MAT1140 – Forelesningsnotater

Høsten 2026

Innhold

1 Logikk og bevis **5**

1.1 Utsagnslogikk 5

1.2 Bevis i utsagnslogikk 7

1.3 Predikatlogikk 11

1.4 Bevis i predikatlogikk 14

2 Mengder **17**

2.1 De første aksiomene 17

2.2 Snitt og union 21

2.3 Potensmengder og kartesiske produkt 24

3 Funksjoner **27**

3.1 Definisjonen av en funksjon 27

3.2 Komposisjon 29

3.3 Familier av mengder 32

4 Naturlige tall **35**

4.1 Uendelighetsaksiomet 35

4.2 Rekursjon 38

4.3 Aritmetikk og litt algebra 41

5 Relasjoner **47**

5.1 Grunnleggende begreper 47

5.2 Ordensrelasjoner 48

5.3 Ekvivalensrelasjoner 52

5.4 Ringer og heltall 57

5.5 Kropper og rasjonale tall 61

5.6 Totalt ordnede ringer 62

6 Tallteori **67**

6.1 Delelighet 67

6.2 Primtall 71

6.3 Kongruensregning 73

7 Reelle tall **77**

7.1 Dedekind-kompletthet 77

Kapittel 1

Logikk og bevis

Målet vårt i dette kapitlet er å vise at alle matematiske utsagn i prinsippet kan kodes med formelle uttrykk som involverer symboler som

$$\wedge,\ \vee,\ \neg,\ \Rightarrow,\ \forall,\ \exists,\ \ldots$$

Dette hjelper oss blant annet med å forstå hvilke bevisteknikker som kan brukes i ulike tilfeller.

For eksempel vil definisjonen av kontinuitet av en funksjon $f\colon \mathbb{R} \to \mathbb{R}$ se slik ut:

$$\forall x \in \mathbb{R}\ \forall \varepsilon > 0\ \exists \delta > 0\ \forall y \in \mathbb{R} \quad \big(|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon\big).$$

Som vi ser er dette komplisert! Det kan forklare litt hvorfor kontinuitetsbevis er vanskelige.

Bevis skal i prinsippet kunne gjøres så formelle at de kan sjekkes av en datamaskin; såkalte *formelle bevis*. Men vi går ikke helt dit.

1.1 Utsagnslogikk

Utsagn: En setning som enten er sann eller usann.

Eksempler:

- 3 er et primtall.
- $1 + 2 = 3$.
- 4 er et primtall.
- $1 + 2 = 7$.

Ikke-eksempler:

- $1 + 2$ (kun et uttrykk; det har ingen sannhetsverdi).
- $x + 2 = 3$ (avhenger av x; umulig å si før vi gir x en verdi).
- $1+ = 2$ (ugyldig setning).

Interessant eksempel: "Alle partall større enn eller lik 4 kan skrives som en sum av to primtall."

Dette er helt klart sant eller usant, altså et utsagn, men ingen vet svaret (Goldbachs formodning).

Hva med: "Denne setningen er usann."

Paradoks! Vi må passe på å bygge opp logikken vår slik at slike setninger ikke kan formuleres.

Logiske konnektiver

Vi bruker variabler som $P, Q, R, \ldots$ for å betegne utsagn. Symbolet $\top$ brukes for verdien "sann" og $\bot$ for "usann" (i boka brukes 1 og 0).

Negasjon: Gitt P, har vi utsagnet $\neg P$, uttalt "ikke P", definert ved sannhetstabellen

P	$\neg P$
$\top$	$\bot$
$\bot$	$\top$

Altså er $\neg P$ usann om P er sann, og sann om P er usann.

Gitt P, Q har vi:

Konjunksjon:	$P \wedge Q$	"P og Q"
Disjunksjon:	$P \vee Q$	"P eller Q"
Implikasjon:	$P \Rightarrow Q$	"P impliserer Q"
Ekvivalens:	$P \Leftrightarrow Q$	"P er ekvivalent med Q".

Sannhetstabellen som definerer disse konnektivene er som følger:

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$	$\top$	$\top$

Merk:

- $P \vee Q$ er sann når minst én av P og Q er sann, ulikt i dagligtale når vi sier "enten ... eller ...".
- $P \Rightarrow Q$ kan være forvirrende, men tenk på det som at Q er "minst like sann" som P: $P \Rightarrow Q$ er kun usann når P er sann og Q er usann.

Sammensatte utsagn

Vi kan bruke de logiske konnektivene til å danne sammensatte utsagn, for eksempel

$$\neg Q \Rightarrow \neg P.$$

Fra sannhetstabellen ser vi at dette uttrykket tar de samme verdiene som $P \Rightarrow Q$:

P	Q	$P \Rightarrow Q$	$\neg Q$	$\neg P$	$\neg Q \Rightarrow \neg P$
$\top$	$\top$	$\top$	$\bot$	$\bot$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$

Vi sier at $P \Rightarrow Q$ og $\neg Q \Rightarrow \neg P$ er *logisk ekvivalente*.

Et sammensatt utsagn som alltid er sant kalles en *tautologi*, for eksempel

$$(P \wedge (P \Rightarrow Q)) \Rightarrow Q.$$

Det finnes mange tautologier. Her er noen:

$$\begin{aligned}
(P \Rightarrow Q) &\Leftrightarrow (\neg P \vee Q),\\
(P \Leftrightarrow Q) &\Leftrightarrow (P \Rightarrow Q) \wedge (Q \Rightarrow P),\\
\neg\neg P &\Leftrightarrow P,\\
\neg(P \wedge Q) &\Leftrightarrow \neg P \vee \neg Q,\\
\neg(P \vee Q) &\Leftrightarrow \neg P \wedge \neg Q,\\
P \wedge (Q \wedge R) &\Leftrightarrow (P \wedge Q) \wedge R,\\
P \vee (Q \vee R) &\Leftrightarrow (P \vee Q) \vee R,\\
P \wedge (Q \vee R) &\Leftrightarrow (P \wedge Q) \vee (P \wedge R),\\
P \vee (Q \wedge R) &\Leftrightarrow (P \vee Q) \wedge (P \vee R).
\end{aligned}$$

Se boka side 15–18 for flere.

Eksempel 1.1. Vi kan bruke tautologiene over for å utlede flere. For eksempel kan tautologien

$$((P \wedge Q) \Rightarrow R) \Leftrightarrow (P \Rightarrow (Q \Rightarrow R)).$$

Utledes ved følgende, der vi bruker tre av tautologiene fra lista over (1, 4 og 7):

$$\begin{aligned}
(P \wedge Q) \Rightarrow R &\Leftrightarrow \neg(P \wedge Q) \vee R\\
&\Leftrightarrow (\neg P \vee \neg Q) \vee R\\
&\Leftrightarrow \neg P \vee (\neg Q \vee R)\\
&\Leftrightarrow P \Rightarrow (Q \Rightarrow R).
\end{aligned}$$

1.2 Bevis i utsagnslogikk

Bevis, uformelt sett: overbevisende argument for at et gitt utsagn er sant.

Litt mer formelt: Bevis for et mål P gitt $Q_1, \ldots, Q_n$ er en sekvens av logisk gyldige deduksjoner der vi kan bruke antagelsene våre $Q_1, \ldots, Q_n$ og ender med P.

Vi går gjennom

- bevisteknikker for å bevise diverse logiske utsagn, og viser strukturen et tilsvarende bevis har;
- slutningsregler som sier hvordan vi kan bruke de logiske konnektivene til å trekke diverse slutninger.

Bevis med implikasjon

Følgende dekkes av Prinsipp 1.4.1 i [1].

Bevisteknikk 1. For å bevise $P \Rightarrow Q$, anta P og utled Q.

Det ser typisk slik ut:

Bevis for $P \Rightarrow Q$:
    Anta P.
    (*Bevis for* Q)
Vi konkluderer med $P \Rightarrow Q$.

Merk at der det står (*Bevis for* Q) må vi fylle inn et faktisk bevis for utsagnet Q, der vi fritt kan benytte antagelsen P. Hvordan dette beviset for Q faktisk utarter seg kommer an på konteksten. Likevel vil strukturen ellers i et bevis for en implikasjon typisk se ut som over.

For å øve oss kan vi bruke Bevisteknikk 1 til å vise at $P \Rightarrow (Q \Rightarrow P)$ er en tautologi.

Eksempel 1.2. La P og Q være utsagn. Bevis

$$P \Rightarrow (Q \Rightarrow P).$$

Løsning:

Vi beviser $P \Rightarrow (Q \Rightarrow P)$:
Anta P. (*Bevisteknikk 1. Målet er nå* $Q \Rightarrow P$.)
Anta Q. (*Bevisteknikk 1. Målet er nå* P.)
Vi har allerede P fra en tidligere antagelse.
Vi konkluderer med $Q \Rightarrow P$.
Vi konkluderer med $P \Rightarrow (Q \Rightarrow P)$.

Vi introduserer første slutningsregel. Den regnes som fundamental i logikk og kalles gjerne *modus ponens*.

Slutningsregel 1. Om vi har P og $P \Rightarrow Q$, kan vi konkludere med Q.

Vi beviser nok en tautologi for å øve oss på bruken av bevisteknikkene og slutningsreglene.

Eksempel 1.3. La P og Q være utsagn. Bevis

$$P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q).$$

Løsning:

Vi beviser $P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)$:
Anta P. (*Bevisteknikk 1. Målet er nå* $(P \Rightarrow Q) \Rightarrow Q$)
Anta $P \Rightarrow Q$. (*Bevisteknikk 1 igjen. Målet er nå* Q)
Vi har P og $P \Rightarrow Q$, så vi får Q. (*Slutningsregel 1)*
Vi konkluderer med $(P \Rightarrow Q) \Rightarrow Q$.
Vi konkluderer med $P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)$.

Bevis med konjunksjon

Bevisteknikk 2. For å bevise $P \wedge Q$, bevis P og Q hver for seg.

Det ser typisk slik ut:

Bevis for $P \wedge Q$:
Bevis 1:
Vi viser P:
(*Bevis for* P)
Bevis 2:
Vi viser Q:
(*Bevis for* Q)
Vi konkluderer med $P \wedge Q$.

Slutningsregel 2. Følgende gjelder:

(i) Om vi har gitt P og vi har gitt Q, kan vi konkludere med $P \wedge Q$.
(ii) Om vi har gitt $P \wedge Q$, kan vi konkludere med P. Om vi har gitt $P \wedge Q$, kan vi også konkludere med Q.

Følgende eksempel illustrerer bruk av Bevisteknikk 2 og Slutningsregel 2.

Eksempel 1.4. La P, Q og R være utsagn. Anta at $P \Rightarrow (Q \wedge R)$ holder. Vis at $(P \Rightarrow Q) \wedge (P \Rightarrow R)$ holder.

Løsning:

Anta at $P \Rightarrow (Q \wedge R)$ holder.
Vi beviser $(P \Rightarrow Q) \wedge (P \Rightarrow R)$:
Bevis 1: (*Bevisteknikk 2*)

Vi viser først $P \Rightarrow Q$:

Anta P. (*Bevisteknikk 1. Målet er nå Q*)
Vi har P og $P \Rightarrow (Q \wedge R)$, som gir $Q \wedge R$. (*Slutningsregel 1*)
Spesielt har vi Q. (*Slutningsregel 2*)

Vi konkluderer med $P \Rightarrow Q$.

Bevis 2:

Deretter viser vi $P \Rightarrow R$:

Anta P. (*Bevisteknikk 1. Målet er nå R*)
Vi har P og $P \Rightarrow (Q \wedge R)$, som gir $Q \wedge R$. (*Slutningsregel 1*)
Spesielt har vi R. (*Slutningsregel 2*)

Vi konkluderer med $P \Rightarrow R$.

Vi konkluderer med $(P \Rightarrow Q) \wedge (P \Rightarrow R)$.

Bevis med disjunksjon

Bevisteknikk 3. Om du har $P \vee Q$ og skal bevise R, del opp i to tilfeller: ett der du har P og skal bevise R, og ett der du har Q og skal bevise R.

Det ser typisk slik ut:

Vi vet at $P \vee Q$ holder.
Bevis for R:
Tilfelle 1:

Anta P.
(*Bevis for R*)

Tilfelle 2:

Anta Q.
(*Bevis for R)*

I hvert tilfelle stemmer R, så vi konkluderer med R.

Slutningsregel 3. Om du har P eller har Q, kan du slutte $P \vee Q$.

Eksempel 1.5. La P, Q og R være påstander slik at $P \wedge (Q \vee R)$. Bevis at $(P \wedge Q) \vee (P \wedge R)$.

Løsning:

Vi vet at $P \wedge (Q \vee R)$.
Vi beviser $(P \wedge Q) \vee (P \wedge R)$
Fra $P \wedge (Q \vee R)$ slutter vi P. (*Slutningsregel 2*)
Fra $P \wedge (Q \vee R)$ slutter vi $Q \vee R$. (*Slutningsregel 2*)
Tilfelle 1: (*Bevisteknikk 3 på $Q \vee R$*)
  Anta Q.
  Siden vi har P og Q, slutter vi $P \wedge Q$. (*Slutningsregel 2*)
  Spesielt har vi da $(P \wedge Q) \vee (P \wedge R)$. (*Slutningsregel 3*)
Tilfelle 2:
  Anta R.
  Siden vi har P og R, slutter vi $P \wedge R$. (*Slutningsregel 2*)
  Spesielt har vi da $(P \wedge Q) \vee (P \wedge R)$. (*Slutningsregel 3*)
I hvert tilfelle stemmer $(P \wedge Q) \vee (P \wedge R)$, så vi konkluderer med $(P \wedge Q) \vee (P \wedge R)$.

Bevis med negasjon

Den vanligste måten å vise $\neg P$ på er å anta P og utlede en usannhet, altså $\bot$. Dette er typisk noe som åpenbart er usant, ofte $Q \wedge \neg Q$ for et eller annet utsagn Q. En slik usannhet kalles ofte en selvmotsigelse, eller noe "absurd". Denne bevisteknikken kan begrunnes med at $\neg P$ og $P \Rightarrow \bot$ er logisk ekvivalente. Bevisteknikk 4 under kan dermed ses på som et spesialtilfelle av Bevisteknikk 1.

Bevisteknikk 4. For å bevise $\neg P$, anta P og utled en usannhet.

Det ser typisk slik ut:

Bevis for $\neg P$:
  Anta P.
  (*Bevis for $\bot$*)
Vi konkluderer med $\neg P$.

Om vi bruker at P og $\neg(\neg P)$ er logisk ekvivalente, ser vi at vi kan også bruke teknikken over på følgende måte: For å vise P, anta $\neg P$ og utled en usannhet. Dette kalles ofte for *selvmotsigelsesbevis*. Vi kan gjerne kalle Bevisteknikk 4 for selvmotsigelsesbevis også, men logikere liker å skille de to.

Eksempel 1.6. Anta at $\neg P \wedge \neg Q$ holder. Bevis at $\neg(P \vee Q)$.

Løsning:

Vi antar $\neg P \wedge \neg Q$.
Vi skal nå vise $\neg(P \vee Q)$.
  For å oppnå en selvmotsigelse, anta $P \vee Q$. (*Bevisteknikk 4. Målet er nå $\bot$*)
    Tilfelle 1: P holder. (*Bevisteknikk 3*)
    Vi har $\neg P \wedge \neg Q$, som spesielt gir $\neg P$. (*Slutningsregel 2*)
    Fra P og $\neg P$ konkluderer vi med $P \wedge \neg P$, som er en selvmotsigelse. (*Slutningsregel 2*)
    Tilfelle 2: Q holder.
    Vi har $\neg P \wedge \neg Q$, som spesielt gir $\neg Q$. (*Slutningsregel 2*)
    Fra Q og $\neg Q$ konkluderer vi med $Q \wedge \neg Q$, som er en selvmotsigelse.
  I hvert tilfelle oppnådde vi en selvmotsigelse.
Vi konkluderer med $\neg(P \vee Q)$.

Vi har sett tidligere at $P \Rightarrow Q$ og $\neg Q \Rightarrow \neg P$ er logisk ekvivalente. For å bevise implikasjonen $P \Rightarrow Q$, kan vi med andre ord bevise $\neg Q \Rightarrow \neg P$ i stedet. Et slikt bevis kalles et *kontrapositivt* bevis.

Bevisteknikk 5. For å bevise $P \Rightarrow Q$, anta $\neg Q$ og utled $\neg P$.

I seksjonen for bevis med disjunksjon ga vi ikke en konkret teknikk for å bevise $P \vee Q$. Vi kan nå formulere en slik teknikk, som er basert på tautologien $(P \vee Q) \Leftrightarrow (\neg P \Rightarrow Q)$. Denne teknikken er ikke alltid naturlig å bruke, man må se litt an situasjonen.

Bevisteknikk 6. For å bevise $P \vee Q$, anta $\neg P$ og utled Q.

Eksempel 1.7. Anta at $\neg(P \wedge Q)$ holder. Bevis at $\neg P \vee \neg Q$ holder.

Vi antar $\neg(P \wedge Q)$.
Vi beviser $\neg P \vee \neg Q$:

Anta $\neg(\neg P)$. (*Bevisteknikk 6. Målet er nå* $\neg Q$)
Vi har $\neg(\neg P)$ og $\neg(\neg P) \Rightarrow P$, så vi får P. (*Slutningsregel 1*)

Anta Q. (*Bevisteknikk 4. Målet er nå* $\perp$)
Vi har P og Q, så vi kan slutte $P \wedge Q$. (*Slutningsregel 2*)
Fra $P \wedge Q$ og $\neg(P \wedge Q)$ slutter vi $(P \wedge Q) \wedge \neg(P \wedge Q)$, en selvmotsigelse. (*Sl.regel 2*)

Vi konkluderer med $\neg Q$.

Vi konkluderer med $\neg P \vee \neg Q$.

Bevis med ekvivalens

Bevis for ekvivalens $P \Leftrightarrow Q$ er rett fram. Vi bruker simpelthen at $P \Leftrightarrow Q$ er logisk ekvivalent med $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. Følgende bevisteknikk kan dermed utledes fra Bevisteknikk 2:

Bevisteknikk 7. For å bevise $P \Leftrightarrow Q$, bevis $P \Rightarrow Q$ og $Q \Rightarrow P$ hver for seg.

Det ser typisk slik ut:

Bevis for $P \Leftrightarrow Q$:
Bevis 1:

Vi viser $P \Rightarrow Q$:
(*Bevis for* $P \Rightarrow Q$)

Bevis 2:

Vi viser $Q \Rightarrow P$:
(*Bevis for* $Q \Rightarrow P$)

Vi konkluderer med $P \Leftrightarrow Q$.

Merknad 1.8. Noen av bevisteknikkene og slutningsreglene kan kanskje oppleves litt pedantiske eller slaviske. Poenget her har vært å vise at et bevis kan reduseres til noen minste byggestener. Målet er at bruk av disse teknikkene skal gå mye mer på automatikk etter hvert. Likevel tror jeg det kan være instruktivt å se hvordan det ville sett ut dersom man begrunner hvert minste lille steg, slik vi har gjort her.

1.3 Predikatlogikk

Vi skal nå ta steget videre fra kun utsagn, og begynne å snakke om *objekter*. Vi bruker variabler som x, y, z, osv., til å betegne dem. De skal tilhøre et eller annet *univers* U. Hva dette universet

er, kommer an på konteksten (men fra kapittel 2 av skal vi konsentrere oss om universet av mengder).

La oss se for oss at vi jobber med heltall som univers, altså $0, \pm 1, \pm 2, \pm 3, \ldots$. Om vi lar x være en variabel, kan vi danne uttrykket

$$x + 1 = 2.$$

Dette er ikke et utsagn, da det ikke har en sannhetsverdi før vi har satt inn en konkret verdi for x. Vi kaller slike uttrykk for *predikater* og bruker symboler som $P(x)$, $Q(x)$, osv. for dem (i boka kalles de egenskaper). Om vi lar $P(x)$ stå for predikatet $x + 1 = 2$, så vil $P(1)$ betegne utsagnet $1 + 1 = 2$ (som er sant), mens $P(2)$ vil betegne utsagnet $2 + 1 = 2$ (som er usant).

Vi kan også ha predikater av flere variable. For eksempel kunne vi betraktet

$$R(x, y) \ : \quad x^2 + y \geq 0.$$

Dette er et predikat av to variable. Her får vi altså et utsagn først nå vi setter inn konkrete verdier for både x og y. For eksempel er $R(-2, -1)$ sant mens $R(1, -4)$ er usant.

Mer generelt kan vi ha predikater $P(x_1, \ldots, x_n)$ av n variable.

Kvantorer

Dersom $P(x)$ er et predikat, så kan vi danne to viktige utsagn:

- $\forall x P(x)$ — "for alle x gjelder $P(x)$",
- $\exists x P(x)$ — "det fins en x slik at $P(x)$ gjelder".

$\forall$ kalles den universelle kvantoren, mens $\exists$ kalles den eksistensielle kvantoren.

For predikatet $P(x) : \ x + 1 = 2$ betraktet over, vil utsagnet $\forall x P(x)$ være *usant*: Det er ikke slik at $P(x)$ stemmer uansett x, for eksempel er $P(2)$ usant. Derimot er utsagnet $\exists x P(x)$ *sant*, fordi det fins en x, nemlig $x = 1$, som gjør at $P(x)$ stemmer.

Kvantorene interagerer med negasjon på følgende grunnleggende måte:

$$\begin{aligned} \neg(\forall x P(x)) &\quad \Leftrightarrow \quad \exists x(\neg P(x)), \\ \neg(\exists x P(x)) &\quad \Leftrightarrow \quad \forall x(\neg P(x)). \end{aligned}$$

Det blir mer spennende når vi bruker kvantorer på predikater av flere variable. Gitt et predikat $P(x, y)$ av to variable x og y vil for eksempel $\forall x P(x, y)$ være et *nytt* predikat av én variabel y. Først når vi bruker to kvantorer, for eksempel $\exists y \forall x P(x, y)$, får vi et utsagn.

Eksempel 1.9. Vi betrakter predikatet

$$R(x, y) \ : \quad x^2 + y \geq 0$$

hvor universet er alle heltall. Ved å bruke universell og eksistensiell kvantor kan vi nå lage 8 apriori ulike utsagn:

1. $\forall x \, \forall y \, R(x, y)$
2. $\forall y \, \forall x \, R(x, y)$
3. $\forall x \, \exists y \, R(x, y)$
4. $\forall y \, \exists x \, R(x, y)$
5. $\exists x \, \forall y \, R(x, y)$
6. $\exists y \, \forall x \, R(x, y)$
7. $\exists x \, \exists y \, R(x, y)$
8. $\exists y \, \exists x \, R(x, y)$

Vi merker oss at 1 og 2 generelt er ekvivalente, og at 7 og 8 er ekvivalente: det spiller ingen rolle hvilken rolle kvantorer av *samme sort* står i. Utover dette er resten av utsagnene generelt ikke ekvivalente.

Utsagn 1 og 2 her påstår at $x^2 + y \geq 0$ for alle verdier av x og y. Dette er usant, for vi kan jo plugge inn for eksempel $x = 0$ og $y = -1$.

Utsagn 3 sier at det for enhver x fins en y slik at $x^2 + y \geq 0$. Dette stemmer, da vi vet at $x^2 \geq 0$ alltid, så vi gitt x bare velge $y = 0$ og følgelig få $x^2 + y = x^2 \geq 0$.

Utsagn 4 sier at det for enhver y fins en x slik at $x^2 + y \geq 0$. Dette stemmer, men her må x avhenge av y. Vi kan for eksempel gitt y velge $x = y$. Vi får da at $x^2 + y = y(y + 1)$. Merk at dette alltid er ikke-negativt for all heltall y: den eneste måten det kunne blitt negativt på er om y og $y + 1$ har motsatt fortegn, men det går ikke.

