at

$$u\langle P\rangle v \Rightarrow u\langle Q\rangle v,$$

det vil si at hver gang P regner ut v fra u så vil Q gjøre det samme.

Hvis vi lar $\equiv \; = \; \hat{\preceq}$ blir $\equiv$ en ekvivalensrelasjon på mengden av programmer, og ekvivalensklassene blir ordnet va $\preceq \; / \equiv$ slik at det svarer til at et program er mindre nyttig enn et annet.

Dette er bare et forsøk på å gi et eksempel på hvordan elementær mengdelære og læren om relasjoner brukes til å lage matematiske modeller med relevans for informatikk-faget. Skulle vi gjort dette på en seriøs måte ville det krevd adskillig flere detaljer og også større generalitet.

4.7 Blandede oppgaver

Oppgave 4.7.1 La $A = \{1, 2, 3\}$ og $B = \{1, 2, 3, 4\}$. La R, S og T være de tre relasjonene fra A til B:

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

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

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

a) Bestem hvilke av disse relasjonene som er funksjoner.

b) Finn R^{-1}, S^{-1} og T^{-1} og bestem hvilke av disse relasjonene som er funksjoner.

c) Finnes det en relasjon U fra A til B slik at både U og U^{-1} er funksjoner? Begrunn svaret.

Oppgave 4.7.2 La A være en mengde, R en partiell ordning på A. La B være mengden av alle endelige sekvenser $a_1, \ldots, a_n$ fra A.
Vi definerer en relasjon S på B som følger:
$(a_1, \ldots, a_n)S(b_1, \ldots, b_m)$ hvis en av to holder:

1. $n \leq m$ og $a_i = b_i$ for alle $i \leq n$.
2. Det finnes en $i \leq min\{n, m\}$ slik at $a_i R b_i$, slik at $a_i \neq b_i$ og slik at $a_j = b_j$ når $j < i$.

a) Vis at S er en partiell ordning.

b) Vis at hvis R er en total ordning, så er også S total.

c) Ordningen S kalles den *leksikografiske ordningen*. Diskuter hvorfor dette er en naturlig betegnelse, ut fra hvordan man ordner artikler i et leksikon, navn i en telefonkatalog m.m.

Oppgave 4.7.3 I avsnitt 3.3 så vi på digitale kretser med forsinkelse. En slik krets kan ta i mot en eller flere datastrømmer i form av strømmer av sannhetsverdier, og den kan sende ut en eller flere datastrømmer. I den forstand kan en digital krets med forsinkelse tolkes som en funksjon som avbilder n datastrømmer på m datastrømmer.
Hvis vi tolker en slik krets som en funksjon uten å ta hensyn til hvordan vi kommer fra inngangs-strømmene til utgangs-strømmene, snakker informatikerne om den *denotasjonelle tolkningen*. Hvis vi derimot finner hvordan algoritmen som ligger under utføres trinn for trinn, snakker vi om den *operasjonelle tolkningen*. Ta utgangspunkt i de eksemplene vi hadde i avsnitt 3.3 med tilhørende oppgaver, og formuler en algoritme som beregner den funksjonen som de digitale kretsene definerer.