Utsagn 5 sier at det finnes en x slik at uansett y så blir $x^2 + y \geq 0$. Dette går ikke: Uansett hva x måtte være, så kan vi for eksempel velge $y = -x^2 - 1$, og få $x^2 + y = -1 < 0$.

Utsagn 6 sier at det finnes en y slik at uansett hva x måtte være, så bli $x^2 + y \geq 0$. Dette finnes! Ta nemlig $y = 0$. Da er $x^2 + y = x^2 \geq 0$. Dette så vi egentlig allerede i utsagn 3: Merk at $\exists x \forall y R(x, y)$ generelt alltid impliserer $\forall y \exists x R(x, y)$!

Videre stemmer utsagn 7 og 8, for her ber vi bare om det finnes et par av verdier x og y som gjør at $x^2 + y \geq 0$. Da kan vi for eksempel velge $x = y = 0$.

Likhet

Uansett hvilket univers vi jobber med så antar vi at det finnes et begrep om *likhet*, altså at for gitte objekter x og x kan vi danne utsagnet $x = y$ (som da er sant eller usant). Vi tar for gitt at likhet tilfredsstiller følgende egenskaper:

(i) $\forall x(x = x)$.
(ii) $\forall x \, \forall y(x = y \Rightarrow y = x)$.
(iii) $\forall x \, \forall y \, \forall z\big((x = y) \wedge (y = z) \Rightarrow x = z\big)$.

I tillegg, dersom $P(x)$ er et predikat, så har vi at

- $\forall x \, \forall y \, \Big((x = y) \quad \Rightarrow \quad \big(P(x) \Rightarrow P(y)\big)\Big)$.

Mer uformelt, dersom x og y er like, så kan vi fritt erstatte forekomster av x med forekomster av y i alle mulige uttrykk.

Unik eksistens

Kvantoren $\exists$ brukes for å uttrykke at noe eksisterer med en gitt egenskap. Vi innfører også $\exists!$, som betegner at det eksisterer et unikt objekt med en gitt egenskap. Vi kan definere bruk av kvantoren som følger: gitt et predikat $P(x)$, så definerer vi

$$\exists! x P(x) \quad \Leftrightarrow \quad \big(\exists x P(x)\big) \ \wedge \ \forall x \, \forall y \, \Big(P(x) \wedge P(y) \implies x = y\Big).$$

1.4 Bevis i predikatlogikk

Vi har følgende grunnleggende måte å bevise et utsagn på formen $\forall x P(x)$.

Bevis med universell kvantor

Bevisteknikk 8. For å bevise $\forall x P(x)$, la a være vilkårlig og utled $P(a)$.

Dette ser typisk slik ut:

Bevis for $\forall x P(x)$:
La a være vilkårlig.
(*Bevis for* $P(a)$).
Vi konkluderer med $\forall x P(x)$.

Slutningsregel 4. Om du har gitt et objekt a og vet at $\forall x P(x)$, kan du slutte $P(a)$.

Igjen illustrerer vi bruk av teknikkene ved å bevise følgende tautologi:

Eksempel 1.10. La $P(x)$ og $Q(x)$ være predikater. Bevis følgende:

$$\forall x(P(x) \wedge Q(x)) \quad \Rightarrow \quad (\forall x P(x)) \wedge (\forall x Q(x)).$$

Løsning:

Vi beviser $\forall x(P(x) \wedge Q(x)) \quad \Rightarrow \quad (\forall x P(x)) \wedge (\forall x Q(x))$:
Anta $\forall x(P(x) \wedge Q(x))$. (*Bevisteknikk 1. Målet er nå* $(\forall x P(x)) \wedge (\forall x Q(x))$)
Bevis 1: (*Bevisteknikk 2*)
Vi skal bevise $\forall x P(x)$.
La a være vilkårlig. (*Bevisteknikk 8. Målet er nå* $P(a)$)
Vi har at $P(a) \wedge Q(a)$. *(Slutningsregel 4)*
Spesielt har vi $P(a)$. (*Slutningsregel 2)*
Vi konkluderer med $\forall x P(x)$.
Bevis 2:
Vi beviser nå $\forall x Q(x)$.
La a være vilkårlig. (*Bevisteknikk 8. Målet er nå* $Q(a)$)
Vi har at $P(a) \wedge Q(a)$. *(Slutningsregel 4)*
Spesielt har vi $Q(a)$. (*Slutningsregel 2)*
Vi konkluderer med $\forall x Q(x)$.
Vi konkluderer med $(\forall x P(x)) \wedge (\forall x Q(x))$.
Vi konkluderer med $\forall x(P(x) \wedge Q(x)) \quad \Rightarrow \quad (\forall x P(x)) \wedge (\forall x Q(x))$.

Bevis med eksistensiell kvantor

Slutningsregel 5. Følgende gjelder:

(i) Om du har gitt $\exists x P(x)$, kan du innføre et objekt a med egenskapen $P(a)$.
(ii) Om du har et objekt a med egenskapen $P(a)$, kan du konkludere med at $\exists x P(x)$.

Eksempel 1.11. La $P(x)$ være et predikat og la Q være et utsagn. Bevis

$$\Big(\exists x\big(P(x) \Rightarrow Q\big)\Big) \Rightarrow \Big(\big(\forall x P(x)\big) \Rightarrow Q\Big).$$

Løsning:

Vi skal bevise $\Big(\exists x\big(P(x) \Rightarrow Q\big)\Big) \Rightarrow \Big(\big(\forall x P(x)\big) \Rightarrow Q\Big)$.

Anta $\exists x(P(x) \Rightarrow Q)$. (*Bevisteknikk 1. Målet er nå* $(\forall x P(x)) \Rightarrow Q$.)

Anta $\forall x P(x)$. (*Bevisteknikk 1. Målet er nå* Q.)

Fra $\exists x(P(x) \Rightarrow Q)$ innfører vi a slik at $P(a) \Rightarrow Q$. (*Slutningsregel 5*)

Fra $\forall x P(x)$ deduserer vi $P(a)$. (*Slutningsregel 4*)

Fra $P(a)$ og $P(a) \Rightarrow Q$ konkluderer vi Q. (*Slutningsregel 1*)

Vi konkluderer med $(\forall x P(x)) \Rightarrow Q$.

Vi konkluderer med $\Big(\exists x\big(P(x) \Rightarrow Q\big)\Big) \Rightarrow \Big(\big(\forall x P(x)\big) \Rightarrow Q\Big)$.

Den siste bevisteknikken gir en måte å bevise eksistens på ved å anta det motsatte og prøve å oppnå en selvmotsigelse. Dette er ikke en teknikk som alltid er naturlig å bruke, men den kan være veldig kraftig i riktig situasjon.

Bevisteknikk 9. For å bevise $\exists x P(x)$, anta $\forall x \neg P(x)$ og oppnå en selvmotsigelse.

Kapittel 2

Mengder

I første kapittel bygget vi først opp utsagnslogikk, og deretter predikatlogikk hvor vi betraktet objekter som tilhørte et eller annet univers. Dette universet kunne for eksempel være alle heltall. I dette kapittelet skal vi bygge opp et helt spesielt univers, nemlig universet av såkalte mengder. Vi skal sette opp utgangspunktet for den vanlige matematikken inne i dette universet.

Vi antar altså at vi har et univers hvor vi skal bruke bokstaver som x, y, z, men også A, B og C, for å betegne objektene. Disse objektene kaller vi altså for *mengder*. I tillegg antar vi et helt grunnleggende predikat av to variable: $x \in y$. Dette er da et utsagn for hvert konkrete par av mengder x og y. Vi uttaler $x \in y$ som at x *er et element av* y, eller at y *inneholder* x. Vi innfører også forkortelsen

$$x \notin y \quad \iff \quad \neg(x \in y).$$

Merk at *alle* matematiske objekter kommer til å være mengder når vi danner et fundament på denne måten: tall, tupler, funksjoner, relasjoner, også videre. Vi kommer imidlertid ikke til å tenke på alle disse objektene som mengder etter at vi har enkodet dem som mengder og utledet deres grunnleggende egenskaper.

Vi skal nå gradvis begynne å innføre aksiomer for hvordan mengder og element-predikatet oppfører seg.

2.1 De første aksiomene

Likhet og inklusjon

Siden vi antar at alle universer av objekter er utstyrt med et begrep om likhet, har vi også et slikt begrep for mengder. Gitt to mengder A og B kan vi altså spørre om $A = B$. En grunnleggende egenskap vi antar at likhet har, er at to like mengder fritt kan byttes ut med hverandre i diverse utsagn. Dette innebærer spesielt at vi har

$$\forall A \forall B \Big(A = B \quad \Rightarrow \quad \forall x (x \in A \Leftrightarrow x \in B) \Big).$$

Sagt med ord: dersom to mengder er like, inneholder de nøyaktig de samme elementene.

Det første aksiomet vårt sier det motsatte: altså at dersom to mengder inneholder nøyaktig de samme elementene, så er de like.

Aksiom 1. Vi har at

$$\forall A \forall B \Big(\forall x (x \in A \Leftrightarrow x \in B) \quad \Rightarrow \quad A = B \Big).$$

Vi innfører nå et av grunnbegrepene for mengder.

Definisjon 2.1. La A og B være mengder. Vi sier at A er en *delmengde* av B og skriver $A \subseteq B$ dersom følgende gjelder:

$$\forall x\big(x \in A \Rightarrow x \in B\big).$$

Lemma 2.2. *Vi har at*

$$\forall A \forall B \forall x \Big((x \in A \ \wedge \ A \subseteq B) \implies x \in B\Big).$$

Bevis. Vi skriver beviset systematisk som vi gjorde i Kapittel 1 og referer eksplisitt til bevisteknikker og slutningsregler.

Vi skal vise at $\forall A \forall B \forall x \Big((x \in A \ \wedge \ A \subseteq B) \implies x \in B\Big)$:

La A, B og x være vilkårlige mengder. (*Bevisteknikk 8*)

Anta $x \in A \ \wedge \ A \subseteq B$. (*Bevisteknikk 1*)
$x \in A \ \wedge \ A \subseteq B$ gir spesielt $x \in A$. (*Slutningsregel 2*)
$x \in A \ \wedge \ A \subseteq B$ gir spesielt $A \subseteq B$. (*Slutningsregel 2*)
Per definisjon av $A \subseteq B$ har vi at $\forall y(y \in A \Rightarrow y \in B)$.
Vi får da at $x \in A \Rightarrow x \in B$. (*Slutningsregel 4*)
Siden vi nå har $x \in A$ og $x \in A \Rightarrow x \in B$, konkluderer vi med at $x \in B$. (*Slutningsregel 1*)

Vi konkluderer med at $(x \in A \ \wedge \ A \subseteq B) \implies x \in B$.

Siden A, B og x var vilkårlige, konkluderer vi med at $\forall A \forall B \forall x \Big((x \in A \ \wedge \ A \subseteq B) \implies x \in B\Big)$.

□

Beviset for følgende proposisjon lar vi være en oppgave.

Proposisjon 2.3. *Vi har at*

$$\begin{aligned} \forall A \quad & A \subseteq A, \\ \forall A \forall B \forall C \quad & \Big(A \subseteq B \ \wedge \ B \subseteq C \implies A \subseteq C\Big), \\ \forall A \forall B \quad & \Big(A \subseteq B \ \wedge \ B \subseteq A \implies A = B\Big). \end{aligned}$$

Tomme mengder

Definisjon 2.4. Vi sier at en mengde A er *tom* dersom den ikke inneholder noen elementer. Altså

$$\forall x(x \notin A).$$

Proposisjon 2.5. *La A og B være tomme mengder. Da er $A = B$.*

Bevis. Vi viser at $\forall x\big(x \in A \Leftrightarrow x \in B\big)$:

La x være vilkårlig. Fra definisjonen av en tom mengde vet vi at $x \notin A$ og $x \notin B$. Ergo er utsagnene $x \in A$ og $x \in B$ usanne, så ekvivalensen $x \in A \Leftrightarrow x \in B$ er sann.

Siden x var vilkårlig, har vi nå vist at $\forall x\big(x \in A \Leftrightarrow x \in B\big)$. Fra Aksiom 1 kan vi konkludere med at $A = B$. □

Proposisjon 2.5 viser at det kan finnes høyst én tom mengde. Men vi vet ikke ennå at det fins en tom mengde i det hele tatt. Faktisk kunne universet vårt av mengder vært helt tomt så langt. Men dette vil neste aksiom endre.

Aksiom 2. Det fins en tom mengde. Altså

$$\exists A \forall x (x \notin A).$$

Notasjon 2.6. Ved Aksiom 2 og Proposisjon 2.5 vet vi nå at det finnes en *unik* tom mengde. Vi betegner den med $\emptyset$. Denne mengden karakteriseres altså ved at

$$\forall x (x \notin \emptyset).$$

Vi vet altså nå at universet vårt i hvert fall inneholder ett objekt, den tomme mengden. Men så langt trenger det ikke inneholder noe mer.

Mengder bestemt av predikater

La $P(x)$ være et predikat. Et legitimt spørsmål er om det eksisterer en mengde B som er karakterisert av at elementene tilfredsstiller predikatet $P(x)$. Med andre ord, fins det en mengde B slik at

$$x \in B \quad \iff \quad P(x) \ ?$$

I boka kaller man slike predikater for *mengdebyggende*, men jeg tror ikke jeg kommer til å bruke det så mye.

Lemma 2.7. *La $P(x)$ være et predikat, og anta at det fins en mengde B slik at*

$$\forall x \left(x \in B \quad \iff \quad P(x)\right).$$

Da er B entydig bestemt. Med andre ord, dersom B' er en mengde slik at

$$\forall x \left(x \in B' \quad \iff \quad P(x)\right),$$

så må $B = B'$.

Bevis. Vi antar at B og B' begge er mengder som tilfredsstiller de overnevnte egenskapene. Vi bruker nå Aksiom 1 til å vise at $B = B'$.

La x være vilkårlig. Dersom $x \in B$, får vi per antagelse om B at $P(x)$. Men per antagelse om B' gir dette $x \in B'$. På den andre siden, dersom $x \in B'$, gir antagelsen om B' at $P(x)$, som igjen gir $x \in B$ fra antagelsen om B.

Argumentet over viser at $\forall x \left(x \in B \Leftrightarrow x \in B'\right)$. Fra Aksiom 1 konkluderer vi med at $B = B'$. □

Notasjon 2.8. La $P(x)$ være et predikat. Vi betegner den unike mengden fra Lemma 2.7, dersom den finnes, med

$$\{x : P(x)\}.$$

Dette leses "mengden av x slik at $P(x)$". Denne mengden karakteriseres altså entydig ved egenskapen

$$\forall y \left(y \in \{x : P(x)\} \quad \iff \quad P(y)\right).$$

Eksempel 2.9. La $P(x)$ stå for predikatet $\bot$, altså predikatet som er universelt usant uavhengig av hva x måtte være. Dette predikatet er mengdebyggende dersom det fins en mengde B slik at

$$\forall x\,(x \in B \quad \iff \quad \bot).$$

Siden $(x \in B) \Leftrightarrow \bot$ er logisk ekvivalent med $x \notin B$, ser vi at utsagnet over karakteriserer den tomme mengden. Vi konkluderer med at $P(x)$ er mengdebyggende, og at

$$\emptyset = \{x : \bot\}.$$

Eksempel 2.10. La $P(x)$ stå for predikatet $x \notin x$. La oss anta at det er mengdebyggende, altså at det fins en mengde B som karakteriseres av

$$\forall x\,(x \in B \quad \iff \quad x \notin x).$$

Nå har det seg slik at enten så er $B \in B$ eller så er $B \notin B$. Dersom $B \in B$ gir den karakteriserende egenskapen til B at $B \notin B$, som er en selvmotsigelse. På den andre siden, dersom $B \notin B$, betyr det igjen fra den karakteriserende egenskapen til B at $B \in B$, som igjen er en selvmotsigelse. I hvert tilfelle får vi en selvmotsigelse.

Konklusjonen vår er dermed at mengden B ikke fins, altså at predikatet $x \notin x$ ikke er mengdebyggende. Selvmotsigelsen over kalles *Russells paradoks*.

Vi har følgende grunnleggende aksiom for mengdebygging.

Aksiom 3. La $P(x)$ være et predikat i én variabel x. Da har vi at

$$\forall A\,\exists B\,\forall x\,\Big(x \in B \quad \Leftrightarrow \quad (x \in A) \wedge P(x)\Big).$$

Aksiomet sier altså at om vi allerede har en mengde A og et predikat $P(x)$, så kan vi danne en mengde B av elementer x som allerede er i A og i tillegg tilfredsstiller $P(x)$. Da unngår vi Russells paradoks.

Notasjon 2.11. Aksiomet sier altså at predikatet $(x \in A) \wedge P(x)$ er mengdebyggende. Det følger fra Lemma 2.7 at mengden B i Aksiom 3 er entydig bestemt. Vi innfører notasjonen

$$\{x \in A : P(x)\} = \{x : (x \in A) \wedge P(x)\}.$$

Aksiomet for par

Følgende aksiom sier at det for alle mengder y og z så fins det en mengde A som inneholder både y og z.

Aksiom 4.

$$\forall y\,\forall z\,\exists A\,(y \in A \wedge z \in A).$$

Aksiomet sier ikke rett ut mengden A inneholder *kun* x og y, men en slik mengde kan vi nå ordne oss ved hjelp av Aksiom 3.

Proposisjon 2.12. *La y og z være mengder. Da er følgende predikat i variabelen x mengdebyggende:*

$$x = y \vee x = z.$$

Bevis. Ved Aksiom 4 så fins det en mengde A slik at $y \in A \wedge z \in A$. Vi bruker nå Aksiom 3 til å danne oss mengden

$$B = \{x \in A : x = y \vee x = z\}.$$

Vi påstår nå at

$$\forall x \, (x \in B \quad \iff \quad x = y \vee x = z).$$

For å vise dette, la x være vilkårlig. Dersom vi antar at $x \in B$, så får vi per definisjon av B at $x \in A$ og $x = y \vee x = z$. Spesielt har vi at $x = y \vee x = z$.

På den andre siden, dersom vi antar at $x = y \vee x = z$, så gir første antagelse at $x \in A$. Vi har dermed at $x \in A$ og $x = y \vee x = z$. Per definisjon av B får vi da at $x \in B$.

Siden x var vilkårlig, viser dette at

$$B = \{x : x = y \vee x = z\}.$$

Vi har dermed vist at predikatet er mengdebyggende, hvilket fullfører beviset. □

Notasjon 2.13. La y og z være mengder. Vi skriver

$$\{y, z\} = \{x : x = y \vee x = z\}.$$

Spesielt skriver vi

$$\{y\} = \{y, y\}.$$

Legg merke til at $\{y\}$ er karakterisert av

$$\forall x \, (x \in \{y\} \quad \iff \quad x = y).$$

Vi har nå gått fra å ha muligens bare én mengde til å ha "uendelig" mange mengder (vi skal definere uendelighet presist senere). Vi kan nå nemlig danne oss mengden $\{\emptyset\}$. Den er ikke tom, og dermed ulik $\emptyset$. Så kan vi danne oss $\{\{\emptyset\}\}$, som igjen er ulik, også videre.

2.2 Snitt og union

Vi skal nå danne snitt og union av mengder. Men først gjør vi noen konvensjoner.

Notasjon 2.14. Dersom $P(x)$ er et predikat av en variabel x og A er en mengde, så innfører vi følgende forkortelse:

$$\forall x \in A \; P(x) \quad \iff \quad \forall x \, (x \in A \Rightarrow P(x)).$$

Dette gir en litt forkortet bevisstrategi: Når vi skal bevise høyresiden ville vi i prinsippet latt x vært en vilkårlig mengde og deretter antatt at $x \in A$ for å utlede $P(x)$. Når vi beviser venstresiden så tenker vi heller at vi lar $x \in A$ fra starten av, og deretter er målet å utlede $P(x)$.

Vi gjør noe lignende for eksistensiell kvantor: Vi innfører forkortelsen

$$\exists x \in A \; P(x) \quad \iff \quad \exists x \, (x \in A \wedge P(x)).$$

Her blir da tanken at for å bevise at det fins en x slik at $x \in A$ og $P(x)$, så beviser vi direkte at det fins en $x \in A$ slik at $P(x)$.

Så, til snitt. Gitt mengder A og B, så vil vi definere snittet $A \cap B$ ved hjelp av følgende predikat av variabelen x:

$$x \in A \wedge x \in B.$$

Vi ønsker at dette predikatet skal være mengdebyggende. Men det er det, for vi kan danne mengden $\{x \in A : x \in B\}$. Vi har imidlertid lyst til å danne snitt av ikke bare to mengder, men av større samlinger av mengder. Vi ser generelt for oss at vi har en ikke-tom mengde $\mathcal{A}$ av mengder. Det tilhørende snittet skal da være mengden av elementer som er inneholdt i hver a mengdene i $\mathcal{A}$. Følgende proposisjon viser at dette allerede er mulig med aksiomene vi har så langt.

Proposisjon 2.15. *La $\mathcal{A}$ være en ikke-tom mengde. Da er følgende predikat av variabelen x mengdebyggende:*

$$\forall A \in \mathcal{A}\,(x \in A).$$

Bevis. Siden $\mathcal{A}$ er ikke-tom, kan vi velge en $A_0 \in \mathcal{A}$. Ved Aksiom 3 kan vi danne mengden

$$B = \{x \in A_0 : \forall A \in \mathcal{A}\,(x \in A)\}.$$

Vi merker oss deretter at, analogt som i beviset for Proposisjon 2.12, at

$$\forall x \big(x \in B \iff \forall A \in \mathcal{A}\,(x \in A)\big).$$

Dette viser at predikatet er mengdebyggende. □

Notasjon 2.16. Gitt en ikke-tom mengde $\mathcal{A}$ så setter vi

$$\bigcap \mathcal{A} = \{x : \forall A \in \mathcal{A}\,(x \in A)\}$$

og kaller denne mengden for *snittet* av $\mathcal{A}$.

Dersom $\mathcal{A} = \{A, B\}$, så skriver vi spesielt

$$\bigcap \mathcal{A} = A \cap B.$$

Eksempel 2.17. La

$$\mathcal{A} = \Big\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\{\emptyset\}\}\}\Big\}.$$

Vi ser at $\emptyset \in \{\emptyset\}$, $\emptyset \in \{\emptyset, \{\emptyset\}\}$, og $\emptyset \in \{\emptyset, \{\{\emptyset\}\}\}$, så $\emptyset \in \bigcap \mathcal{A}$. På den andre siden, dersom $x \in \bigcap \mathcal{A}$, så må $x \in \{\emptyset\}$, som gir $x = \emptyset$. Dette viser at

$$\bigcap \mathcal{A} = \{\emptyset\}.$$

Vi går nå videre til unioner. Igjen er ideen at vi har en mengde $\mathcal{A}$ av mengder, og ønsker å danne mengden av elementer som er inneholdt i minst én av mengdene i $\mathcal{A}$. Vi ønsker med andre ord at følgende predikat i variabelen x er mengdebyggende:

$$\exists A \in \mathcal{A}\,(x \in A).$$

I motsetning til snitt, så trenger vi et nytt aksiom for å danne unioner.

Aksiom 5. Vi har at

$$\forall \mathcal{A}\, \exists B\, \forall x \Big(\big(\exists A \in \mathcal{A}\,(x \in A)\big) \implies x \in B\Big).$$

Proposisjon 2.18. *La $\mathcal{A}$ være en mengde. Da er følgende predikat av variabelen x mengdebyggende:*

$$\exists A \in \mathcal{A}\,(x \in A).$$

Vi lar beviset for proposisjonen over være en oppgave.

Notasjon 2.19. Gitt en mengde $\mathcal{A}$, så setter vi

$$\bigcup \mathcal{A} = \{x : \exists A \in \mathcal{A}\,(x \in A)\}$$

og kaller denne mengden for *unionen* av $\mathcal{A}$.

Dersom $\mathcal{A} = \{A, B\}$, så skriver vi spesielt

$$\bigcup \mathcal{A} = A \cup B.$$

Proposisjon 2.20. *La A, B, C og D være mengder. Da gjelder følgende:*

$$A \cap (B \cap C) = (A \cap B) \cap C \tag{2.1}$$
$$A \cup (B \cup C) = (A \cup B) \cup C, \tag{2.2}$$
$$A \cap B = B \cap A, \tag{2.3}$$
$$A \cup B = B \cup A, \tag{2.4}$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \tag{2.5}$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \tag{2.6}$$
$$A \cap \emptyset = \emptyset, \tag{2.7}$$
$$A \cup \emptyset = A, \tag{2.8}$$
$$(A \subseteq C \ \wedge \ B \subseteq D) \implies (A \cap B \subseteq C \cap D \ \wedge \ A \cup B \subseteq C \cup D). \tag{2.9}$$

Bevis. La oss bevise $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, resten lar vi være en oppgave.

La x være vilkårlig. Anta først at $x \in A \cap (B \cup C)$. Per definisjon av snitt får vi da at $x \in A$ og $x \in B \cup C$. Per definisjon av union får vi da at $x \in B$ eller $x \in C$. I tilfellet der $x \in B$, har vi at $x \in A \cap B$, så $x \in (A \cap B) \cup (A \cap C)$. I tilfellet der $x \in C$, får vi at $x \in A \cap C$, så $x \in (A \cap B) \cup (A \cap C)$.

I motsatt retning, anta at $x \in (A \cap B) \cup (A \cap C)$. I tilfellet der $x \in A \cap B$, har vi at både $x \in A$ og $x \in B$. Sistnevnte gir spesielt $x \in B \cup C$, så $x \in A \cap (B \cup C)$. I tilfellet der $x \in A \cap C$, har vi både $x \in A$ og $x \in C$. Sistnevnte gir spesielt $x \in B \cup C$, så vi får at $x \in A \cap (B \cup C)$.

Siden x var vilkårlig, konkluderer vi med at $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. □

Med unioner kan vi nå lage oss mengder med tre elementer, fire elementer, også videre. For eksempel, om vi har mengder x, y og z, så definerer vi

$$\{x, y, z\} = \{x, y\} \cup \{z\}.$$

Om w er et fjerde element, definerer vi

$$\{x, y, z, w\} = \{x, y, z\} \cup \{w\},$$

og slik kan man fortsette. Vi skal imidlertid gjøre dette mer systematisk straks vi har utviklet naturlige tall.

Definisjon 2.21. Gitt mengder A og B, så definerer vi *komplementet* av B i A til å være mengden

$$A \setminus B = \{x \in A : x \notin B\}.$$

Dette kalles også *differansen* av A og B.

Proposisjon 2.22. *For mengder A, B og C gjelder følgende:*

$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B), \tag{2.10}$$
$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B). \tag{2.11}$$

Bevis. Oppgave. □

2.3 Potensmengder og kartesiske produkt

Vårt neste aksiom garanterer at potensmengder eksisterer, altså mengden av alle delmengder av en gitt mengde.

Aksiom 6. Vi har at

$$\forall A \, \exists \mathcal{A} \, \forall B \Big(B \subseteq A \implies B \in \mathcal{A} \Big).$$

Ved å kombinere Aksiom 6 med Aksiom 3 får vi at følgende predikat i variabelen B er mengdebyggende:

$$B \subseteq A.$$

Vi kan derfor innføre følgende terminologi og notasjon:

Notasjon 2.23. Vi innfører notasjonen

$$\mathcal{P}(A) = \{B : B \subseteq A\}$$

og kaller denne mengden for *potensmengden* til A.

Eksempel 2.24. La oss bestemme potensmengden noen mengder. Vi begynner med $\emptyset$. Gitt en mengde A så har vi at $A \subseteq \emptyset$ hvis og bare hvis $A = \emptyset$. Dermed er $\mathcal{P}(\emptyset) = \{\emptyset\}$.

La oss nå bestemme potensmengden til $\{\emptyset\}$. Vi har umiddelbart at $\emptyset \subseteq \{\emptyset\}$ og $\{\emptyset\} \subseteq \{\emptyset\}$, så $\{\emptyset, \{\emptyset\}\} \subseteq \mathcal{P}(\{\emptyset\})$. For å se at dette er hele potensmengden, la $A \in \mathcal{P}(\{\emptyset\})$. Vi må vise at $A = \emptyset \ \vee \ A = \{\emptyset\}$. Vi tar i bruk Bevisteknikk 6: Anta at $A \neq \emptyset$. Da må det finnes en $x \in A$, men siden $A \subseteq \{\emptyset\}$ så må $x \in \{\emptyset\}$ som $x = \emptyset$. Vi har da at $\{\emptyset\} \subseteq A \subseteq \{\emptyset\}$. Vi må da konkludere med at $A = \{\emptyset\}$. Vi har dermed vist at

$$\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}.$$

Vi skal nå begynne å jobbe oss mot konstruksjonen av det kartesiske produktet av to mengder. Først trenger vi følgende lemma.

Lemma 2.25. *La x, y, a og b være mengder. Da gjelder*

$$\{x, y\} = \{a, b\} \quad \iff \quad \Big((x = a \wedge y = b) \vee (x = b \wedge y = a) \Big).$$

Bevis. Oppgave. □

Definisjon 2.26. La x og y være mengder. Vi definerer

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Vi kaller (x, y) et *ordnet par* med første koordinat lik x og andre koordinat lik y.

Proposisjon 2.27. *La x, y, a og b være mengder. Da har vi at*

$$(x, y) = (a, b) \quad \Longleftrightarrow \quad (x = a) \wedge (y = b).$$

Bevis. Vi viser først implikasjonen fra høyre til venstre. Dersom $x = a \wedge y = b$, får vi umiddelbart $(x, y) = (a, b)$.

Så viser vi implikasjonen fra venstre til høyre. Anta at $(x, y) = (a, b)$. Siden $\{\{x\}, \{x, y\}\} = \{\{a\}, \{a, b\}\}$ gir Lemma 2.25 da to tilfeller:

- Dersom $\{x\} = \{a\}$ og $\{x, y\} = \{a, b\}$, gir førstnevnte $x = a$. Sistnevnte gir $y \in \{a, b\}$, så $y = a$ eller $y = b$.
  - Dersom $y = a$ får vi $x = y = a$. Siden $b \in \{x, y\}$, får vi at $x = y = a = b$, hvilket gir ønsket konklusjon $(x = a) \wedge (y = b)$.
  - Dersom $x = b$, har vi ønsket konklusjon $x = a \wedge y = b$.
- Dersom $\{x\} = \{a, b\}$ og $\{x, y\} = \{a\}$, gir førstnevnte at $a \in \{x\}$ og $b \in \{x\}$, så $a = b = x$. Sistnevnte gir $y \in \{a\}$, som gir $y = a$. Vi har da spesielt $(x = a) \wedge (y = b)$.

I hvert tilfelle har vi altså at $x = a \wedge y = b$. Dette viser implikasjonen fra venstre til høyre. □

Proposisjon 2.28. *La A og B være mengder. Følgende predikat i variabelen z er mengdebyggende:*

$$\exists x \in A\, \exists y \in B\, (z = (x, y)).$$

Bevis. La $x \in A$ og $y \in B$. Da er $\{x\} \subseteq A \subseteq A \cup B$ og $\{x, y\} \subseteq A \cup B$, så $\{x\} \in \mathcal{P}(A \cup B)$ og $\{x, y\} \in \mathcal{P}(A \cup B)$. Det følger at

$$(x, y) = \{\{x\}, \{x, y\}\} \in \mathcal{P}(\mathcal{P}(A \cup B)).$$

La

$$C = \{z \in \mathcal{P}(\mathcal{P}(A \cup B)) : \exists x \in A\, \exists y \in B\, (z = (x, y))\}.$$

Da ser vi på samme måte som i lignende tidligere bevis at

$$\forall z \Big(z \in C \quad \Leftrightarrow \quad \exists x \in A\, \exists y \in B\, (z = (x, y))\Big).$$

Dette fullfører beviset. □

På grunn av Proposisjon 2.28 kan vi nå komme med følgende definisjon:

Definisjon 2.29. La A og B være mengder. Vi lar

$$A \times B = \{z : \exists x \in A\, \exists y \in B\, (z = (x, y))\}$$

og kaller denne mengden det *kartesiske produktet* av A og B.

Proposisjon 2.30. *La A, B og C være mengder. Da gjelder følgende:*

$$A \times (B \cap C) = (A \times B) \cap (A \times C),$$
$$A \times (B \cup C) = (A \times B) \cup (A \times C),$$
$$A \times \emptyset = \emptyset \times A = \emptyset.$$

Vi definerer ordnede tripler som følger: gitt mengder x, y og z, så setter vi

$$(x, y, z) = ((x, y), z).$$

Man kan da sjekke at for mengder a, b og c så gjelder $(x, y, z) = (a, b, c)$ hvis og bare hvis $x = a$, $y = b$ og $z = c$. Vi skal systematisk definere kartesisk produkt av flere enn to mengder senere.

Kapittel 3

Funksjoner

Vi skal nå definere et av de viktigste begrepene i matematikk innenfor det mengdeteoretiske rammeverket vi har utviklet, nemlig begrepet om en *funksjon*. Siden alle objektene våre er mengder, vil funksjoner også defineres til å være visse typer mengder.

3.1 Definisjonen av en funksjon

Definisjon 3.1. En funksjon er en trippel $f = (A, B, R)$ der

(i) A er en mengde.
(ii) B er en mengde.
(iii) R er en delmengde av $A \times B$ som tilfredsstiller følgende egenskap:

$$\forall x \in A \, \exists! y \in B \, \big((x, y) \in R\big).$$

Notasjon 3.2. Vi introduserer viktig terminologi og notasjon for funksjoner. La $f = (A, B, R)$ være en funksjon.

- Vi kaller A for *domenet* til f og B for *kodomenet* til f.
- Vi kaller R for *grafen* til f. Egenskapen til grafen sier da at for hver x i domenet til f så skal det finnes en entydig y i kodomenet til f slik at (x, y) er i grafen til f. Siden denne y-en er entydig bestemt av x, kan vi gi den et navn. Vi kaller den

$$y = f(x).$$

- I stedet for å skrive la $f = (A, B, R)$ være en funksjon, så kommer vi til å, gitt mengder A og B, skrive "la $f \colon A \to B$" være en funksjon. Dette uttrykket indikerer da at f er en funksjon med domene lik A og kodomene lik B.
- For å angi en funksjon f må man altså angi domenet A, kodomenet B, og beskrive $f(x)$ for hver $x \in A$.

Proposisjon 3.3. *La f og g være funksjoner. Da gjelder $f = g$ hvis og bare hvis de tre følgende egenskapene holder:*

(i) f og g har samme domene.
(ii) f og g har samme kodomene.
(iii) For alle x i det felles domenet til f og g gjelder

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

Bevis. Siden f og g er funksjoner, kan vi skrive $f = (A, B, R)$ og $g = (C, D, S)$ der A, B, C og D er mengder, og $R \subseteq A \times B$ og $S \subseteq C \times D$ tilfredsstiller kriteriet i Definisjon 3.1 (iii).

Anta først at $f = g$. Fra den grunnleggende egenskapen til ordnede tripler får vi umiddelbart at $A = C$, $B = D$, og $R = S$. De to første likhetene sier nettopp at f og g har samme domene og kodomene. For å vise den siste egenskapen (iii), la $x \in A$ være vilkårlig. Da er $(x, f(x)) \in R$. Siden $R = S$, får vi at $(x, f(x)) \in S$. På den andre siden er $(x, g(x)) \in S$. Siden det fins en entydig $y \in B$ slik at $(x, y) \in S$, kan vi slutte at $f(x) = y = g(x)$. Siden x var vilkårlig, viser dette (iii).

I motsatt retning, la oss anta at (i), (ii), og (iii) over er tilfredsstilt. Da gir (i) og (ii) gir umiddelbart $A = C$ og $B = D$. Det gjenstår å vise at $R = S$. La $(x, y) \in R$. Da må $y = f(x)$. Per antagelse har vi at $f(x) = g(x)$. Men da er $(x, g(x)) \in S$. Vi konkluderer med at $(x, y) \in S$. I motsatt retning, anta at $(x, y) \in S$. Da må $y = g(x)$. Per antagelse har vi at $f(x) = g(x)$, men da er $(x, f(x)) \in R$. Vi konkluderer med at $(x, y) \in R$. Dette viser at $R = S$, og vi kan slutte at $f = g$. □

Merknad 3.4. Det er viktig å presisere at definisjonen av en funksjon her er annerledes enn i [1]. Vi krever at en funksjon skal være definert overalt på domenet A. Vårt begrep om en funksjon er altså det samme som begrepet om en *avbildning* i [1].

Eksempel 3.5. La A være en mengde. La oss se på hva det innebærer å ha en funksjon $f\colon \emptyset \to A$. Grafen R til f må da være en delmengde av $\emptyset \times A = \emptyset$. Det fins dermed én eneste mulighet: $R = \emptyset$. Dette valget av graf tilfredsstiller kriteriet i Definisjon 3.1 (iii), for kriteriet blir tomt. Vi konkluderer med at det fins nøyaktig én funksjon fra $\emptyset$ til A. Denne funksjonen kalles ofte den *tomme funksjonen*.

La oss se hva det innebærer å ha en funksjon $A \to \emptyset$. Nå skal grafen være en delmengde av $A \times \emptyset = \emptyset$. Men kriteriet $\forall x \in A \exists! y \in \emptyset (x, y) \in \emptyset$ kan nå umulig tilfredsstilles med mindre $A = \emptyset$. Vi konkluderer med at det kun fins en funksjon fra A til $\emptyset$ når $A = \emptyset$, i hvilket tilfelle vi har den tomme funksjonen.

Eksempel 3.6. La A være en mengde. Da kaller vi funksjonen $\mathrm{id}_A\colon A \to A$ gitt ved

$$\mathrm{id}_A(x) = x, \quad x \in A,$$

for *identitetsfunksjonen* på A. Grafen til id_A er altså mengden $\{z \in A \times A : \exists x \in X(z = (x, x))\}$.

Eksempel 3.7. La A og B være mengder. Da fins det en "kanonisk" funksjon $p_1\colon A \times B \to A$ gitt ved

$$p_1(x, y) = x, \quad (x, y) \in A \times B.$$

Tilsvarende har vi en kanonisk funksjon $p_2\colon A \times B \to B$ gitt ved

$$p_2(x, y) = y, \quad (x, y) \in A \times B.$$

Disse to funksjonene kalles ofte projeksjonene av det kartesiske produktet $A \times B$ på henholdsvis faktoren A og B.

Legg merke til at om $z, w \in A \times B$ tilfredsstiller $p_1(z) = p_1(w)$ og $p_2(z) = p_2(w)$, så må $z = w$.

Eksempel 3.8. La A være en mengde og la $C \subseteq A$. Da kan vi definere en funksjon $i\colon C \to A$ ved

$$i(x) = x, \quad x \in C.$$

Denne funksjonen kalles *inklusjonen* av C inn i A.

La nå B være en mengde og la $f\colon A \to B$ være en funksjon. Vi definerer *restriksjonen* av f til C til være funksjonen $f|_C\colon C \to B$ gitt ved

$$f|_C(x) = f(x), \quad x \in C.$$

Dersom $g\colon C \to B$ er en funksjon, så sier vi at f er en *utvidelse* av g dersom $f|_C = g$.

Eksempel 3.9. La A og B være mengder. Anta at A_1 og A_2 er delmengder av A slik at $A = A_1 \cup A_2$ og $A_1 \cap A_2 = \emptyset$. Om vi har funksjoner $f_1\colon A_1 \to B$ og $f_2\colon A_2 \to B$, så kan vi definere en funksjon $f\colon A \to B$ på følgende vis:

$$f(x) = \begin{cases} f_1(x), & x \in A_1, \\ f_2(x), & x \in A_2. \end{cases}$$

Med dette så mener vi funksjonen fra A til B som har graf

$$R = \{(x, y) \in A \times B : (x \in A_1 \implies y = f_1(x)) \wedge (x \in A_2 \implies y = f_2(x))\}.$$

At denne grafen faktisk tilfredsstiller Definisjon 3.1 (iii) kommer av at $A = A_1 \cup A_2$ og $A_1 \cap A_2 = \emptyset$.

Proposisjon 3.10. *La A og B være mengder. Da er følgende predikat i variabelen f mengdebyggende:*

$$f \text{ er en funksjon fra } A \text{ til } B.$$

Vi betegner den korresponderende mengden med B^A. Med andre ord består mengden B^A av alle funksjoner fra A til B.

Bevis. Fra definisjonen av en funksjon kan vi skrive predikatet på følgende måte:

$$\exists R \in \mathcal{P}(A \times B)\Big(f = (A, B, R) \wedge \big(\forall x \in A\ \exists! y \in B\ ((x, y) \in R)\big)\Big).$$

Kall dette predikatet for $Q(f)$. Vi kan da danne mengden

$$C = \{f \in (\{A\} \times \{B\}) \times \mathcal{P}(A \times B) : Q(f)\}.$$

Det følger da at C er en mengde slik at $f \in C$ hvis og bare hvis $Q(f)$. Dette fullfører beviset. □

3.2 Komposisjon

En av de aller mest grunnleggende tingene vi kan gjøre med funksjoner er å komponere dem.

Definisjon 3.11. La A, B og C være mengder, og la $f\colon A \to B$ og $g\colon B \to C$ være funksjoner. Da definerer vi *g komponert med f* til å være funksjonen $g \circ f\colon A \to C$ gitt ved

$$(g \circ f)(x) = g(f(x)), \quad x \in A.$$

Vi kan skrive komposisjoner diagrammatisk på følgende måte:

$$A \xrightarrow{f} B \xrightarrow{g} C$$

Eksempel 3.12. La $f\colon A \to B$ være en funksjon og la $C \subseteq A$ være en delmengde. Da er restriksjonen $f|_C\colon C \to B$ av f til C intet annet enn komposisjonen $f|_C = f \circ i$, der $i\colon C \to A$ er inklusjonen av C inn i A.

Proposisjon 3.13. *La A, B, C og D være mengder, og la $f\colon A \to B$, $g\colon B \to C$ og $h\colon C \to D$ være funksjoner. Da gjelder*

$$(h \circ g) \circ f = h \circ (g \circ f),$$
$$f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f.$$

Bevis. Beviset for den første identiteten er som følger: La $x \in A$. Da har vi at

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

Siden x var vilkårlig, kan vi slutte at $(h \circ g) \circ f = h \circ (g \circ f)$.

Vi overlater neste identitet som en oppgave. □

Definisjon 3.14. La $f\colon A \to B$ være en funksjon. En funksjon $g\colon B \to A$ kalles

(i) *venstreinvers* for f dersom
$$g \circ f = \mathrm{id}_A.$$

(ii) *høyreinvers* for f dersom
$$f \circ g = \mathrm{id}_B.$$

(iii) *invers* for f dersom den både er en venstreinvers og en høyreinvers for f.

Eksempel 3.15. La A være en mengde. Da har $\mathrm{id}_A\colon A \to A$ en invers, nemlig seg selv.

Eksempel 3.16. La A og B være ikke-tomme mengder der A er en delmengde av B. Betrakt inklusjonen $i\colon A \to B$.

Vi kan definere en venstre-invers til i på følgende vis: Velg et hvilket som helst element $a \in A$ (vi kan gjøre dette siden $A \neq \emptyset$) og definer $g\colon B \to A$ ved

$$g(x) = \begin{cases} x, & x \in A, \\ a, & x \notin A. \end{cases}$$

For alle $x \in A$ får vi da at
$$(g \circ i)(x) = g(i(x)) = g(x) = x.$$

Dette viser at $g \circ i = \mathrm{id}_A$.

Anta derimot at i har en høyreinvers h. Vi skal da ha $i \circ h = \mathrm{id}_B$, altså $i(h(x)) = x$ for alle $x \in B$. Siden $i(h(x)) \in A$, gir dette $x \in A$. Vi må altså ha at $A = B$ for at i skal kunne ha en høyreinvers. Men i dette tilfellet er $i = \mathrm{id}_A$, som er sin egen invers.

Proposisjon 3.17. *Anta at $f\colon A \to B$ har en venstreinvers g og en høyreinvers h. Da er $g = h$. Dermed har f en invers, og inversen er entydig bestemt.*

Bevis. Siden g er en venstreinvers for f, så har vi at $g \circ f = \mathrm{id}_A$. Siden h er en høyreinvers for f, så har vi at $f \circ h = \mathrm{id}_B$. Vi får nå at

$$g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h.$$

□

Notasjon 3.18. Dersom $f\colon A \to B$ har en invers, så sier vi at f er *invertibel*. I så fall betegner vi inversen til f med f^{-1}.

Proposisjon 3.19. *Følgende holder:*

(i) Dersom $f\colon A \to B$ er invertibel, så er $f^{-1}\colon B \to A$ invertibel, og $(f^{-1})^{-1} = f$.
(ii) Dersom $f\colon A \to B$ og $g\colon B \to C$ begge er invertible, så er $g \circ f$ invertibel, og

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Bevis. (i): Per definisjon har vi at $f \circ f^{-1} = \mathrm{id}_B$ og $f^{-1} \circ f = \mathrm{id}_A$. Om vi leser disse på riktig måte, faller det rett ut at f^{-1} er invertibel, med invers gitt ved f.

(ii): Anta at $f\colon A \to B$ og $g\colon B \to C$ er invertible. Vi beregner da at

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_B \circ f = f^{-1} \circ f = \mathrm{id}_A.$$

Tilsvarende får vi at

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{id}_B \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_C.$$

Dette fullfører beviset. □

Definisjon 3.20. La $f\colon A \to B$ være en funksjon. Vi sier at f er

(i) *injektiv* dersom

$$\forall x \in A \forall x' \in A \left(f(x) = f(x') \implies x = x'\right),$$

(ii) *surjektiv* dersom

$$\forall y \in B \exists x \in A \left(f(x) = y\right).$$

(iii) *bijektiv* dersom f er både injektiv og surjektiv.

Vi kan omformulere injektivitet på følgende måte: For hver $y \in B$ fins det *høyst én* $x \in A$ slik at $f(x) = y$. Vi ser da at bijektivitet er det samme som at det for hver $y \in B$ fins *nøyaktig én* $x \in A$ slik at $f(x) = y$.

Proposisjon 3.21. *La $f\colon A \to B$ og $g\colon B \to C$ være funksjoner. Da gjelder følgende:*

(i) Dersom f og g er injektive, så er $g \circ f$ injektiv.
(ii) Dersom f og g er surjektive, så er $g \circ f$ surjektiv.
(iii) Dersom $g \circ f$ er injektiv, så er f injektiv.
(iv) Dersom $g \circ f$ er surjektiv, så er g surjektiv.

Bevis. Sterkt anbefalt oppgave. □

Proposisjon 3.22. *La $f\colon A \to B$ være en funksjon. Da er f invertibel hvis og bare hvis f er bijektiv.*

Bevis. Anta først at f er invertibel. Vi viser først at f er injektiv. La derfor $x, x' \in A$ og anta at $f(x) = f(x')$. Vi får da at

$$x = f^{-1}(f(x)) = f^{-1}(f(x')) = x'.$$

Dette viser at f er injektiv. La så $y \in B$. Sett $x = f^{-1}(y)$. Vi ser da at

$$f(x) = f(f^{-1}(y)) = y.$$

Dette viser at f er surjektiv. Altså er f bijektiv.

Nå antar vi at f er bijektiv. Da fins det for enhver $y \in B$ en entydig $g(y) \in A$ slik at $f(g(y)) = y$. Dette definerer en funksjon $g\colon B \to A$ med egenskapen $f \circ g = \mathrm{id}_B$. Spesielt får vi for hver $x \in A$ at $f(g(f(x))) = f(x)$. Fra entydigheten gir dette at $g(f(x)) = x$. Vi kan dermed slutte at $g \circ f = \mathrm{id}_A$. Dette viser at f er invertibel. □

Eksempel 3.23. La A, B og C være mengder. Vi betrakter det kartesiske produktet $A \times B$ med projeksjonene p_1 og p_2 fra Eksempel 3.7. La funksjoner $f_1 \colon C \to A$ og $f_2 \colon C \to B$ være gitt. Vi kan da danne en funksjon $f \colon C \to A \times B$ ved

$$f(z) = (f_1(z), f_2(z)), \quad z \in C. \tag{3.1}$$

Denne funksjonen har egenskapen at $p_1 \circ f = f_1$ og $p_2 \circ f = f_2$: Dersom $z \in C$, så ser vi at

$$(p_1 \circ f)(z) = p_1(f(z)) = p_1(f_1(z), f_2(z)) = f_1(z).$$

Dette viser at $p_1 \circ f = f_1$, og et tilsvarende argument viser at $p_2 \circ f = f_2$.

På den andre siden, gitt en funksjon $f \colon C \to A \times B$ kan vi danne funksjonene $p_1 \circ f \colon C \to A$ og $p_2 \circ f \colon C \to B$.

Dette er et typisk eksempel på en én-til-én-korrespondanse i matematikk. Vi gjør det formelt ved å definere en funksjon

$$\Phi \colon (A \times B)^C \to (A^C) \times (B^C)$$

ved

$$\Phi(f) = (p_1 \circ f, p_2 \circ f), \quad f \in (A \times B)^C.$$

Argumentet over viser at denne funksjonen er surjektiv: Vi så nettopp at om vi starter med $(f_1, f_2) \in (A^C) \times (B^C)$, så fins en funksjon $f \in (A \times B)^C$ slik at $\Phi(f) = (p_1 \circ f, p_2 \circ f) = (f_1, f_2)$.

La oss nå vise at Φ er injektiv. La $f, g \in (A \times B)^C$ og anta at $\Phi(f) = \Phi(g)$. Dette gir $p_1 \circ f = p_1 \circ g$ og $p_2 \circ f = p_2 \circ g$. La $z \in C$ være vilkårlig. Disse identitetene gir

$$\begin{aligned} p_1(f(z)) &= (p_1 \circ f)(z) = (p_1 \circ g)(z) = p_1(g(z)), \\ p_2(f(z)) &= (p_2 \circ f)(z) = (p_2 \circ g)(z) = p_2(g(z)). \end{aligned}$$

Altså stemmer både første og andre koordinater til $f(z)$ og $g(z)$ overens. Dette gir $f(z) = g(z)$. Siden z var vilkårlig, kan vi slutte at $f = g$. Dette beviser injektivitet.

Vi kan skrive $(A \times B)^C \cong (A^C) \times (B^C)$, men den fulle betydningen av denne notasjonen får vi ikke dekket i dette kurset. Legg merke til hvordan dette minner om identiteten $(ab)^c = a^c b^c$ for positive reelle tall.

3.3 Familier av mengder

Definisjon 3.24. La I være en mengde. En *familie av mengder indeksert av I* er en surjektiv funksjon $I \to \mathcal{A}$.

Notasjon 3.25. Dersom $A \colon I \to \mathcal{A}$ er en familie av mengder indeksert av I, skriver vi gjerne $A(i) = A_i$ for hver $i \in I$. Dersom $B \colon I \to \mathcal{A}$ er en annen familie av mengder indeksert av I, og vi skriver $B(i) = B_i$ for hver $i \in I$, så overlater vi det som en oppgave å sjekke at $A = B$ hvis og bare hvis $A_i = B_i$ for hver $i \in I$. Vi skriver derfor ofte $(A_i)_{i \in I}$ istedenfor A når vi betegner familien.

La $(A_i)_{i \in I}$ være en familie av mengder indeksert av I. Vi sier at $(A_i)_{i \in I}$ er en familie av delmengder av en mengde X dersom $A_i \subseteq X$ for hver $i \in I$.

Definisjon 3.26. La $(A_i)_{i\in I}$ være en familie av mengder. Da definerer vi

$$\bigcap_{i\in I} A_i = \bigcap\{A : \exists i \in I\ (A = A_i)\}, \quad \text{dersom } I \neq \emptyset,$$
$$\bigcup_{i\in I} A_i = \bigcup\{A : \exists i \in I\ (A = A_i)\},$$
$$\prod_{i\in I} A_i = \Big\{a \in \Big(\bigcup_{i\in I} A_i\Big)^I \ :\ \forall i \in I\ (a(i) \in A_i)\Big\}.$$

Disse mengdene kalles henholdsvis *snittet*, *unionen* og *produktet* av $(A_i)_{i\in I}$.

Notasjon 3.27. Dersom a er et element av produktet $\prod_{i\in I} A_i$ skriver vi ofte funksjonsverdiene som $a(i) = a_i$ og betegner ofte $a = (a_i)_{i\in I}$.

Definisjon 3.28. La $f\colon A \to B$ være en funksjon, la $U \subseteq A$ og la $V \subseteq B$.

(i) Vi kaller mengden

$$f[U] = \{f(x) : x \in U\} = \{y \in B : \exists x \in U\ (y = f(x))\}$$

for *direktebildet* (eller bare *bildet*) til U (under f). Spesielt kaller vi $f(A)$ for *bildet* eller *verdimengden* til f, og skriver også $\mathrm{Im}(f)$ for denne mengden.

(ii) Vi kaller mengden

$$f^{-1}[V] = \{x \in A : f(x) \in V\}$$

for *inversbildet* til V (under f).

Merk at en funksjon $f\colon A \to B$ er surjektiv hvis og bare hvis $\mathrm{Im}(f) = B$.

Proposisjon 3.29. *La $f\colon A \to B$ være en funksjon, la $(U_i)_{i\in I}$ være en familie av delmengder av A og la $(V_i)_{i\in I}$ være en familie av delmengder av B. Da gjelder følgende:*

$$f^{-1}[\bigcap_{i\in I} V_i] = \bigcap_{i\in I} f^{-1}[V_i], \quad I \neq \emptyset, \tag{3.2}$$
$$f^{-1}[\bigcup_{i\in I} V_i] = \bigcup_{i\in I} f^{-1}[V_i], \tag{3.3}$$
$$f[\bigcap_{i\in I} U_i] \subseteq \bigcap_{i\in I} f[U_i], \quad I \neq \emptyset, \tag{3.4}$$
$$f[\bigcup_{i\in I} U_i] = \bigcup_{i\in I} f[U_i]. \tag{3.5}$$

Bevis. Oppgave. □

Kapittel 4

Naturlige tall

4.1 Uendelighetsaksiomet

Siden vårt matematiske univers består utelukkende av mengder, må naturlige tall også være mengder. Kanskje noe uventet skal vi definere tallet 0 til å være den tomme mengden, altså $0 = \emptyset$. Så skal vi innføre en grunnleggende operasjon som gitt et naturlig tall n gir det neste naturlige tallet, altså det vi vanligvis ville beskrevet som $n + 1$.

Mer spesifikt: gitt et naturlig tall n, så skal mengden

$$n \cup \{n\}$$

uttrykke det "neste" naturlige tallet, også kalt *suksessoren* til n. Dette gir for eksempel

$$\begin{aligned} 1 &= 0 \cup \{0\} = \{0\}, \\ 2 &= 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}, \\ 3 &= 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}, \end{aligned}$$

også videre. Generelt ser vi at n kommer til å være mengden av alle de foregående naturlige tallene.

Vårt første aksiom sier at det i hvert fall må finnes en mengde som inneholder tallet $0 = \emptyset$ og som er lukket under denne suksessor-operasjonen.

Aksiom 7. Vi har at

$$\exists I \Big(\emptyset \in I \ \wedge \ \big(\forall x \, (x \in I \implies x \cup \{x\} \in I) \big) \Big).$$

Definisjon 4.1. Vi kaller en mengde I *induktiv* dersom følgende holder:

(i) $\emptyset \in I$.
(ii) For alle $x \in I$ har vi at $x \cup \{x\} \in I$.

Aksiom 7 sier da altså at det eksisterer en induktiv mengde.

Lemma 4.2. *La $\mathcal{A}$ være en ikke-tom mengde bestående av induktive mengder. Da er $\bigcap \mathcal{A}$ induktiv.*

Bevis. Først observerer vi at for hver $A \in \mathcal{A}$ så gir induktiviteten av A at $\emptyset \in A$. Det følger at $\emptyset \in \bigcap \mathcal{A}$, som viser (i) i Definisjon 4.1.

Deretter lar vi x være vilkårlig og antar at $x \in \bigcap \mathcal{A}$. La nå $A \in \mathcal{A}$ være vilkårlig. Siden $x \in \bigcap \mathcal{A}$, så er $x \in A$. Siden A er induktiv, følger det at $x \cup \{x\} \in A$. Siden $A \in \mathcal{A}$ var vilkårlig, slutter vi at $x \cup \{x\} \in \bigcap \mathcal{A}$. Siden x var vilkårlig, har vi altså vist (ii) i Definisjon 4.1. □

Proposisjon 4.3. *Følgende gjelder:*

(i) Følgende predikat i variabelen x er mengdebyggende:

$$P(x): \quad \forall I(I \text{ er induktiv } \Rightarrow\ x \in I). \tag{4.1}$$

(ii) Mengden

$$\{x : P(x)\}$$

er induktiv.

Bevis. Ved Aksiom 7 eksisterer det en induktiv mengde I_0. Definer

$$\mathcal{A} = \{I \in \mathcal{P}(I_0) : I \text{ er induktiv}\}.$$

Siden $I_0 \in \mathcal{A}$, er $\mathcal{A}$ ikke-tom. Definer $C = \bigcap \mathcal{A}$. Ved Lemma 4.2 er da C induktiv.

Vi viser nå at

$$\forall x(x \in C \Leftrightarrow P(x)).$$

La x være vilkårlig. Først antar vi at $x \in C$. For å vise $P(x)$, la I være en vilkårlig induktiv mengde. Da er $I \cap I_0$ induktiv ved Lemma 4.2, og $I \cap I_0 \in \mathcal{A}$. Siden $x \in C = \bigcap \mathcal{A}$, slutter vi at $x \in I \cap I_0$, så $x \in I$. Dette viser at $P(x)$ stemmer.

På den andre siden, anta at $P(x)$ stemmer. Vi vil vise at $x \in C$, så la $I \in \mathcal{A}$, altså er $I \in \mathcal{P}(I_0)$ være en induktiv mengde. Da får vi umiddelbart fra $P(x)$ at $x \in I$. Fra dette kan vi slutte at $x \in C$.

Vi har nå vist at $C = \{x : P(x)\}$, altså er predikatet $P(x)$ mengdebyggende. Dermed er (i) vist. Siden vi allerede har vist at C er induktiv, følger nå (ii). Dette fullfører beviset. □

Definisjon 4.4. Vi bruker notasjonen $\mathbb{N}$ for den induktive mengden

$$\mathbb{N} = \{x : \forall I(I \text{ er induktiv } \Rightarrow\ x \in I)\}.$$

Vi kaller elementene av denne mengden for *naturlige tall*. Videre definerer vi en funksjon $s\colon \mathbb{N} \to \mathbb{N}$ ved

$$s(n) = n \cup \{n\}, \quad n \in \mathbb{N}.$$

Denne funksjonen kaller vi *suksessor-funksjonen*.

Følgende aksiomer brukes ofte som utgangspunkt når man bygger opp de naturlige tallene.

Definisjon 4.5. La $(N, 0, s)$ være en trippel der

- N er en mengde,
- 0 er et element i N, og
- $s\colon N \to N$ er en funksjon.

Vi sier at $(N, 0, s)$ *tilfredsstiller Peano-aksiomene* dersom følgende holder:

(i) $\forall n \in N\,(s(n) \neq 0)$.
(ii) s er injektiv.

(iii) For enhver delmengde $A \subseteq N$ gjelder følgende: Dersom

$$0 \in A, \text{ og}$$
$$\forall n \in N\,(n \in A \;\Rightarrow\; s(n) \in A),$$

så må $A = N$.

Teorem 4.6. *Trippelet $(\mathbb{N}, \emptyset, s)$ tilfredsstiller Peano-aksiomene.*

Bevis. (i) La $n \in \mathbb{N}$. Vi har da at $n \in \{n\} \subseteq n \cup \{n\} = s(n)$, så $s(n) \neq \emptyset$, det vil si $s(n) \neq 0$.

(iii) La A være en delmengde som tilfredsstiller $0 \in A$ og $\forall n\,(n \in A \Rightarrow s(n) \in A)$. Da er A en induktiv mengde. Fra Proposisjon 4.3 har vi at $\mathbb{N} \subseteq A$. Vi konkluderer med at $A = \mathbb{N}$.

(ii) Vi viser først at $\bigcup s(n) = n$ for alle $n \in \mathbb{N}$ ved å bruke (iii). Definer

$$B = \{n \in \mathbb{N} : \bigcup s(n) = n\}.$$

- Merk at $\bigcup s(\emptyset) = \bigcup\{\emptyset\} = \emptyset$. Med andre ord er $\emptyset \in B$.
- La nå n være vilkårlig og anta at $n \in B$, det vil si $\bigcup s(n) = n$. Da får vi at

$$\bigcup s(s(n)) = \bigcup(s(n) \cup \{s(n)\}) = \Big(\bigcup s(n)\Big) \cup \Big(\bigcup\{s(n)\}\Big) = n \cup s(n) = s(n).$$

  I siste likhet brukte vi at $n \subseteq n \cup \{n\} = s(n)$. Dermed er $s(n) \in B$.

Dette viser at $B = \mathbb{N}$, altså at $\bigcup s(n) = n$ for alle $n \in \mathbb{N}$.

Vi kan nå vise at s er injektiv. Anta nemlig at $m, n \in \mathbb{N}$ tilfredsstiller $s(m) = s(n)$. Vi får da at

$$m = \bigcup s(m) = \bigcup s(n) = n.$$

Dette fullfører beviset. □

Merknad 4.7. Det tredje Peano-aksiomet (iii) forteller oss at induksjonsbevis er gyldig. La nemlig $P(n)$ være et predikat som vi har lyst til å bevise for alle $n \in \mathbb{N}$. Definer $A = \{n \in \mathbb{N} : P(n)\}$. La oss si at vi klarer å bevise de to følgende påstandene:

(i) $P(0)$.
(ii) $\forall n \in \mathbb{N}\,(P(n) \Rightarrow P(s(n)))$.

Vi har da vist at $0 \in A$ og $\forall n \in \mathbb{N}\,(n \in A \Rightarrow s(n) \in A)$. Ved (iii) kan vi da konkludere med at $A = \mathbb{N}$, altså at $P(n)$ stemmer for alle $n \in \mathbb{N}$.

Det første steget over kalles grunnsteget, mens det andre steget kalles induksjonssteget.

Proposisjon 4.8. *Vi har at*

$$\mathbb{N} = \{0\} \cup \mathrm{Im}(s).$$

Bevis. La $P(n)$ betegner predikatet

$$P(n): \quad n = 0 \;\vee\; (\exists m \in \mathbb{N}(n = s(m))).$$

Da stemmer $P(0)$. La så $n \in \mathbb{N}$ og anta at $P(n)$ stemmer. Da stemmer $P(s(n))$, siden $s(n) = s(m)$ der $m = n$. Dette viser utsagnet ved induksjon. □

Proposisjon 4.9. *La $(N, 0, s)$ og $(N', 0', s')$ være tripler som tilfredsstiller Peano-aksiomene. Da fins det en entydig funksjon $\phi\colon N \to N'$ slik at $\phi(0) = 0'$ og $\phi \circ s = s' \circ \phi$. Videre er ϕ bijektiv.*

Bevis. Gis som oppgave. □

4.2 Rekursjon

Definisjon 4.10. La A være en mengde. En *følge* i A er en funksjon $u\colon \mathbb{N} \to A$.

Notasjon 4.11. Når vi har en følge $u\colon \mathbb{N} \to A$, så skriver vi ofte $u_n = u(n)$ og betegner følgen som helhet med $u = (u_n)_{n\in\mathbb{N}}$ eller til og med

$$u = (u_0, u_1, u_2, \ldots).$$

Andre ganger ønsker vi imidlertid å betrakte u mer som en funksjon, og da vil vi bruke notasjon som understreker dette.

Teorem 4.12. *La (A, x, f) være en trippel der*

- *A er en mengde,*
- *$x \in A$, og*
- *$f\colon A \to A$ er en funksjon.*

Da fins det en unik funksjon $u\colon \mathbb{N} \to A$ slik at

$$\begin{aligned} u(0) &= x, \\ u \circ s &= f \circ u. \end{aligned}$$

Vi sier at u er rekursivt definert fra (A, x, f).

Merknad 4.13. Ofte vil vi betrakte funksjonen $u\colon \mathbb{N} \to A$ i Teorem 4.12 som en følge. Da vil egenskapene til u se slik ut:

$$\begin{aligned} u_0 &= x, \\ \forall n \in \mathbb{N} \quad u_{s(n)} &= f(u_n). \end{aligned}$$

Før vi beviser teoremet, ser vi på noen eksempler.

Eksempel 4.14. La oss betrakte mengden $\mathbb{N}$ selv med elementet $0 \in \mathbb{N}$ og suksessor-funksjonen $s\colon \mathbb{N} \to \mathbb{N}$. Trippelet $(\mathbb{N}, 0, s)$ gir da fra Teorem 4.12 en unik følge $(u_n)_{n\in\mathbb{N}}$ slik at

$$\begin{aligned} u_0 &= 0, \\ \forall n \in \mathbb{N} \quad u_{s(n)} &= s(u_n). \end{aligned}$$

Vi ser at følgen gitt ved $u_n = n$ for $n \in \mathbb{N}$ tilfredsstiller disse egenskapene. Ved entydigheten i Teorem 4.12 er det altså denne følgen $(u_n)_{n\in\mathbb{N}} = (n)_{n\in\mathbb{N}}$ rekursivt definert fra $(\mathbb{N}, 0, s)$.

Eksempel 4.15. La A være en mengde og la $x \in A$. Vi kan da betrakte trippelet (A, x, id_A). Den tilsvarende følgen $(u_n)_{n\in\mathbb{N}}$ i A er da karakterisert ved

$$\begin{aligned} u_0 &= x, \\ u_{s(n)} &= \mathrm{id}_A(u_n) = u_n. \end{aligned}$$

Vi ser at følgen gitt ved $u_n = x$ for alle $n \in \mathbb{N}$ tilfredsstiller disse egenskapene. Ved entydighet er det altså denne konstante følgen rekursivt definert fra (A, x, id_A).

Eksempel 4.16. La A være en mengde og la $f\colon A \to A$ være en funksjon. Vi kan definere en funksjon $T\colon A^A \to A^A$ gitt ved

$$T(g) = f \circ g, \quad g \in A^A.$$

Betrakt nå trippelet (A^A, id_A, T). Ved å bruke Teorem 4.12 får vi en følge $(f^n)_{n\in\mathbb{N}}$ av elementer i A^A slik at

$$f^0 = \mathrm{id}_A,$$
$$f^{s(n)} = T(f^n) = f \circ f^n.$$

Notasjonen vi velger er altså ingen tilfeldighet, for denne følgen svarer til iterert komposisjon.

Dersom vi $x \in A$ så får vi en følge $(f^n(x))_{n\in\mathbb{N}}$ i A ved å evaluere funksjonene f^n i x. Dersom vi setter $u_n = f^n(x)$, merker vi oss at

$$u_0 = f^0(x) = \mathrm{id}_A(x) = x,$$
$$u_{s(n)} = f^{s(n)}(x) = (f \circ f^n)(x) = f(f^n(x)) = f(u_n).$$

Men dette er nøyaktig egenskapene som følgen definert rekursivt fra (A, x, f) tilfredsstiller. Vi konkluderer med at denne følgen sammenfaller med $(f^n(x))_{n\in\mathbb{N}}$, og skal ofte bruke denne notasjonen.

Bevis. Beviset er langt, så vi deler det inn i seg.

Steg 1: Vi begynner med det letteste, nemlig entydigheten til u. La u og v være følger i A slik at

$$u_0 = x, \qquad \forall n \in \mathbb{N}\ \ u_{s(n)} = f(u_n),$$
$$v_0 = x, \qquad \forall n \in \mathbb{N}\ \ v_{s(n)} = f(v_n).$$

Vi beviser følgende påstand med induksjon:

$$Q(n): \quad u_n = v_n.$$

Først har vi at $u_0 = x = v_0$. Dette gir oss $Q(0)$.

La så $n \in \mathbb{N}$ være vilkårlig, og anta at $Q(n)$ holder, altså at $u_n = v_n$. Vi får da at

$$u_{s(n)} = f(u_n) = f(v_n) = v_{s(n)}.$$

Dette etablerer $Q(s(n))$.

Ved induksjon kan vi nå konkludere med at $Q(n)$ holder for alle $n \in \mathbb{N}$. Dette gir $u = v$.

Steg 2: Vi begynner nå beviset for eksistensen av u. Vi går tilbake til definisjonen av u som en trippel $u = (\mathbb{N}, A, R)$, se Definisjon 3.1, og begynner med å konstruere en kandidat for grafen R.

La oss kalle en delmengde $B \subseteq \mathbb{N} \times A$ *induktiv* dersom følgende holder:

- $(0, x) \in B$.
- $\forall\, (n, y) \in B\ \big(s(n), f(y)\big) \in B$.

La $\mathcal{A}$ betegne mengden av alle induktive delmengder av $\mathbb{N} \times A$. Siden $\mathbb{N} \times A$ er induktiv, er $\mathcal{A}$ ikke-tom. Definer

$$R = \bigcap \mathcal{A}.$$

Ved lignende argumentasjon som i beviset for Proposisjon 4.3 så vil R være en induktiv mengde (her overlater vi det altså til leseren å sjekke detaljene).

Steg 3: Definer nå

$$G = \{(0, x)\} \cup \{(s(n), f(y)) : (n, y) \in R\}.$$

I dette steget ønsker vi å vise at $G = R$.

For å se at $G \subseteq R$, så ser vi først at $(0, x) \in R$ siden R er induktiv. Videre, dersom $(n, y) \in R$, så følger det at $(s(n), f(y)) \in R$, igjen siden R er induktiv. Vi konkluderer med at $G \subseteq R$.

For å se at $R \subseteq G$, holder det å vise at G er induktiv. Siden R er snittet av alle induktive delmengder av $\mathbb{N} \times A$, vil det følge at $R \subseteq G$.

- Vi ser fra definisjonen av G at $(0, x) \in G$.
- Anta så at $(n, y) \in G$. Siden $G \subseteq R$, får vi at $(n, y) \in R$. Per definisjon av G har vi da at $(s(n), f(y))) \in G$.

Vi har nå vist at G er induktiv, og kan konkludere med at $R \subseteq G$. Dermed har vi etablert at $R = G$.

Steg 4: Vi må sjekke at R tilfredsstiller egenskapen i Definisjon 3.1 (iii). La $P(n)$ betegne predikatet

$$P(n): \quad \exists! z \in A\, ((n, z) \in R).$$

Vi ønsker altså å etablere $P(n)$ for alle $n \in \mathbb{N}$. Dette gjør vi med induksjon.

For grunnsteget $n = 0$ har vi at $(0, x) \in R$. Dette viser eksistens. Anta så at $(0, z) \in R$. Vi ønsker nå å vise at $z = x$. Fra likheten $R = G$ i Steg 3 får vi da to tilfeller:

- Dersom $(0, z) \in \{(0, x)\}$, får vi at $(0, z) = (0, x)$, som gir $z = x$.
- Dersom $(0, z) \in \{(s(n), f(y)) : (n, y) \in R\}$, får vi at det fins $(n, y) \in R$ slik at $0 = s(n)$ og $z = f(y)$. Førstnevnte er umulig fra første Peano-aksiom, så dette tilfellet kan ikke inntreffe.

Vi konkluderer med at $z = x$. Vi har dermed vist $P(0)$.

Så kommer induksjonssteget. Anta at $P(n)$ stemmer. Vi vil nå vise $P(s(n))$. Fra antagelsen om at $P(n)$ stemmer vet vi at det fins en entydig $w \in A$ slik at $(n, w) \in R$. Siden R er induktiv, følger det at $(s(n), f(w)) \in R$. Dette viser eksistensdelen av $P(n)$.

For å vise entydighetsdelen av $P(s(n))$, anta at $(s(n), z) \in R$. Bruker vi igjen $G = R$ fra Steg 3 så må $(s(n), z) = (s(m), f(y))$ for en $(m, y) \in R$. Dette gir $s(n) = s(m)$ og $z = f(y)$. Fra første Peano-aksiom vet vi at s er injektiv, så får vi at $m = n$. Men nå er $(n, w), (n, y) \in R$, så ved entydighetsdelen av induksjonshypotesen $P(n)$ kan vi konkludere med at $y = w$. Dermed får vi $z = f(y) = f(w)$. Dette fullfører entydighetsbeviset, og dermed beviset for $P(s(n))$.

Ved induksjon har vi nå vist at R er en gyldig graf.

Steg 5: I det aller siste steget skal vi vise at funksjonen $u = (\mathbb{N}, A, R)$ tilfredsstiller de ønskede egenskapene.

For det første vet vi at $(0, x) \in R$, så $u_0 = u(0) = x$.

La nå $n \in \mathbb{N}$. Vi vet da at $(n, u_n) \in R$. Siden R er induktiv, fås $(s(n), f(u_n)) \in R$. Men dette betyr at

$$u_{s(n)} = f(u_n).$$

Dermed har u den ønskede egenskapen. Dette fullfører beviset. □

Følgende er en mer generell versjon av Teorem 4.12 der vi kan la det neste elementet $u_{s(n)}$ i en følge avhenge ikke bare av det forrige leddet u_n, men også av indeksen n.

Proposisjon 4.17. *La (A, x, F) være en trippel der*

- *A er en mengde,*
- *$x \in A$, og*
- *$F\colon \mathbb{N} \times A \to A$ er en funksjon.*

Da fins det en unik følge $(u_n)_{n\in\mathbb{N}}$ i A slik at

$$\begin{aligned} u_0 &= x, \\ \forall n \in \mathbb{N}\ \ u_{s(n)} &= F(n, u_n). \end{aligned}$$

Bevis. Oppgave. □

Eksempel 4.18. Det fins en unik funksjon $p\colon \mathbb{N} \to \mathbb{N}$ slik at

$$\begin{aligned} p(0) &= 0, \\ \forall n \in \mathbb{N}\ \ p(s(n)) &= n. \end{aligned}$$

Denne funksjonen svarer altså til rekursjon for trippelet $(\mathbb{N}, 0, F)$ der $F\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ er gitt ved

$$F(n, m) = n.$$

4.3 Aritmetikk og litt algebra

I denne seksjonen skal vi introdusere grunnleggende aritmetikk med naturlige tall, altså addisjon og multiplikasjon. Vi skal samtidig introdusere algebraiske egenskaper i en mer generell kontekst.

Definisjon 4.19. La A være en mengde. Vi kaller en funksjon $+\colon A \times A \to A$ for en *binæroperasjon* på A. Gitt $a, b \in A$, så skriver vi gjerne $a + b$ for funksjonsverdien $+(a, b)$.

(i) Vi sier at $+$ er *assosiativ* dersom følgende gjelder for alle $a, b, c \in A$:

$$(a + b) + c = a + (b + c).$$

(ii) Vi sier at $+$ er *kommutativ* dersom følgende gjelder for alle $a, b \in A$:

$$a + b = b + a.$$

(iii) Vi sier at $0 \in A$ er et *nøytralt element* for $+$ dersom følgende gjelder for alle $a \in A$:

$$a + 0 = 0 + a = a.$$

(iv) Vi sier at $+$ er *kansellativ* dersom følgende implikasjoner gjelder for alle $a, b, c \in A$:

$$\begin{aligned} a + c = b + c &\implies a = b, \\ c + a = c + b &\implies a = b. \end{aligned}$$

Proposisjon 4.20. *La $+$ være en assosiativ binæroperasjon på A. Dersom det fins et nøytralt element for $+$, så er det unikt.*

Bevis. Anta at 0 og $0'$ er nøytrale elementer. Vi får da at

$$0 = 0 + 0' = 0'.$$

□

Addisjon

Definisjon 4.21. For hver $a \in \mathbb{N}$ lar vi $(a+)\colon \mathbb{N} \to \mathbb{N}$ være funksjonen rekursivt definert fra trippelet $(\mathbb{N}, a, s)$ i Teorem 4.12. Videre definerer vi en binæroperasjon $+$ på $\mathbb{N}$ ved

$$a + b = (a+)(b), \quad a, b \in \mathbb{N}.$$

Altså er $+$ karakterisert ved at følgende holder for alle $a, b \in \mathbb{N}$:

$$\begin{aligned} a + 0 &= a, \\ a + s(b) &= s(a + b). \end{aligned}$$

Vi kaller denne binæroperasjonen for *addisjon*.

Proposisjon 4.22. *Addisjon er en assosiativ, kommutativ og kansellativ binæroperasjon på* $\mathbb{N}$ *med* 0 *som nøytralt element.*

Bevis. La oss vise at $+$ er assosiativ. Vi lar $a, b \in \mathbb{N}$ og lar $P(c)$ betegnet utsagnet

$$P(c): \quad (a + b) + c = a + (b + c).$$

Vi beviser $P(c)$ ved induksjon.

Vi ser først at

$$(a + b) + 0 = a + b = a + (b + 0).$$

Dette viser at $P(0)$ stemmer.

Deretter lar vi $c \in \mathbb{N}$ og antar at $P(c)$ stemmer. Vi får da at

$$(a + b) + s(c) = s((a + b) + c) = s(a + (b + c)) = a + s(b + c) = a + (b + s(c)).$$

Dette viser at $P(s(c))$ stemmer. Vi konkluderer med at $P(c)$ stemmer for alle $c \in \mathbb{N}$. Med andre ord er addisjon assositativ.

Vi lar kommutativitet og nøytralitet av 0 være en oppgave.

La oss til slutt vise den ene kansellasjonsloven. Den andre følger siden addisjon er kommutativ. Vi lar a og b være naturlige tall og lar $Q(c)$ betegne utsagnet

$$Q(c): \quad a + c = b + c \implies a = b.$$

Vi begynner med å betrakte $Q(0)$, altså utsagnet $a + 0 = b + 0 \ \Rightarrow \ a = b$. Dette ser vi at stemmer.

La nå $c \in \mathbb{N}$ og anta at $Q(c)$ stemmer. Vi skal vise at $Q(s(c))$ også stemmer. Vi antar derfor at $a + s(c) = b + s(c)$. Per definisjon av addisjon får vi at

$$s(a + c) = a + s(c) = b + s(c) = s(b + c).$$

Siden s er injektiv, konkluderer vi med at $a + c = b + c$. Men da gir antagelsen $Q(c)$ at $a = b$. Dette fullfører beviset for $Q(s(c))$.

Vi har dermed bevist at kansellasjonsloven holder ved induksjon. □

En annen viktig egenskap addisjon av naturlige tall har er følgende:

Proposisjon 4.23. *La $a, b \in \mathbb{N}$. Da gjelder implikasjonen*

$$a + b = 0 \implies a = b = 0.$$

Bevis. Vi antar at $a + b = 0$. Ved Proposisjon 4.8 er $b \in \{0\} \cup \mathrm{Im}(s)$, så vi kan dele inn i to tilfeller:

- Dersom $b = 0$, får vi $a + 0 = 0$, altså også $a = 0$.
- Dersom det fins en $c \in \mathbb{N}$ slik at $b = s(c)$, så får vi at

$$s(a + c) = a + s(c) = a + b = 0.$$

  Dette motstrider det første Peano-aksiomet. Altså kan ikke dette tilfellet inntreffe.

Vi konkluderer med at $a = b = 0$. □

Multiplikasjon

Definisjon 4.24. La A være en mengde, og la $\cdot$ og $+$ være binæroperasjoner på A. Vi sier at $\cdot$ er *distributiv* over $+$ dersom følgende gjelder for alle $a, b, c \in A$:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Proposisjon 4.25. *La A være en mengde med en kansellativ binæroperasjon $+$ med nøytralt element 0. La $\cdot$ være en binæroperasjon på A som er distributiv over $+$. De gjelder følgende for alle $a \in A$:*

$$a \cdot 0 = 0 \cdot a = 0.$$

Bevis. La $a \in A$. Vi har at

$$(a \cdot 0) + 0 = a \cdot 0 = a \cdot (0 + 0) = (a \cdot 0) + (a \cdot 0).$$

Siden $+$ er kansellativ, konkluderer vi med at $a \cdot 0 = 0$. Et tilsvarende argument viser at $0 \cdot a = 0$. Vi overlater det som en oppgave. □

Definisjon 4.26. Gitt $a \in \mathbb{N}$ så lar vi $(a\cdot)\colon \mathbb{N} \to \mathbb{N}$ være funksjonen man får fra Teorem 4.12 via rekursjon med trippelet $(\mathbb{N}, 0, (a+))$. Videre definerer vi en binæroperasjon $\cdot$ på $\mathbb{N}$ ved

$$a \cdot b = (a\cdot)(b), \quad a, b \in \mathbb{N}.$$

Med andre ord er $\cdot$ karakterisert ved at følgende holder for alle $a, b \in \mathbb{N}$:

$$a \cdot 0 = 0,$$
$$a \cdot s(b) = a + a \cdot b.$$

Vi kaller denne binæroperasjonen for *multiplikasjon.*

Proposisjon 4.27. *Multiplikasjon på de naturlige tallene er en assosiativ og kommutativ binæroperasjon på $\mathbb{N}$ med 1 som nøytralt element. Videre er multiplikasjon distributiv over addisjon.*

Bevis. Vi viser først at multiplikasjon er distributiv over addisjon ved induksjon. Mer presist skal vi, gitt $a, b \in \mathbb{N}$, vise utsagnet

$$P(c): \quad a(b+c) = ab + ac$$

ved induksjon. Per definisjon har vi at $a0 = 0$. Dette gir

$$a(b+0) = ab = ab + 0 = ab + a0.$$

Dermed har vi vist $P(0)$.

La nå $c \in \mathbb{N}$ og anta at $P(c)$ holder, dvs. at $a(b+c) = ab+ac$. Vi får da, ved å bruke assosiativitet og kommutativitet av addisjon, at

$$a(b+s(c)) = as(b+c) = a + a(b+c) = a + (ab+ac) = ab + (a+ac) = ab + as(c).$$

Dette gir at $P(s(c))$ holder. Vi konkluderer med at $P(c)$ holder for alle $c \in \mathbb{N}$ ved induksjon.

Vi overlater identiteten $(a+b)c = ac + bc$ som en oppgave.

La oss nå bevise at multiplikasjon er assosiativ. Vi lar $a, b \in \mathbb{N}$ være gitt og beviser

$$Q(c): \quad (ab)c = a(bc)$$

ved induksjon. I grunnsteget har vi både $(ab)0 = 0$ og $a(b0) = a0 = 0$ Per definisjon av multiplikasjon. Dermed stemmer $Q(0)$.

Anta så at $c \in \mathbb{N}$ og at $Q(c)$ stemmer, altså at $(ab)c = a(bc)$. Vi ser da ved å bruke distributiviteten vi allerede har bevist at

$$(ab)s(c) = ab + (ab)c = ab + a(bc) = a(b+bc) = a(bs(c)).$$

Vi overlater beviset for at 1 er et nøytralt element, og beviset for at multiplikasjon er kommutativt, som en oppgave. □

Til slutt beviser vi kansellasjonsloven for multiplikasjon:

Proposisjon 4.28. *Følgende holder:*

(i) For alle $a, b \in \mathbb{N}$ har vi at

$$ab = 0 \implies (a = 0 \vee b = 0).$$

(ii) For alle $a, b, c \in \mathbb{N}$ der $c \neq 0$ har vi at

$$ca = cb \implies a = b.$$

Spesielt er multiplikasjon på $\mathbb{N} \setminus \{0\}$ en kansellativ binæroperasjon.

Bevis. (i) La $a, b \in \mathbb{N}$ og anta at $ab = 0$. Fra Proposisjon 4.8 så vet vi en av to tilfeller inntreffer:

- I det første tilfellet er $b = 0$. Da har vi at $a = 0 \ \vee \ b = 0$, hvilket fullfører beviset.
- I det andre tilfellet er $b = s(c)$ for en eller annen $c \in \mathbb{N}$. Da er

  $$ab = as(c) = a + ac = 0.$$

  Dermed gir Proposisjon 4.23 at $a = 0$. Vi har altså oppnådd ønsket konklusjon i dette tilfellet også.

(ii) Fikser $c \in \mathbb{N} \setminus \{0\}$. Vi skal bevise utsagnet

$$P(b): \quad \forall a \in \mathbb{N}\,(ca = cb \implies a = b).$$

For å bevise $P(0)$ lar vi $a \in \mathbb{N}$ og antar at $ca = c0 = 0$. Da gir (i) at enten $c = 0$ eller $a = 0$. Siden $c \neq 0$, konkluderer vi med at $a = 0$. Dette viser $P(0)$.

Anta nå at $b \in \mathbb{N}$ er slik at $P(b)$ stemmer. For å vise $P(s(b))$ lar vi $a \in \mathbb{N}$ og antar at $ca = cs(b)$. Siden $c \neq 0$ og $s(b) \neq 0$ gir (i) at $cs(b) \neq 0$. Dermed er $ca \neq 0$, så $a \neq 0$. Ve Proposisjon 4.8 fins det en $d \in \mathbb{N}$ slik at $s(d) = a$. Vi kan da skrive

$$c + cd = cs(d) = ca = cs(b) = c + cb.$$

Siden addisjon er kansellativ, konkluderer vi med $cd = cb$. Vi kan da endelig bruke induksjonshypotesen og konkludere med at $d = b$. Dette gir $a = s(d) = s(b)$. Dermed har vi vist $P(s(b))$. Dette fullfører beviset. □

Vi definerer også potenser rekursivt.

Definisjon 4.29. La $a \in \mathbb{N} \setminus \{0\}$. Vi bruker Teorem 4.12 til å definere a^n rekursivt ved

$$a^0 = 1,$$
$$\forall n \in \mathbb{N} \;\; a^{s(n)} = a^n \cdot a.$$

Proposisjon 4.30. *La $a, b \in \mathbb{N} \setminus \{0\}$ og $m, n \in \mathbb{N}$. Da gjelder*

$$(ab)^n = a^n b^n, \tag{4.2}$$
$$a^{m+n} = a^m \cdot a^n, \tag{4.3}$$
$$(a^m)^n = a^{m \cdot n}. \tag{4.4}$$

Bevis. Oppgave. □

Kapittel 5

Relasjoner

Dette kapittelet omhandler relasjoner og følger kapittel 5 i [1] ganske tett. Vi skal i tillegg innføre ordensrelasjonen på de naturlige tallene i dette kapittelet, og konstruere heltallene og de rasjonale tallene. Merk at konstruksjonen av heltallene ble gjort allerede i 3.3 i [1], og konstruksjonen der er en annen enn den vi skal presentere. Rasjonale tall blir vel aldri direkte konstruert i [1], så vi skal ikke bruke veldig mye tid på det.

Vi skal gjøre noen induksjonsbevis i dette kapittelet, og vi begynner å skrive $a + 1$ istedenfor $s(a)$ for $a \in \mathbb{N}$.

5.1 Grunnleggende begreper

Definisjon 5.1. La A være en mengde. En *relasjon* på A er en delmengde av $A \times A$.

Notasjon 5.2. La $\triangle$ være en relasjon på en mengde A. Vi bruker notasjonen $x \triangle y$ i stedet for $(x, y) \in \triangle$. Generelt tenker vi på relasjonen som et predikat $x \triangle y$ av to variable x og y som tilhører mengden A, og vi skal som regel definere relasjoner ved å karakterisere predikatet $x \triangle y$. Gitt $x, y \in A$ slik at utsagnet $x \triangle y$ holder, så sier vi at x er relatert til y (via $\triangle$).

Eksempel 5.3. For enhver mengde A har vi to relasjoner i hver sin ekstreme retning: Den indiskrete relasjonen gitt ved $\triangle = A \times A$, og den diskrete relasjonen gitt ved $\triangle' = \{(x, x) : x \in A\}$. I notasjonen vi skal bruke hovedsakelig har vi altså at den indiskrete relasjonen er karakterisert ved

$$\forall x \in A \;\; x \triangle y,$$

mens den diskrete relasjonen er karakterisert ved

$$\forall x \in A \;\; (x \triangle' y \quad \iff \quad x = y).$$

Den diskrete relasjonen på A kan vi altså tenke på som likhetsrelasjonen mellom elementer i A.

Definisjon 5.4. Vi kaller en relasjon $\triangle$ på en mengde A for

(i) *refleksiv* dersom

$$\forall x \in A \quad x \triangle x.$$

(ii) *symmetrisk* dersom

$$\forall x, y \in A \quad (x \triangle y \implies y \triangle x).$$

(iii) *anti-symmetrisk* dersom

$$\forall x, y \in A \;\; \Big((x \triangle y \;\wedge\; y \triangle x) \implies x = y \Big).$$

(iv) *transitiv* dersom

$$\forall x, y, z \in A \ \Big((x \triangle y \ \wedge \ y \triangle z) \implies x \triangle z \Big).$$

Legg merke til at den diskrete relasjonen på en mengde A er refleksiv, symmetrisk og transitiv. Videre er den indiskrete relasjonen den entydige relasjonen på A som er refleksiv, symmetrisk, og antisymmetrisk.

Eksempel 5.5. Gitt en relasjon $\triangle$ på en mengde A, så kan vi alltids definere en relasjon $\triangle^{\text{op}}$ på A ved

$$\forall x, y \in A \, (x \triangle^{\text{op}} y \quad \iff \quad y \triangle x).$$

Dette kalles for den *motsatte relasjonen* av $\triangle$. Vi merker oss at dersom $\triangle$ har en eller flere av egenskapene i Definisjon 5.4, så vil $\triangle^{\text{op}}$ ha de tilsvarende egenskapene.

5.2 Ordensrelasjoner

Definisjon 5.6. Vi kaller en relasjon for en *ordensrelasjon* (eller *partiell ordning*) dersom den er refleksiv, transitiv og antisymmetrisk. Dersom A er en mengde og $\leq$ er en ordensrelasjon på A, så kaller vi paret $(A, \leq)$ for en *ordnet mengde*.

Vi bruker ofte symboler som $\leq$, $\preceq$, og lignende, for ordensrelasjoner.

Eksempel 5.7. La A være en mengde og betrakt relasjonen $\subseteq$ på $\mathcal{P}(A)$, altså delmengden

$$\{(U, V) \in \mathcal{P}(A) \times \mathcal{P}(A) : U \subseteq V\}$$

av $\mathcal{P}(A) \times \mathcal{P}(A)$. Da er $\subseteq$ en ordensrelasjon. Dette bunner i identitetene fra Proposisjon 2.3.

Eksempel 5.8. La $(A, \leq)$ være en ordnet mengde, og la $B \subseteq A$. Vi definerer en relasjon $\leq_B$ på B ved at

$$\forall x, y \in B \quad (x \leq_B y \quad \iff \quad x \leq y).$$

Da er $\leq_B$ en ordensrelasjon på B, så $(B, \leq_B)$ er en ordnet mengde. Vi kommer som oftest til å droppe indeksen B i $\leq_B$ og bare skrive $\leq$ for ordensrelasjonen på B også. Denne kalles gjerne for *restriksjonen* av $\leq$ til B.

Proposisjon 5.9. *Relasjonen $\leq$ på $\mathbb{N}$ gitt ved*

$$a \leq b \quad \iff \quad \exists c \in \mathbb{N} \, (a + c = b),$$

er en ordensrelasjon.

Bevis. Refleksivitet: La $a \in \mathbb{N}$. Siden $a + 0 = a$, ser vi fra definisjonen at $a \leq a$.

Antisymmetri: La $a, b \in \mathbb{N}$ og anta at $a \leq b$ og $b \leq a$. Det fins da $u, v \in \mathbb{N}$ slik at $a + c = b$ og $b + d = a$. Dette gir

$$a + (c + v) = (a + c) + d = b + d = a.$$

Kansellasjonsloven for addisjon gir da at $b + d = 0$. Ved å bruke Proposisjon 4.23 slutter vi at $b = d = 0$. Dermed har vi at $a = b$.

Transitivitet: La $a, b, c \in \mathbb{N}$ og anta at $a \leq b$ og $b \leq c$. Per definisjon fins det da $u, v \in \mathbb{N}$ slik at

$$a + u = b,$$
$$b + v = c.$$

Vi får da at

$$a + (u + v) = (a + u) + v = b + v = c.$$

Dette viser at $a \leq c$. □

Vi kommer alltid til å betrakte $\mathbb{N}$ som en ordnet mengde $(\mathbb{N}, \leq)$ med ordensrelasjonen definert i Proposisjon 5.9.

Notasjon 5.10. Dersom $\leq$ er en ordensrelasjon på en mengde A, så vet vi fra Eksempel 5.5 at den motsatte relasjonen også er en ordensrelasjon. Denne betegner vi med $\geq$. Vi har tilsvarende symboler for andre relasjoner, f.eks. $\preceq$ svarer til $\succeq$, $\subseteq$ svarer til $\supseteq$, også videre.

I tillegg definerer vi for alle $x, y \in A$ at

$$x < y \quad \iff \quad (x \leq y \ \wedge x \neq y),$$

og $x > y$ hvis og bare hvis $y < x$.

Proposisjon 5.11. *De følgende egenskapene holder for ordensrelasjonen på de naturlige tallene:*

(i) For alle $a \in \mathbb{N}$ gjelder

$$a \geq 0.$$

(ii) For alle $a, b, c \in \mathbb{N}$ gjelder

$$a \leq b \quad \iff \quad a + c \leq b + c.$$

(iii) For alle $a, b, c \in \mathbb{N}$ gjelder

$$a \leq b \quad \implies \quad ac \leq bc.$$

Dersom $c > 0$, gjelder også den motsatte implikasjonen.

(iv) For alle $a, b \in \mathbb{N}$ gjelder

$$a < b \quad \iff \quad a + 1 \leq b.$$

Bevis. Vi beviser (iv) og overlater resten som en oppgave.

La $a, b \in \mathbb{N}$. Anta først at $a < b$. Da gjelder $a \neq b$ og $a \leq b$. Sistnevnte gir en $c \in \mathbb{N}$ slik at $a + c = b$. Fra Proposisjon 4.8 har vi to tilfeller: Enten så er $c = 0$ eller så er $c \in \mathrm{Im}(s)$. I det første tilfellet får vi $a = a + 0 = b$, som motsiger $a \neq b$. Dermed konkluderer vi med at det fins en $c' \in \mathbb{N}$ slik at $c = c' + 1$. Da får vi at

$$b = a + c = a + (c' + 1) = (a + 1) + c'.$$

Dette gir $a + 1 \leq b$.

På den andre siden, anta at $a + 1 \leq b$. Siden $a \leq a + 1$, gir transitivitet at $a \leq b$. For å vise at $a \neq b$, anta for en selvmotsigelse at $a = b$. Vi får da at $a + 1 \leq a$, som ved antisymmetri gir $a + 1 = a$. Dette gir $1 = 0$ ved kansellasjon, en selvmotsigelse. Derfor må $a \neq b$. Vi konkluderer med at $a < b$. □

Definisjon 5.12. Vi sier at en ordensrelasjon $\leq$ på en mengde A er *total* dersom

$$\forall x, y \in A \quad (x \leq y \ \vee \ y \leq x).$$

I så fall sier vi at $(A, \leq)$ er en *totalt ordnet mengde*.

Eksempel 5.13. Ordensrelasjonen $\subseteq$ på $\mathcal{P}(A)$ fra Eksempel 5.7 er generelt ikke total. La for eksempel $A = \{0, 1\}$, $U = \{0\}$ og $V = \{1\}$. Da stemmer det hverken at $U \subseteq V$ eller $V \subseteq U$.

Proposisjon 5.14. *Ordensrelasjonen på de naturlige tallene er total.*

Bevis. Definer følgende predikat:

$$P(a): \quad \forall b \in \mathbb{N}\ (a \leq b\ \vee\ b \leq a).$$

Vi beviser $P(a)$ for alle $a \in \mathbb{N}$ ved induksjon. Siden $b \geq 0$ for alle $b \in \mathbb{N}$ ved Proposisjon 5.11 (i), har vi at $P(0)$ stemmer.

La nå $a \in \mathbb{N}$ og anta at $P(a)$ stemmer. La $b \in \mathbb{N}$. Ved Proposisjon 4.8 har vi to tilfeller:

- I det ene tilfellet er $b = 0$. Da vet vi at $a + 1 \geq 0 = b$, igjen ved Proposisjon 5.11 (i).
- I det andre tilfellet fins det en $c \in \mathbb{N}$ slik at $b = c + 1$. Ved å bruke induksjonsantagelsen $P(a)$ får vi to videre tilfeller:
  - I det ene tilfellet gjelder $a \leq c$. Da gir Proposisjon 5.11 (iv) at

    $$a + 1 \leq c + 1 = b.$$

  - I det andre tilfellet gjelder $a \geq c$. Da gir Proposisjon 5.11 (iv) at

    $$a + 1 \geq c + 1 = b.$$

  I hvert tilfellet oppnår vi altså at utsagnet $a + 1 \leq b \vee a + 1 \geq b$ stemmer.

Siden $b \in \mathbb{N}$ var vilkårlig, kan vi slutte at $P(a+1)$ stemmer. Dette fullfører induksjonsbeviset. □

Merknad 5.15. Legg merke til at dersom $(A, \leq)$ er en totalt ordnet mengde, så vil for ethvert par $x, y \in A$ nøyaktig ett av de tre følgende utsagnene gjelde:

- $x < y$.
- $x = y$.
- $x > y$.

Vi kan se dette som følger: Dersom $x \leq y$, så gjelder enten $x = y$ eller $x < y$, og dersom $x \geq y$, så gjelder enten $x = y$ eller $x > y$. Videre kan ikke $x < y$ og $x = y$ eller $x > y$ og $x = y$ gjelde samtidig per definisjon, og dersom $x < y$ og $x > y$ gjelder samtidig, får vi $x = y$, som igjen er en selvmotsigelse.

Definisjon 5.16. La $(A, \leq)$ være en ordnet mengde, og la $a \in A$. Da kaller vi a et

- *minste element* eller *minimum* dersom

  $$\forall x \in A\ (a \leq x),$$

- *største element* eller *maksimum* dersom

  $$\forall x \in A\ (a \geq x),$$

- *minimalt element* dersom

  $$\forall x \in A\ (x \leq a \implies x = a).$$

- *maksimalt element* dersom

  $$\forall x \in A\ (x \geq a \implies x = a).$$

Proposisjon 5.17. *La $(A, \leq)$ være en ordnet mengde.*

(i) Dersom A har et minste element, så er det unikt. Vi betegner det med $\min A$. *Videre er ethvert minimalt element lik* $\min A$.

(ii) Dersom A har et største element, så er det unikt. Vi betegner det med $\max A$. *Videre er ethvert maksimalt element lik* $\max A$.

Dersom $(A, \leq)$ er totalt ordnet, er ethvert minimalt element et minste element, og ethvert maksimalt element er et største element.

Bevis. (i) La $a, a' \in A$ begge være minste elementer. Da gjelder både $a \leq a'$ og $a' \leq a$. Fra antisymmetri konkluderer vi med at $a = a'$.

La $b \in A$ være minimalt og anta at A har et minste element. Siden $\min A \leq b$, får vi per definisjon at $\min A = b$.

(ii) Argumentene er tilsvarende.

Anta til slutt at $(A, \leq)$ er total og at $a \in A$ er minimal. La $x \in A$. Da gjelder $x \leq a$ eller $a \leq x$. I førstnevnte tilfellegir minimalitet av a at $x = a$, så vi har spesielt at $a \leq x$. Derfor får vi at $a \leq x$ i begge tilfellene. Vi konkluderer derfor med at $a = \min A$. □

Eksempel 5.18. La A være en mengde og betrakt den ordnede mengden $(\mathcal{P}(A), \subseteq)$ der $\subseteq$ betegner inklusjonsrelasjonen på $\mathcal{P}(A)$. Da har $\mathcal{P}(A)$ både et minste element og et største element, og de er gitt ved henholdsvis

$$\min \mathcal{P}(A) = \emptyset, \qquad \max \mathcal{P}(A) = A.$$

La oss heller betrakte $\mathcal{A} = \mathcal{P}(A) \setminus \{\emptyset\}$ med den restikterte ordenen fra $\mathcal{P}(A)$ som i Eksempel 5.8. Da er hver ettpunktsmengde minimal: La nemlig $x \in A$, la $B \in \mathcal{A}$ være vilkårlig og anta at $B \subseteq \{x\}$. Generelt gir dette $B = \emptyset$ eller $B = \{x\}$, men siden $B \in \mathcal{A}$ er $B \neq \emptyset$, så $B = \{x\}$. Dette viser at $\{x\}$ er minimal. Et ekstra argument viser at de minimale elementene er nøyaktig ettpunktsmengdene.

Videre har $\mathcal{A}$ inget minste element dersom A har minst to ulike elementer x og y: Dersom $B \in \mathcal{A}$ hadde vært et minste element, ville vi fått både $B \subseteq \{x\}$ og $B \subseteq \{y\}$, men dette er ikke mulig dersom $B \neq \emptyset$.

I eksempelet over betraktet vi minste elementer for den restrikterte ordenen til en delmengde Generelt innfører vi følgende terminologi dersom $(A, \leq)$ er en ordnet mengde og $B \subseteq A$. Vi sier at $b \in A$ er *minste element i* B dersom $b \in B$ og b er minste element med hensyn på $(B, \leq_B)$. Vi innfører tilsvarende terminologi for største element, og minimale og maksimale elementer.

Eksempel 5.19. Vi betrakter $\mathbb{N}$ med sin naturlige ordning. Da har $\mathbb{N}$ et minste element, nemlig 0, siden vi vet at $0 \leq a$ for alle $a \in \mathbb{N}$ fra Proposisjon 5.11 (i). Derimot har $\mathbb{N}$ inget største element: Anta nemlig at det fins en $a \in \mathbb{N}$ slik at $n \leq a$ for alle $n \in \mathbb{N}$. Setter vi $n = a + 1$ får vi at $a + 1 \leq a$, en umulighet.

Følgende er et nøkkelresultat for ordenen på de naturlige tallene.

Teorem 5.20 (Velordningsprinsippet)**.** *Enhver ikke-tom mengde $A \subseteq \mathbb{N}$ har et minste element.*

Bevis. La $A \subseteq \mathbb{N}$ være ikke-tom og anta for en selvmotsigelse at A ikke har noe minste element. La $P(n)$ betegne predikatet

$$P(n): \quad \forall a \in A \ (n \leq a).$$

Siden $0 \leq a$ for alle $a \in A$, har vi at $P(0)$ er sant.

La nå $n \in \mathbb{N}$ og anta $P(n)$. Da må $n \notin A$, for ellers ville n være minste element for A. Dermed gjelder $n < a$ for alle $a \in A$. Ved Proposisjon 5.11 (iv) får vi at $n + 1 \leq a$ for alle $a \in A$. Dette beviset $P(n + 1)$.

Ved induksjon kan vi nå konkludere med at $P(n)$ stemmer for alle $n \in \mathbb{N}$. Siden A er ikke-tom kan vi la $a \in A$, og da må $P(a + 1)$ stemme, så $a + 1 \leq a$. Ved Proposisjon 5.11 (iv) er dette ekvivalent med at $a < a$, en selvmotsigelse. Vi konkluderer derfor med at alle ikke-tomme delmengder av $\mathbb{N}$ har et minste element. □

Definisjon 5.21. La $(A, \leq)$ være en ordnet mengde, la $B \subseteq A$ og la $a \in A$. Vi har følgende definisjoner:

- a er en *nedre skranke for* B dersom $a \leq b$ for alle $b \in B$, og vi kaller B for *nedad begrenset* dersom det fins en nedre skranke for B.
- a er en *øvre skranke for* B dersom $a \geq b$ for alle $b \in B$, og vi kaller B for *oppad begrenset* dersom det fins en øvre skranke for B.

Videre har vi følgende:

- Dersom mengden av nedre skranker for B har et største element, skriver vi

  $$\inf B = \max\{a \in A : a \text{ er en nedre skranke for } B\}$$

  og kaller dette elementet for infimum av B.
- Dersom mengden av øvre skranker for B har et minste element, skriver vi

  $$\sup B = \min\{a \in A : a \text{ er en øvre skranke for } B\}$$

  og kaller dette elementet for supremum av B.

Eksempel 5.22. La A være en mengde. Vi betrakter den ordende mengden $(\mathcal{P}(A), \subseteq)$ der $\mathcal{P}(A)$ er ordnet med inklusjon.

La $\mathcal{B} \subseteq \mathcal{P}(A)$ være ikke-tom. En nedre skranke for $\mathcal{B}$ er en mengde $C \subseteq A$ slik at $C \subseteq B$ for alle $B \in \mathcal{B}$. Dette betyr nøyaktig at $C \subseteq \bigcap \mathcal{B}$. Spesielt er $\bigcap \mathcal{B}$ en nedre skranke for $\mathcal{B}$. Siden $C \subseteq \bigcap \mathcal{B}$ for alle nedre skranker C for $\mathcal{B}$, ser vi at $\bigcap \mathcal{B}$ er infimum for $\mathcal{B}$, altså har vi at

$$\inf \mathcal{B} = \bigcap \mathcal{B}.$$

Analogt kan man vise at

$$\sup \mathcal{B} = \bigcup \mathcal{B}.$$

Proposisjon 5.23. *La $(A, \leq)$ være en ordnet mengde. Da gjelder følgende:*

(i) B har et minimum hvis og bare hvis B har et infimum og $\inf B \in B$. I så fall er $\min B = \inf B$.

(ii) B har et maksimum hvis og bare hvis B har et supremum og $\sup B \in B$. I så fall er $\max B = \sup B$.

Bevis. Oppgave. □

5.3 Ekvivalensrelasjoner

Definisjon 5.24. Vi kaller en relasjon for en *ekvivalensrelasjon* dersom den er refleksiv, symmetrisk og transitiv.

Vi betegner ofte ekvivalensrelasjoner med symbolet $\sim$ eller lignende.

Eksempel 5.25. Som vi har sett er både den diskrete og den indiskrete relasjonen på A ekvivalensrelasjoner.

Vi tenker på en ekvivalensrelasjon på en mengde A som en måte å identifisere elementer i A på. Vi skal se i denne seksjonen at vi kan gjøre denne ideen formell ved konseptet om en *kvotientmengde*.

Definisjon 5.26. La $\sim$ være en ekvivalensrelasjon på en mengde A. La $x \in A$. Da kaller vi mengden

$$[x] = \{y \in A : y \sim x\}$$

for *ekvivalensklassen* til x. Videre kaller vi

$$A/\sim \ = \{[x] : x \in A\}$$

for *kvotienten av A med hensyn på $\sim$*. Funksjonen

$$p\colon A \to A/\sim$$

gitt ved

$$p(x) = [x], \quad x \in A,$$

kalles for den *kvotientfunksjonen* av A ned på $A/\sim$.

Lemma 5.27. *La $\sim$ være en ekvivalensrelasjon på en mengde A, og la $x, y \in A$. Da er følgende ekvivalent:*

(i) $x \sim y$.
(ii) $x \in [y]$.
(iii) $y \in [x]$.
(iv) $[x] = [y]$.

Bevis. Vi har per definisjon at $x \in [y]$ hvis og bare hvis $x \sim y$, og at $y \in [x]$ hvis og bare hvis $y \sim x$. Siden $\sim$ er symmetrisk, viser dette at (i), (ii) og (iii) er ekvivalente.

Vi viser nå at (i) er ekvivalent med (iv). Anta først at $x \sim y$. Vi skal vise at $[x] = [y]$. La $z \in A$. Dersom $z \in [x]$, får vi at $z \sim x$. Transitivitet gir nå $z \sim y$, så $z \in [y]$. Dette viser at $[x] \subseteq [y]$.

I motsatt retning, anta at $z \in [y]$. Dette gir $z \sim y$. Symmetri gir at $y \sim x$. Nå gir transitivitet at $z \sim x$. Dermed er $z \in [x]$. Dette viser at $[y] \subseteq [x]$. Vi kan dermed konkludere med at $[x] = [y]$.

Til slutt antar vi at $[x] = [y]$. Siden $x \in [x]$, får vi at $x \in [y]$. Da gjelder $x \sim y$. Dette viser at (i) og (iv) er ekvivalente. Beviset er dermed ferdig. □

Vi har altså at $x \sim y$ hvis og bare hvis $[x] = [y]$. I mengden $A/\sim$ har elementene som representerer x og y dermed "blitt like" i kvotientmengden. Derfor tenker vi på kvotientmengden som en konstruksjon som forvandler $\sim$ om til faktisk likhet.

Eksempel 5.28. La oss se hvordan ekvivalensklasser og kvotientmengden blir seende ut for den diskrete og den indiskrete ekvivalensrelasjonen.

La A være en mengde og la $\sim$ betegne den indiskrete relasjonen, altså der $x \sim y$ for alle $x, y \in A$. Da er ekvivalensklassen til et element $x \in A$ gitt ved

$$[x] = \{y \in A : y \sim x\} = A.$$

Dermed blir $A/\sim = \{A\}$ dersom $A \neq \emptyset$. Dersom $A = \emptyset$ får vi at $A/\sim = \emptyset$.

I den andre enden betrakter vi den diskrete relasjonen, som vi bare betegner med likhetstegnet $=$. Da er

$$[x] = \{y \in A : y = x\} = \{x\}.$$

Dermed blir $A/\sim = \{\{x\} : x \in A\}$.

Vi innfører nå et viktig begrep, nemlig partisjoner av en mengde.

Definisjon 5.29. La A være en mengde. En *partisjon* av A er en mengde $\mathcal{A} \subseteq \mathcal{P}(A)$ som har følgende egenskaper:

(i) $\emptyset \notin \mathcal{A}$.
(ii) $\mathcal{A}$ er *parvis disjunkt*, altså for alle $B, C \in \mathcal{A}$ med $B \neq C$ så gjelder $B \cap C = \emptyset$.
(iii) $\mathcal{A}$ *dekker* A, det vil si $\bigcup \mathcal{A} = A$.

Vi ser at en partisjon $\mathcal{A}$ av A har følgende egenskap:

$$\forall x \in A \; \exists! B \in \mathcal{A} \quad (x \in B).$$

For (iii) gir nemlig eksistens, og (ii) gir entydigheten: Dersom $B, B' \in \mathcal{A}$ er slik at $x \in B$ og $x \in B'$, så er $B \cap B' \neq \emptyset$, og dermed $B = B'$.

Følgende eksempel viser at en ekvivalensrelasjon på A alltid gir oppgav til en partisjon av A.

Eksempel 5.30. La A være en mengde og la $\sim$ være en ekvivalensrelasjon på A. Da er $A/\sim$ en partisjon av A:

(i) Ethvert element at $A/\sim$ er på formen $[x]$ for en $x \in A$. Siden $x \in [x]$ ved refleksivitet, følger det at $\emptyset \notin A/\sim$.
(ii) La $B, C \in A/\sim$. Vi kan da finne $x, y \in A$ slik at $B = [x]$ og $C = [y]$. Dersom vi antar at $B \cap C \neq \emptyset$, så kan vi finne $z \in A$ slik at $z \in [x] \cap [y]$. Vi har dermed at $z \sim x$ og $z \sim y$. Symmetri gir $x \sim z$, og transitivitet gir $x \sim y$. Dermed er $[x] = [y]$ ved Lemma 5.27.
(iii) For enhver $x \in A$ har vi at $x \in [x]$ og $[x] \in A/\sim$. Dermed er $\bigcup A/\sim = A$.

Det neste eksempelet viser at vi også kan gå fra en partisjon av A til en ekvivalensrelasjon på A.

Eksempel 5.31. La A være en mengde og la $\mathcal{A}$ være en partisjon av A. Definer en relasjon $\sim_{\mathcal{A}}$ på A via

$$x \sim_{\mathcal{A}} y \quad \iff \quad \exists B \in \mathcal{A} \, (x, y \in B).$$

Da er $\sim_{\mathcal{A}}$ en ekvivalensrelasjon på A:

(i) Refleksivitet: La $x \in A$. Siden $\mathcal{A}$ dekker A, fins det en $B \in \mathcal{A}$ slik at $x \in B$. Vi har da at $x \sim_{\mathcal{A}} x$.
(ii) Symmetri: Anta at $x \sim_{\mathcal{A}} y$. Da fins det en $B \in \mathcal{A}$ slik at $x, y \in B$. Siden dette trivielt er det samme som å si at $y, x \in B$, får vi at $y \sim_{\mathcal{A}} x$.
(iii) Transitivitet: Anta at $x \sim_{\mathcal{A}} y$ og $y \sim_{\mathcal{A}} z$. Vi får da at det fins $B, C \in \mathcal{A}$ slik at $x, y \in B$ og $y, z \in C$. Siden $y \in B \cap C$ må vi konkludere med at $B = C$, siden $\mathcal{A}$ er en partisjon. Dermed får vi $x, z \in B = C$, så $x \sim_{\mathcal{A}} z$.

Følgende teorem viser at de to eksemplene over danner en én-til-én-korrespondanse mellom ekvivalensrelasjonene på en gitt mengde A og partisjonene av A.

Teorem 5.32. *La A være en mengde, la $\mathrm{Eq}(A)$ betegne mengden av ekvivalensrelasjoner på A og la $\mathrm{Part}(A)$ betegne mengden av partisjoner av A. Da er funksjonen*

$$\Phi\colon \mathrm{Eq}(A) \to \mathrm{Part}(A)$$

gitt ved

$$\Phi(\sim) = A/\sim$$

en bijeksjon. Inversen $\Psi\colon \mathrm{Part}(A) \to \mathrm{Eq}(A)$ til Φ er gitt ved $\Psi(\mathcal{A}) = \sim_{\mathcal{A}}$, der $\sim_{\mathcal{A}}$ er som definert i Eksempel 5.31.

Bevis. Først viser vi at $\Psi \circ \Phi = \mathrm{id}_{\mathrm{Eq}(A)}$. La $\sim$ være en ekvivalensrelasjon på A og sett $\mathcal{A} = A/\sim$. Vi må vise at $\sim_{\mathcal{A}} = \sim$. La $x, y \in A$. Da har vi følgende:

- Dersom $x \sim y$, er $x, y \in [x]$, så $x \sim_{\mathcal{A}} y$.
- Dersom $x \sim_{\mathcal{A}} y$, fins en $B \in \mathcal{A}$ slik at $x, y \in B$. La $z \in A$ være slik at $B = [z]$. Vi får da at $x \sim z$ og $x \sim y$, så $x \sim y$ ved symmetri og transitivitet.

Dette viser at $x \sim y$ hvis og bare hvis $x \sim_{\mathcal{A}} y$. Siden x og y var vilkårlige, viser dette at $\sim_{\mathcal{A}} = \sim$.

Nå viser vi at $\Phi \circ \Psi = \mathrm{id}_{\mathrm{Part}(A)}$. La $\mathcal{A}$ være en partisjon av A og sett $\sim = \sim_{\mathcal{A}}$. La $B \subseteq A$.

- Anta først at $B \in \mathcal{A}$. Siden $\mathcal{A}$ er en partisjon, fins det en $x \in B$. Vi påstår nå at $B = [x]$, ekvivalensklassen under relasjonen $\sim$. For å vise dette, merk at $y \in B$ hvis og bare hvis $x, y \in B$, hvis og bare hvis $x \sim y$, hvis og bare hvis $y \in [x]$. Siden $B = [x]$, har vi etablert at $B \in A/\sim$.
- Anta så at $B \in A/\sim$. Da fins det en $x \in A$ slik at $B = [x]$. La $B' \in \mathcal{A}$ være slik at $x \in B'$. Vi påstår at $B = B'$: La nemlig $y \in A$. Vi får da at $y \in B$ hvis og bare hvis $y \sim x$, hvis og bare hvis $y \in B'$. Vi har dermed vist at $B = B' \in \mathcal{A}$.

Vi har nå vist at $A \in A/\sim$ hvis og bare hvis $A \in \mathcal{A}$. Vi konkluderer med at $A/\sim = \mathcal{A}$. □

Veldefinerthet

I mange sammenhenger kommer vi til å ønske å definere en funksjon med en kvotientmengde som domene. Mer presist, la A og B være mengder og la $\sim$ være en ekvivalensrelasjon på A. Vi ønsker da ofte å definere en funksjon $g\colon A/\sim \to B$ ved å bestemme funksjonsuttrykket $g([x])$ for $x \in A$. Som regel vil vi da skrive opp et uttrykk som avhenger av x. I realiteten forsøker vi altså å definere en funksjon på $A/\sim$ ved å bruke en funksjon $f\colon A \to B$, vi forsøker å definere $g\colon A/\sim \to B$ ved å sette

$$g([x]) = f(x), \quad x \in A.$$

Dette kan gi et problem, ettersom x ikke unikt bestemmer sin ekvivalensklasse $[x]$: Dersom $x \sim y$, så er jo $[x] = [y]$, og for at g skal være en faktisk funksjon, må da $g([x]) = g([y])$. I ligningen over må da $f(x) = f(y)$ for at dette skal gi mening.

Eksempel 5.33. La $A = \{0, 1, 2\}$ med ekvivalensrelasjonen gitt ved $0 \sim 0$, $0 \sim 1$, $1 \sim 0$, $1 \sim 1$ og $2 \sim 2$. La oss si at vi forsøker å definere en funksjon $g\colon A/\sim \to \{0, 1\}$ ved å sette $g([0]) = 0$, $g([1]) = 1$ og $g([2]) = 1$. Det vi i realiteten prøver å gjøre da er å sette $g([x]) = f(x)$ for alle $x \in A$ der $f\colon A \to \{0, 1\}$ er funksjonen gitt ved $f(0) = 0$, $f(1) = 1$ og $f(2) = 1$. Vi ser umiddelbart at dette gir et problem, da $[0] = [1]$ siden $0 \sim 1$, men vi forsøker å definere $g([0])$ til å være noe annet enn $g([1])$. Problemet er at $f(0) \neq f(1)$ selv om $0 \sim 1$.

Dette leder oss til følgende terminologi:

Definisjon 5.34. La A være en mengde med en ekvivalensrelasjon $\sim$, og la $f\colon A \to B$ være en funksjon. Vi sier at f *bevarer* $\sim$ dersom følgende holder:

$$\forall x, y \in A \quad (x \sim y \implies f(x) = f(y)).$$

Proposisjon 5.35. *La A være en mengde med en ekvivalensrelasjon $\sim$, og la $f\colon A \to B$ være en funksjon. Da er følgende ekvivalent:*

(i) f bevarer $\sim$.
(ii) Det fins en funksjon $\overline{f}\colon A/\!\sim \to B$ slik at

$$\forall x \in A \quad (\overline{f}([x]) = f(x)).$$

Dersom de to ekvivalente utsagnene over holder, så er funksjonen $\overline{f}$ entydig bestemt. Vi kaller $\overline{f}$ for avbildningen på $A/\!\sim$ indusert *av f.*

Bevis. La oss være veldig formelle og konstruere $\tilde{f}$ som et trippel $(A/\!\sim, B, R)$. Vi setter

$$R = \{([x], f(x)) : x \in A\} \subseteq (A/\!\sim) \times B.$$

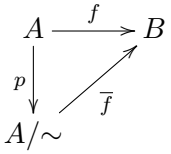
Vi viser at R tilfredsstiller Definisjon 3.1 (iii), nemlig at

$$\forall C \in A/\!\sim \quad \exists! y \in B \quad (C, y) \in R. \tag{5.1}$$

La $C \in A/\!\sim$. Da fins det en $x \in A$ slik at $C = [x]$, så $([x], f(x)) \in R$ fra definisjonen av R. Dette gir oss eksistensen vi trenger i (5.1). For å beviset entydighet antar vi at $(C, y), (C, y') \in R$. Fra definisjonen av R kan vi da finne $x, x' \in A$ slik at $(C, y) = ([x], f(x))$ og $(C, y') = ([x'], f(x'))$. Dette gir $C = [x]$ og $C = [x']$, så $[x] = [x']$. Vi konkluderer da med at $x \sim x'$ (Lemma 5.27). Siden f bevarer $\sim$, kan vi slutte at $f(x) = f(x')$. Men da er $y = f(x) = f(x') = y'$. Dette viser entydigheten vi trenger i (5.1). Vi har dermed vist at R er en gyldig graf, så vi kan definere funksjonen $\overline{f} = (A/\!\sim, B, R)$.

Per definisjon av R ser vi at $\overline{f}([x]) = f(x)$ for hver $x \in A$. For å bevise entydigheten av $\overline{f}$, la $g\colon A/\!\sim \to B$ slik at $g([x]) = f(x)$ for hver $x \in A$. Vi får da umiddelbart $\overline{f}([x]) = g([x])$ for alle $x \in A$, så $\overline{f} = g$. Dette fullfører beviset. □

Merk at vi kan omformulere (ii) i Proposisjon 5.35 som at det fins en $\overline{f}\colon A/\!\sim \to B$ slik at $f = \overline{f} \circ p$, der $p\colon A \to A/\!\sim$ betegne kvotientavbildningen. Dette kan illustreres med et diagram:



Vi skal se på en variasjon av veldefinerthet for binæroperasjoner. Denne gangen har vi en mengde A utstyrt med en ekvivalensrelasjon $\sim$ og en binæroperasjon $+$. Vi ønsker å definere en binæroperasjon $\overline{+}$ på $A/\!\sim$ ved å sette

$$[x]\overline{+}[y] = [x + y], \quad x, y \in A,$$

og undrer hva som må til for at dette skal være veldefinert. I denne situasjonen sier vi at $+$ *bevarer* $\sim$ dersom følgende gjelder:

$$\forall x, y, x', y' \in A \quad ((x \sim x' \wedge y \sim y') \implies x + y \sim x' + y')).$$

Korollar 5.36. La A være en mengde med en binæroperasjon $+$ og en ekvivalensrelasjon $\sim$. Da er følgende ekvivalent:

(i) $+$ bevarer $\sim$.
(ii) Det fins en binæroperasjon $\overline{+}$ på $A/\sim$ slik at

$$\forall x, y \in A \quad \big([x]\overline{+}[y] = [x+y]\big).$$

Dersom de to ekvivalente utsagnene over holder, så er $\overline{+}$ entydig bestemt. Vi kaller den for binæroperasjonen *indusert* av $+$.

Bevis. Oppgave. □

5.4 Ringer og heltall

I denne seksjonen følger vi [1, Delkapittel 6.3] parallelt med at vi konstruerer heltallene $\mathbb{Z}$ fra de naturlige tallene $\mathbb{N}$.

La $+$ være en assosiativ binæroperasjon på en mengde A med nøytralt element 0. Gitt et element $a \in A$, så sier vi at $b \in A$ er en *invers* for a dersom

$$a + b = b + a = 0.$$

Merk at dersom b og b' begge er inverser for a, så får vi at

$$b = b + 0 = b + (a + b') = (b + a) + b' = 0 + b' = b'.$$

Det følger at dersom a har en invers, så er den unik. Vi betegner den med $-a$.

Legg merke til at dersom c har en invers, så vil alltid implikasjonene

$$a + c = b + c \implies a = b, \qquad c + a = c + b \implies a = b$$

gjelde, for vi kan addere enten på høyre eller venstre side med $-a$. Spesielt er en binæroperasjon kansellativ dersom alle elementer har en invers.

Dersom vi bruker multiplikativ notasjon for binæroperasjonen, altså $\cdot$, så er det vanlig å betegne inversen til a dersom den eksisterer med a^{-1} istedenfor $-a$.

Definisjon 5.37. La $(A, +, \cdot, 0, 1)$ være et femtuppel der A er en mengde, $+$ og $\cdot$ er binæroperasjoner på A, og $0, 1 \in A$. Vi sier at $(A, +, \cdot, 0, 1)$ er en *ring* dersom følgende gjelder:

(i) $+$ er en assosiativ og kommutativ binæroperasjon på A med nøytralt element 0 der hvert element $a \in A$ har en (additiv) invers (som vi betegner med $-a$).
(ii) $\cdot$ er en assosiativ binæroperasjon på A med nøytralt element 1.
(iii) $\cdot$ er distributiv over $+$.

Dersom i tillegg følgende holder, så kaller vi $(A, +, \cdot)$ en *kommutativ ring*:

(iv) $\cdot$ er en kommutativ binæroperasjon.

Vi betegner som regel binæroperasjonen $\cdot$ kun ved å skrive elementer ved siden av hverandre, altså $ab = a \cdot b$.

Eksempel 5.38. La $A = \{0\}$ der 0 betegner det naturlige tallet 0 (det er ikke vesentlig hva det ene elementet i A er, så lenge A består av nøyaktig ett element). Vi definerer addisjon og multiplikasjon som følger:

$$0 + 0 = 0,$$
$$0 \cdot 0 = 0.$$

Da vil alle aksiomene for en ring være trivielt tilfredsstilt. Av den grunn kalles ringen $(\{0\}, +, \cdot, 0, 0)$ for den *trivielle ringen*. Legg merke til at i denne ringen er det nøytrale elementet for addisjon det samme som det nøytrale elementet for multiplikasjon, dvs. $0 = 1$. Faktisk er den trivielle ringen den eneste ringen med denne egenskapen: Dersom vi antar at $(B, +, \cdot)$ er en ring der $0 = 1$, og lar $y \in B$, så får vi at

$$y = y \cdot 1 = y \cdot 0 = 0$$

der den siste likheten kommer av Proposisjon 4.25.

Vi kommer til å bruke adjektivet *triviell* om en ring som kun har ett element, og som da (opptil å gi dette ene elementet et nytt navn) må være lik med ringen presentert her.

Eksempel 5.39. $(\mathbb{N}, +, \cdot, 0, 1)$ er ikke en ring, fordi ikke alle elementer har en additiv invers. Faktisk er 0 det eneste naturlige tallet med en additiv invers: Antar vi at $a \in \mathbb{N}$ har en $b \in \mathbb{N}$ slik at $a + b = 0$, gir Proposisjon 4.23 at $a = b = 0$. Bortsett fra dette tilfredsstiller $(\mathbb{N}, +, \cdot)$ alle egenskapene en kommutativ ring må tilfredsstille.

I en ring $(A, +, \cdot, 0, 1)$ har vi følgende grunnleggende forhold mellom additive inverser og multiplikasjon:

$$(-a)b = a(-b) = -ab.$$

Begrunnelsen for $(-a)b = -ab$ ser ut som følger:

$$(-a)b + ab = ((-a) + a)b = 0b = 0,$$

der $0b = 0$ følger fra Proposisjon 4.25. Den andre identiteten vises tilsvarende.

I en ring kan vi også danne differanser av elementer: Gitt $a, b \in A$, så definerer vi

$$a - b = a + (-b).$$

Til sammen kan vi utlede en rekke identiteter, deriblant

$$\begin{aligned} a(b - c) &= ab - ac, \\ (b - c)a &= ba - ca, \\ (-a)(-b) &= ab, \\ -a &= (-1)a = a(-1). \end{aligned}$$

Definisjon 5.40. En ikke-triviell kommutativ ring $(A, +, \cdot, 0, 1)$ kalles et *integritetsområde* dersom vi har at

$$ab = 0 \implies (a = 0 \ \vee \ b = 0)$$

for alle $a, b \in A$.

Legg merke til at i et integritetsområde er $\cdot$ kansellativ i den forstand at dersom $a, b, c \in A$ og $c \neq 0$, så vil

$$ac = bc \implies a = b, \qquad ca = cb \implies a = b.$$

Grunnen er som følger: Dersom $ac = bc$, så vil

$$0 = ac - ac = bc - ac = (b - a)c$$

Bruker vi den antatte egenskapen, får vi at $a - b = 0$ eller $c = 0$. Siden $c \neq 0$, er eneste mulige konklusjon at $b - a = 0$, altså $a = b$. Den andre kansellative egenskapen vises tilsvarende.

Vi skal nå konstruere heltallene fra de naturlige tallene. Konstruksjonen er litt annerledes enn det som er gjort i [1, Seksjon 3.3], men helt ekvivalent (og dessuten ganske standard). Intuisjonen bak konstruksjonen er å uttrykke et heltall a som en differanse

$$a = a_1 - a_2$$

der $a_1, a_2 \in \mathbb{N}$. Et heltall skal altså være gitt av et par med naturlige tall, altså et element i $\mathbb{N} \times \mathbb{N}$. Men hva betyr det at to slike differanser er like? Jo, dersom $a_1 - a_2 = a_1' - a_2'$ for $a_1, a_2, a_1', a_2' \in \mathbb{N}$, så vil vi at dette skal være ekvivalent med at $a_1 + a_2' = a_1' + a_2$. Dette motiverer følgende ekvivalensrelasjon:

Proposisjon 5.41. *Definer en relasjon $\sim$ på $\mathbb{N} \times \mathbb{N}$ ved*

$$(a_1, a_2) \sim (a_1', a_2') \quad \iff \quad a_1 + a_2' = a_1' + a_2.$$

Da er $\sim$ en ekvivalensrelasjon.

Bevis. Vi beviser at $\sim$ er refleksiv, symmetrisk og transitiv.

(i) Refleksivitet: Siden $a_1 + a_2 = a_1 + a_2$, slutter vi at $(a_1, a_2) \sim (a_1, a_2)$.

(ii) Symmetri: Anta at $(a_1, a_2) \sim (a_1', a_2')$. Vi får da at $a_1 + a_2' = a_1' + a_2$. Ved å lese likheten motsatt vei, får vi at $(a_1', a_2') \sim (a_1, a_2)$.

(iii) Transitivitet: Anta at $(a_1, a_2) \sim (a_1', a_2')$ og $(a_1', a_2') \sim (a_1'', a_2'')$. Vi får da at $a_1 + a_2' = a_1' + a_2$ og $a_1' + a_2'' = a_1'' + a_2'$. Ved å bruke regneregler for addisjon får vi at

$$(a_1 + a_2'') + a_2' = (a_1 + a_2') + a_2'' = (a_1' + a_2) + a_2'' = (a_1' + a_2'') + a_2 = (a_1'' + a_2') + a_2 = (a_1'' + a_2) + a_2'.$$

Kansellasjon gir nå $a_1 + a_2'' = a_1'' + a_2$. Dermed kan vi konkludere med at $(a_1, a_2) \sim (a_1'', a_2'')$.

Dette fullfører beviset. □

Definisjon 5.42. Vi kaller mengden

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim$$

for *mengden av heltall*. Gitt et element $(a, b) \in \mathbb{N} \times \mathbb{N}$, så betegner vi ekvivalensklassen i $\mathbb{Z}$ med

$$[(a, b)] = a - b.$$

Legg merke til at $(a_1, a_2) \sim (a_1 + c, a_2 + c)$ for alle $a_1, a_2, c \in \mathbb{N}$, siden $a_1 + (a_2 + c) = a_2 + (a_1 + c)$. Vi får dermed at

$$a_1 - a_2 = (a_1 + c) - (a_2 + c). \tag{5.2}$$

Spesielt er $c - c = (0 + c) - (0 + c) = 0 - 0$.

Lemma 5.43. *Følgende binæroperasjoner på $\mathbb{N} \times \mathbb{N}$ bevarer relasjonen $\sim$:*

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1 + a_2 b_2, a_1 b_2 + a_2 b_1).$$

Bevis. Vi viser kun at $+$ bevarer $\sim$, $\cdot$ er mer knot og overlates som en oppgave.

Anta at $(a_1, a_2) \sim (a_1', a_2')$ og $(b_1, b_2) \sim (b_1', b_2')$. Dette gir

$$\begin{aligned} a_1 + a_2' &= a_1' + a_2, \\ b_1 + b_2' &= b_1' + b_2. \end{aligned}$$

Dermed får vi

$$(a_1 + b_1) + (a_2' + b_2') = (a_1 + a_2') + (b_1 + b_2') = (a_1' + a_2) + (b_1' + b_2) = (a_1' + b_1') + (a_2 + b_2).$$

Dette viser at

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \sim (a_1' + b_1', a_2' + b_2') = (a_1', a_2') + (b_1', b_2').$$

Dermed har vi vist at binæroperasjonen bevarer $\sim$. □

Proposisjon 5.44. *La $+$ og $\cdot$ betegne binæroperasjonene på $\mathbb{Z}$ indusert ved Lemma 5.43. Da er $(\mathbb{Z}, +, \cdot, 0-0, 1-0)$ et integritetsområde.*

Bevis. Her er det mye å sjekke. Vi overlater mesteparten som en oppgave, men illustrerer hvordan assosiativitet av addisjon og kommutativitet av multiplikasjon vises her. For førstnevnte, la $a_1 - a_2, b_1 - b_2, c_1 - c_2 \in \mathbb{Z}$. Vi har da at

$$\begin{aligned} ((a_1 - a_2) + (b_1 - b_2)) + (c_1 - c_2) &= ((a_1 + b_1) - (a_2 + b_2)) - (c_1 + c_2) \\ &= ((a_1 + b_1) + c_1) - ((a_2 + b_2) + c_2) \\ &= (a_1 + (b_1 + c_1)) - (a_2 + (b_2 + c_2)) \\ &= (a_1 - a_2) + ((b_1 + c_1) - (b_2 + c_2)) \\ &= (a_1 - a_2) + ((b_1 - b_2) + (c_1 - c_2)). \end{aligned}$$

Sistnevnte ser ut som følger:

$$\begin{aligned} (a_1 - a_2) \cdot (b_1 - b_2) &= (a_1 b_1 + a_2 b_2) - (a_1 b_2 + a_2 b_1) \\ &= (b_1 a_1 + b_2 a_2) - (b_1 a_2 + b_2 a_1) \\ &= (b_1 - b_2) \cdot (a_1 - a_2). \end{aligned}$$

Man kan sjekke at det nøytrale elementet for addisjon er gitt ved $0 - 0$, og at det nøytrale elementet for multiplikasjon er gitt ved $1 - 0$.

Til slutt sjekker vi at ethvert element i $\mathbb{Z}$ har en additiv invers. La $a_1 - a_2 \in \mathbb{Z}$. Vi påstår da at $a_2 - a_1$ er inversen, noe som framkommer ved følgende utregning der vi bruker (5.2):

$$(a_1 - a_2) + (a_2 - a_1) = (a_1 + a_2) - (a_2 + a_1) = 0 - 0 = 0.$$

□

I vanlig matematikk betrakter man $\mathbb{N}$ som en delmengde av $\mathbb{Z}$. Slik vi har definert $\mathbb{N}$ og $\mathbb{Z}$ nå så stemmer ikke dette formelt sett: $\mathbb{Z}$ er en kvotient av $\mathbb{N} \times \mathbb{N}$, som ikke strengt tatt har $\mathbb{N}$ som delmengde. Vi skal imidlertid vise at det fins en veldig naturlig funksjon $i \colon \mathbb{N} \to \mathbb{Z}$ som vi kan bruke til å identifisere $\mathbb{N}$ med bildet $i(\mathbb{N})$ inne i $\mathbb{Z}$.

Proposisjon 5.45. *La $i \colon \mathbb{N} \to \mathbb{Z}$ være gitt ved*

$$i(a) = a - 0, \quad a \in \mathbb{N}.$$

Da er i en injektiv funksjon som tilfredsstiller følgende for alle $a, b \in \mathbb{N}$:

$$\begin{aligned} i(a+b) &= i(a) + i(b), \\ i(a \cdot b) &= i(a) \cdot i(b), \\ i(1) &= 1 - 0. \end{aligned}$$

Bevis. La $a, b \in \mathbb{N}$. Vi har da at

$$i(a+b) = (a+b) - 0 = (a+b) - (0+0) = (a-0) + (b-0) = i(a) + i(b),$$

(ii) i Definisjon 5.53 og

$$i(a \cdot b) = ab - 0 = (a-0)(b-0) = i(a) \cdot i(b).$$

Siden $1 = 1 - 0$ er det nøytrale elementet for multiplikasjon i $\mathbb{Z}$, ser vi at $i(1) = 1$. □

Notasjon 5.46. Gitt et naturlig tall $a \in \mathbb{N}$ så skriver vi simpelthen a for heltallet $i(a) = a - 0 \in \mathbb{Z}$. Vi får dermed at $-a = -(a-0) = 0 - a$ for $a \in \mathbb{N}$. Vi skal videre skrive simpelthen $\mathbb{N}$ for $i(\mathbb{N}) \subseteq \mathbb{Z}$.

Proposisjon 5.47. *La $-\mathbb{N}$ betegne mengden $\{-a : a \in \mathbb{N}\} \subseteq \mathbb{Z}$. Vi har da følgende egenskaper:*

(i) Dersom $a, b \in \mathbb{N}$, så er $a + b \in \mathbb{N}$ og $ab \in \mathbb{N}$.
(ii) $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$.
(iii) $\mathbb{N} \cup (-\mathbb{N}) = \mathbb{Z}$.

Bevis. (i) Dette følger fra Proposisjon 5.45.

(ii) La $a \in \mathbb{N}$ og anta at $a \in -\mathbb{N}$. Det fins da $b \in \mathbb{N}$ slik at $a = -b$. Dette gir $a + b = 0$, som gir $a = b = 0$ ved Proposisjon 4.23.

(iii) La $a = a_1 - a_2 \in \mathbb{Z}$. Dersom $a_1 \geq a_2$, så fins $c \in \mathbb{N}$ slik at $a_1 = a_2 + c$. Vi får da at $a = a_2 + c - a_2 = c \in \mathbb{N}$. Dersom $a_1 \leq a_2$, så fins $d \in \mathbb{N}$ slik at $a_1 + d = a_2$. Da får vi at $a = a_1 - (a_1 + d) = -d \in -\mathbb{N}$. □

Vi skal bruke Proposisjon 5.47 til å danne en ordensrelasjon på $\mathbb{Z}$ i **??** 5.6

5.5 Kropper og rasjonale tall

La $(A, +, \cdot, 0, 1)$ være en ring, der som vanlig 0 betegner det nøytrale elementet for $+$, og 1 betegner det nøytrale elementet for $\cdot$. Vi kaller et element $a \in A$ for *invertibelt* dersom det har en invers med hensyn på $\cdot$, altså et element $b \in A$ slik at

$$ab = ba = 1.$$

Vi vet at det slikt element b i så fall er unikt, og vi betegner det med a^{-1}.

Legg merke til at dersom 0 er invertibelt, så må $0 = 1$, for Proposisjon 4.25 gir at

$$1 = 0 \cdot 0^{-1} = 0.$$

Men som vi så i Eksempel 5.38 er det kun én ring som har denne egenskapen, nemlig den trivielle ringen.

Det fins med andre ord kun én ring der alle elementer i en ring er invertible, nemlig den trivielle ringen. Dersom vi derimot krever at alle elementer *bortsett* fra 0 er invertible, får vi noe mye mer interessant:

Definisjon 5.48. En ikke-triviell kommutativ ring $(A, +, \cdot, 0, 1)$ kalles en *kropp* dersom alle elementer bortsett fra 0 er invertible.

Vi skal nå se hvordan man konstruerer kanskje den mest fundamentale kroppen av dem alle, nemlig de rasjonale tallene, fra heltallene som vi konstruerte i forrige seksjon. Mesteparten av bevisene her kommer til å overlates som anbefalte oppgaver. I [1] behandles denne konstruksjonen mer generelt i [1, Teorem 5.6.4], men beviset overlates til [1, Oppgave 5.56].

Proposisjon 5.49. *Definer en relasjon $\sim$ på $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ ved*

$$(a, b) \sim (a', b') \quad \iff \quad ab' = a'b.$$

Da er $\sim$ en ekvivalensrelasjon.

Bevis. Oppgave. □

Lemma 5.50. *Følgende definerer binæroperasjoner på $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ som bevarer $\sim$:*

$$\begin{aligned}(a, b) + (c, d) &= (ad + bc, bd),\\ (a, b) \cdot (c, d) &= (ac, bd).\end{aligned}$$

Bevis. Oppgave. □

Definisjon 5.51. Vi setter

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\sim$$

og kaller elementene i denne mengden for *rasjonale tall*. Videre betegner vi ekvivalensklassen til et element $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ med

$$[(a, b)] = a/b = \frac{a}{b}.$$

Proposisjon 5.52. *Med de induserte binæroperasjonene fra Lemma 5.50 er $(\mathbb{Q}, +, \cdot, 0/1, 1/1)$ en kropp. Videre tilfredsstiller avbildningen $i \colon \mathbb{Z} \to \mathbb{Q}$ gitt ved*

$$i(a) = \frac{a}{1}, \quad a \in \mathbb{Z},$$

følgende egenskaper:

$$\begin{aligned}i(a + b) &= i(a) + i(b),\\ i(ab) &= i(a)i(b),\\ i(1) &= 1/1.\end{aligned}$$

Videre er i injektiv. Vi bruker derfor i til å identifisere $\mathbb{Z}$ som en delmengde av $\mathbb{Q}$.

Bevis. Oppgave. □

5.6 Totalt ordnede ringer

Til slutt ønsker vi å utvide ordensrelasjonen vi konstruerte på de naturlige tallene til en ordensrelasjon på heltallene, og deretter på de rasjonale tallene. Vi følger [1, s. 233] og betrakter konseptet om en totalt ordnet ring. Dette blir også viktigere senere når vi ser på de relle tallene.

Definisjon 5.53. En *totalt ordnet ring* er et sekstuppel $(A, +, \cdot, 0, 1, \leq)$ der

- $(A, +, \cdot, 0, 1)$ er en kommutativ ring, og
- $(A, \leq)$ er en totalt ordnet mengde,

slik at følgende holder:

(i) For alle $a, b, c \in A$ gjelder
$$a \leq b \implies a + c \leq b + c.$$

(ii) For alle $a, b \in A$ gjelder
$$(0 \leq a \ \wedge \ 0 \leq b) \implies 0 \leq ab.$$

Dersom ringen i tillegg er et integritetsområde eller en kropp, så sier vi at $(A, +, \cdot, 0, 1, \leq)$ er et *totalt ordnet integritetsområde* eller en *totalt ordnet kropp*.

Aksiomene over virker kanskje minimale, men de er nok til å få de fleste egenskapene vi kjenner:

Proposisjon 5.54. *I en totalt ordnet ring $(A, +, \cdot, 0, 1, \leq)$ har vi følgende egenskaper for alle $a, b, c \in A$:*

(i) Vi har $a \geq 0$ hvis og bare hvis $-a \leq 0$.

(ii) Vis at følgende implikasjoner gjelder:
$$\begin{aligned} ((a \geq 0 \ \wedge \ b \geq 0) \ \vee \ (a \leq 0 \ \wedge \ b \leq 0)) &\implies ab \geq 0, \\ ((a \geq 0 \ \wedge \ b \leq 0) \ \vee \ (a \leq 0 \ \wedge \ b \geq 0)) &\implies ab \leq 0. \end{aligned}$$
Vis at implikasjonene også gjelder motsatt vei om A er et integritetsområde.

(iii) $a^2 \geq 0$.

(iv) Dersom $c \geq 0$ har vi at
$$a \leq b \implies ac \leq bc.$$
Dersom vi er i et integritetsområde og $c > 0$, gjelder også motsatt implikasjon.

(v) Dersom $c \leq 0$ har vi at
$$a \leq b \implies ac \geq bc.$$
Dersom vi er i et integritetsområde og $c < 0$, gjelder også motsatt implikasjon.

Bevis. Vi beviser (i), (ii) og (iii), og etterlater resten som en oppgave.

(i) Dersom $a \geq 0$, så gir egenskap (i) i Definisjon 5.53 at $a + (-a) \geq 0 + (-a)$, altså $0 \geq -a$. Dersom $0 \geq -a$, gir det samme aksiomet at $0 + a \geq (-a) + a$, altså $a \geq 0$.

(ii) Dersom $a \geq 0$ og $b \geq 0$, gir (ii) i Definisjon 5.53 at $ab \geq 0$. Dersom $a \leq 0$ og $b \leq 0$, gir (i) at $-b \geq 0$ og $-a \geq 0$, så $(-a)(-b) \geq 0$ ved (ii) i Definisjon 5.53. Men $(-a)(-b) = ab$, så vi får $ab \geq 0$.

Dersom $a \geq 0$ og $b \leq 0$, gir (i) at $-b \geq 0$, så (ii) i Definisjon 5.53 gir $a(-b) \geq 0$. Men $a(-b) = -ab$, så nå gir (i) at $ab \leq 0$. Til slutt, dersom $a \leq 0$ og $b \geq 0$, så er $-a \geq 0$ ved (i), så $(-a)b \geq 0$. Men $(-a)b = -ab$, så da gir (i) igjen at $ab \leq 0$.

Anta nå at A er et integritetsområde. Anta at $ab \geq 0$. Vi ønsker å vise at enten $a \geq 0$ og $b \geq 0$, eller at $a \leq 0$ og $b \leq 0$. Siden $a \geq 0$ eller $a \leq 0$ og $b \geq 0$ eller $b \leq 0$, får vi totalt fire tilfeller:

- Dersom $a \geq 0$ og $b \geq 0$, har vi oppnådd det vi ønsker å vise.

- Dersom $a \geq 0$ og $b \leq 0$, får vi $ab \leq 0$ som allerede vist. Men da gir antagelsen $ab \geq 0$ at $ab = 0$. Siden A er et integritetsområde, konkluderer vi med at $a = 0$ eller $b = 0$. Dersom $a = 0$, får vi at $a \leq 0$ og $b \leq 0$, og dersom $b = 0$, får vi at $a \geq 0$ og $b \geq 0$.
- Dersom $a \leq 0$ og $b \geq 0$, får vi $ab \leq 0$ som allerede vist. Men da gir antagelsen $ab \geq 0$ at $ab = 0$. Siden A er et integritetsområde, konkluderer vi med at $a = 0$ eller $b = 0$. Dersom $a = 0$, får vi at $a \geq 0$ og $b \geq 0$, og dersom $b = 0$, får vi at $a \leq 0$ og $b \leq 0$.
- Dersom $a \leq 0$ og $b \leq 0$, har vi også oppnådd det vi ønsker å vise.

(iii) Dersom $a \geq 0$ gir Definisjon 5.53 direkte at $a^2 = aa \geq 0$. Dersom $a \leq 0$ gir del (ii) av Proposisjon 5.54 at $a^2 = aa \geq 0$. □

Vi skal nå definere ordensrelasjonene på $\mathbb{Z}$ og $\mathbb{Q}$. Disse følger samme mønster via et konsept som kalles en ikke-negativ kjegle. Vi kommer til å overlate detaljene her som en oppgave i oppgavesett 43.

Proposisjon 5.55. *Vi definerer relasjonen $\leq$ på $\mathbb{Z}$ ved følgende:*

$$a \leq b \quad \iff \quad b - a \in \mathbb{N}.$$

Da er $(\mathbb{Z}, +, \cdot, 0, 1, \leq)$ et totalt ordnet integritetsområde som har de to videre egenskapene:

(i) For alle $a, b \in \mathbb{Z}$ har vi at

$$a < b \quad \iff \quad a + 1 \leq b.$$

(ii) Enhver ikke-tom oppad begrenset delmengde av $\mathbb{Z}$ har et største element, og enhver ikke-tom nedad begrenset delmengde har et minste element.

I tillegg har funksjonen $i \colon \mathbb{N} \to \mathbb{Z}$ gitt ved $i(a) = a - 0$ for $a \in \mathbb{N}$ følgende egenskap for alle $a, b \in \mathbb{N}$:

$$a \leq b \quad \iff \quad i(a) \leq i(b).$$

Bevis. Beviset for at $(\mathbb{Z}, +, \cdot, 0, 1, \leq)$ er en totalt ordnet ring kommer til å følge fra Proposisjon 5.47. Vi gir detaljene som en oppgave på oppgavesettet i uke 43.

Vi viser (i). Anta først at $a < b$. Vi får da at $b - a \in \mathbb{N}$ og $a \neq b$, så $b - a \neq 0$. Vi kan da skrive $b - a = c + 1$ der $c \in \mathbb{N}$ ved å bruke Proposisjon 4.8. Dermed er $b - (a + 1) = c \in \mathbb{N}$, så $a + 1 \leq b$. I den andre retningen får vi at $b - (a + 1) = c' \in \mathbb{N}$, så $b - a = c' + 1$, som gir $a \leq b$ og $a < b$.

(ii) La $A \subseteq \mathbb{Z}$ være ikke-tom og nedad begrenset. La $x \in \mathbb{Z}$ være en nedre skranke for A. Betrakt mengden

$$B = \{a - x : a \in A\}.$$

Da er 0 en nedre skranke for B, siden vi for alle $a \in A$ har at $a \geq x$, altså $a - x \geq 0$. Dermed har vi at $B \subseteq \mathbb{N}$. Videre er også B ikke-tom, så Teorem 5.20 gir at B har et minste element b. Vi får da at $a - x \geq b$ for alle $a \in A$, altså at $a \geq x + b$ for alle $a \in A$. Dette gir at $x + b$ er en nedre skranke for A. Siden $b \in B$, kan vi skrive $b = a' - x$ for en $a' \in A$. Dermed er $x + b = x + (a' - x) = a' \in A$, så $x + b$ er minimum for A.

Beviset for øvre skranker kan vi nå få ved å negere elementene i en gitt ikke-tom, oppad begrenset mengde. Vi overlater det som en oppgave. □

Korollar 5.56. Dersom $a, b \in \mathbb{Z}$ og $ab = 1$, så er enten $a = b = 1$ eller $a = b = -1$.

Bevis. Vi antar at $a, b \in \mathbb{Z}$ tilfredsstiller $ab = 1$. Siden $1 \geq 0$, gir Proposisjon 5.54 (ii) at enten $a \geq 0$ og $b \geq 0$, eller $a \leq 0$ og $b \leq 0$. Vi begynner med det første tilfellet. Dersom $a = 0$ eller

$b = 0$ ville det gitt $ab = 0 \neq 1$, så vi har at $a > 0$ og $b > 0$. Da gir Proposisjon 5.55 (i) at $a \geq 1$ og $b \geq 1$. Men vi får også, ved å bruke Proposisjon 5.54 (iv), at

$$a = a \cdot 1 \leq a \cdot b = 1.$$

Dermed er $a = 1$ ved antisymmetri. På samme måte fås $b = 1$.

I tilfellet der $a \leq 0$ og $b \leq 0$, vet vi at $-a \geq 0$ og $-b \geq 0$ ved Proposisjon 5.54 (i). I tillegg er $(-a)(-b) = ab = 1$. Dermed kan vi bruke det vi allerede har vist til å konkludere at $-a = 1$ og $-b = 1$, som gir $a = b = -1$. □

Proposisjon 5.57. *La*

$$\mathbb{Q}_{\geq 0} = \{a/b : (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}),\ ab \geq 0\}.$$

Vi definerer en relasjon $\leq$ på $\mathbb{Q}$ ved

$$x \leq y \quad \iff \quad y - x \in \mathbb{Q}_{\geq 0}.$$

Da er $(\mathbb{Q}, +, \cdot, 0, 1)$ en totalt ordnet kropp. Videre har funksjonen $i \colon \mathbb{Z} \to \mathbb{Q}$ gitt ved $i(a) = a/1$ for $a \in \mathbb{Z}$ følgende egenskap for alle $a, b \in \mathbb{Z}$:

$$a \leq b \quad \iff \quad i(a) \leq i(b).$$

Bevis. Dette overlates også som en oppgave på oppgavesett 43. □

Kapittel 6

Tallteori

6.1 Delelighet

Nøkkelresultatet for heltallsdivisjon er følgende:

Teorem 6.1. *La $a, b \in \mathbb{Z}$ der $b > 0$. Da fins det unike tall $q, r \in \mathbb{Z}$ slik at*

$$a = qb + r, \quad 0 \leq r < b.$$

Bevis. La $a, b \in \mathbb{Z}$ der $b > 0$. Definer

$$A = \{a - qb : q \in \mathbb{Z}\} \cap \mathbb{N}.$$

Dersom $a \geq 0$, så er $a - (-a)b \in A$ og $a - (-a)b = a(b + 1) \geq 0$ (Proposisjon 5.55), så $A \neq \emptyset$. Dersom $a < 0$, så er $a - ab \in A$ og $a - ab = -a(b - 1) \geq 0$ (Proposisjon 5.55), så $A \neq \emptyset$. Uansett er altså A en ikke-tom delmengde av $\mathbb{N}$. Ved Teorem 5.20 har A et minste element r. Siden $r \in A$, fins det per definisjon et tall $q \in \mathbb{Z}$ slik at $r = a - qb$. Vi har da at $a = qb + r$ og $r \geq 0$.

Legg merke til at

$$a = (qb + r) + (b - b) = (q + 1)b + (r - b).$$

Dersom $r - b \geq 0$, får vi at $r - b \in A$. Siden r er minste element i A, gir dette $r \leq r - b$. Dette gir $0 \leq -b$, en selvmotsigelse siden $b > 0$. Vi konkluderer derfor med at $r - b < 0$, altså $r < b$.

Vi viser nå unikhet. Anta at $a = q'b + r'$ for $q', r' \in \mathbb{Z}$ der $0 \leq r' < b$. Vi får da at $-b < -r' \leq 0$, så $-b < r - r' < b$. På den andre siden er $r - r' = (q' - q)b$, så vi får at

$$-b < (q' - q)b < b.$$

Siden $b > 0$, gir dette at $-1 < q' - q < 1$. Dermed er eneste mulighet at $q = q'$ ved Proposisjon 5.55 (i). Dermed får vi også at $r = r'$. □

Vi kaller tallet q for *kvotienten* og r for *resten* i divisjonen av a på b.

Eksempel 6.2. La $b = 2$. Da gir teoremet over at enhver $a \in \mathbb{Z}$ fins det unike tall $q, r \in \mathbb{Z}$ slik at $a = 2q + r$ og $0 \leq r < 2$, altså $r = 0$ eller $r = 1$. Tallene på formen $a = 2q$ kaller vi for *partall*, mens tallene på formen $a = 2q + 1$ kaller vi for *oddetall*. Altså er alle heltall enten et partall eller et oddetall, og aldri begge to samtidig.

I spesialtilfellet der resten blir lik 0, gir vi følgende terminologi:

Definisjon 6.3. Vi definerer en relasjon $\mid$ på $\mathbb{Z}$ ved

$$\forall b, a \in \mathbb{Z} \quad \big(b \mid a \quad \iff \quad \exists q \in \mathbb{Z}\ (a = qb)\big).$$

Dersom $b \mid a$, så sier vi at b *deler* a, eller at a er *delelig* med b.

Vi kommer ofte til å betrakte $\mid$ som en relasjon på $\mathbb{N}$ i tillegg til som en relasjon på $\mathbb{Z}$.

Proposisjon 6.4. *Følgende holder for delelighet:*

(i) For alle $a \in \mathbb{Z}$ har vi at $a \mid a$, $a \mid 0$, $1 \mid a$, og

$$0 \mid a \implies a = 0.$$

(ii) For alle $a, b \in \mathbb{Z}$ gjelder

$$a \mid b \ \wedge\ b \mid a \implies a = \pm b.$$

(iii) For alle $a, b, c \in \mathbb{Z}$ gjelder

$$a \mid b \ \wedge\ b \mid c \implies a \mid c.$$

(iv) Dersom $a, b, c \in \mathbb{Z}$, $a \mid b$ og $a \mid c$, så gjelder

$$\forall x, y \in \mathbb{Z} \quad \big(a \mid (bc + cy)\big).$$

(v) Dersom $a, b \in \mathbb{N}$ er positive og $a \mid b$, så gjelder $a \leq b$.

Spesielt er delelighet en ordensrelasjon på $\mathbb{N}$ med 1 som minste element og 0 som største element.

Bevis. (i) Siden $a \cdot 1 = a$, $a \cdot 0 = 0$ og $1 \cdot a = a$, følger de tre første identitetene. Dersom $0 \mid a$, fins en $q \in \mathbb{Z}$ slik at $0 \cdot q = a$. Dermed er $a = 0$.

(ii) Dersom $a \mid b$ og $b \mid a$ fins $q, l \in \mathbb{Z}$ slik at $aq = b$ og $bl = a$. Dette gir

$$b \cdot 1 = aq = b \cdot (lq).$$

Dersom $b = 0$, gir (i) og $b \mid a$ at $a = 0$. Spesielt gjelder da $a = \pm b$. Dersom $b \neq 0$, gir ligningen over og kansellasjonsloven for multiplikasjon at $1 = lq$. Men da gir **??** at $l = q = 1$ eller $l = q = -1$. I første tilfellet får vi $a = b$, mens i andre tilfelle får vi $a = -b$.

(iii) Anta at $a \mid b$ og at $b \mid c$. Da fins $q, l \in \mathbb{Z}$ slik at $aq = b$ og $bl = c$. Dette gir

$$aql = bl = c,$$

som betyr at $a \mid c$.

(iv) Anta at $a \mid b$ og $a \mid c$, og la $x, y \in \mathbb{Z}$. Det fins da $q, l \in \mathbb{Z}$ slik at $aq = b$ og $al = c$. Vi får da at

$$a(qx + ly) = (aq)x + (al)y = bx + cy.$$

Dette viser at $a \mid (bx + cy)$.

(v) La $a, b \in \mathbb{N}$ med $a \geq 1$ og $b \geq 1$. Vi antar at $a \mid b$, så da fins $q \in \mathbb{Z}$ slik at $aq = b$. Vi må da ha at $q \geq 0$, og siden $b \neq 0$ kan vi ikke ha $q = 0$. Vi slutter da at $q > 0$, altså $q \geq 1$. Ved å multiplisere denne ulikheten med det positive tallet a, får vi at $b = qa \geq 1a = a$, som gir ønsket konklusjon. □

Vi betrakter delelighet på $\mathbb{N}$. La oss se hva det betyr å ha en nedre skranke for en mengde $\{a, b\}$ bestående av to elementer $a, b \in \mathbb{N}$. Dette vil være et tall $d \in \mathbb{N}$ slik at $d \mid a$ og $d \mid b$. Et slikt tall kaller vi for en *felles faktor* av a og b. Videre vil *infimum* av mengden $\{a, b\}$ være en felles faktor d slik at for enhver annen felles faktor d' så vil $d' \mid d$. Vi kaller et slikt tall for *største felles faktor* av a og b. Merk at dette er unikt dersom det eksisterer, siden infimum alltid er unikt.

Mer generelt, når $a, b \in \mathbb{Z}$ (ikke nødvendigvis i $\mathbb{N}$), skal vi også kalle et tall $d \in \mathbb{Z}$ som deler a og b for en felles faktor for a og b, og dersom det er delelig på enhver felles faktor av a og b *og* er positivt, så kaller vi det for største felles faktor av a og b. Merk at det slikt tall er unikt dersom det eksisterer, siden vi krever at det er positivt.

Gitt $d \in \mathbb{Z}$ så skriver vi

$$d\mathbb{Z} = \{dk : k \in \mathbb{Z}\}.$$

Legg merke til at dette er mengden av alle tall som er delelige med d. Dersom $a, b \in \mathbb{Z}$ så kaller vi et tall på formen $ax + by$ der $x, y \in \mathbb{Z}$ en *lineærkombinasjon* av a og b.

Proposisjon 6.5 (Bézouts identitet)**.** *La $a, b \in \mathbb{Z}$. Da fins det unikt tall $d \in \mathbb{N}$ slik at*

$$\{ax + by : x, y \in \mathbb{Z}\} = d\mathbb{Z}.$$

Dette tallet er største felles faktor av a og b. Vi betegner det med

$$d = a \wedge b.$$

Bevis. La oss kalle mengden til venstre for A. Vi merker oss først at A har egenskapen at dersom $k, l \in A$, så er $kx + ly \in A$ for alle $x, y \in \mathbb{Z}$: For dersom det fins $x', y', x'', y'' \in \mathbb{Z}$ slik at $k = ax' + by'$ og $l = ax'' + by''$, så får vi at

$$kx + ly = (ax' + by')x + (ax'' + by'')y = a(x'x + x''y) + b(xy' + yy'') \in A.$$

Vi sier at A er *lukket* under lineærkombinasjoner.

Dersom $a = b = 0$, så får vi at $A = \{0\}$, og da er $d = 0$ det unike naturlige tallet slik at $A = d\mathbb{Z}$. I resten av beviset antar vi derfor at $a \neq 0$ eller $b \neq 0$, som gir at $A \neq \{0\}$. Faktisk er mengden $\{k \in A : k > 0\}$ ikke-tom, så ved Teorem 5.20 har den et minste element d.

Vi viser nå at $A \subseteq d\mathbb{Z}$. Anta at $k \in A$. Ved å bruk Teorem 6.1 får vi $q, r \in \mathbb{Z}$ slik at $k = qd + r$ og $0 \leq r < d$. Siden A er lukket under lineærkombinasjoner, har vi at $r = k - qd \in A$. Vi kan dermed ikke ha at $r > 0$, for da ville $r \in A$ og $r < d$ motstridet at d er det minste, positive elementet i A. Vi konkluderer med at $r = 0$, så $k = qd$. Dette viser $A \subseteq d\mathbb{Z}$, som ønsket.

I den andre retningen så har vi at $d \in A$, så ved det faktum at A er lukket under lineærkombinasjoner, får vi også at $qd \in A$ for alle $q \in \mathbb{Z}$. Dette gir $d\mathbb{Z} \subseteq A$.

Vi viser nå unikheten: Anta at $d\mathbb{Z} = d'\mathbb{Z}$ der $d, d' \in \mathbb{N}$. Da er $d \in d'\mathbb{Z}$ og $d' \in d\mathbb{Z}$, så det fins $q, q' \in \mathbb{Z}$ slik at $d = d'q'$ og $d' = dq$. Dette gir $d \mid d'$ og $d' \mid d$, som ved Proposisjon 6.4 impliserer at $d = d'$ siden begge er naturlige tall.

Til slutt viser vi at d er største felles faktor for a og b. Siden $a, b \in A = d\mathbb{Z}$, ser vi at d er en felles faktor for a og b. Anta nå at $d' \in \mathbb{Z}$ og $d' \mid a$, $d' \mid b$. Ved Proposisjon 6.4 (iv) vet vi da at d' deler alle lineærkombinasjoner av a og b. Men siden $A = d\mathbb{Z}$, vet vi at d er en lineærkombinasjon av a og b, så d' må dele d. □

Merknad 6.6. ???

Merknad 6.7. Dersom $a, b \in \mathbb{Z}$ og $a \neq 0$ eller $b \neq 0$, så er største felles faktor $d = a \wedge b$ for a og b også det største tallet som deler både a og b, i forstand av den vanlige ordningen på $\mathbb{Z}$: Dersom d' er en felles faktor for a og b, så må d' nødvendigvis være positiv. Siden vi får $d' \mid d$ fra egenskapen til d, gir nå Proposisjon 6.4 (v) at $d' \leq d$.

Merk imidlertid at dersom $a = b = 0$ så er $a \wedge b = 0$, selv om i dette tilfellet ethvert tall er en felles faktor for a og b.

Hvordan beregner man så største felles divisor d for a og b? Og hvordan uttrykker vi d som en lineærkombinasjon av a og b? Dersom $a = qb + r$ så viser Proposisjon 6.4 (iv) at enhver felles divisor for a og b er en felles divisor for b og r. Det følger at

$$a \wedge b = b \wedge r.$$

Videre har vi at $a \wedge 0 = a$ for enhver $a \in \mathbb{N}$. Dette kan vi bruke til å beregne største felles divisor. Vi illustrerer med et eksempel:

Eksempel 6.8. La $a = 78$ og $b = 30$. Vi kan da skrive

$$\begin{aligned} 78 &= 2 \cdot 30 + 18, \\ 30 &= 1 \cdot 18 + 12, \\ 18 &= 1 \cdot 12 + 6, \\ 12 &= 2 \cdot 6 + 0. \end{aligned}$$

Da er $78 \wedge 30 = 30 \wedge 18 = 18 \wedge 12 = 12 \wedge 6 = 6 \wedge 0 = 6$. Ved å bruke ligningene over, får vi at

$$6 = 18 - 1 \cdot 12 = 18 - 1 \cdot (30 - 1 \cdot 18) = 2 \cdot 18 - 1 \cdot 30 = 2 \cdot (78 - 2 \cdot 30) - 1 \cdot 30 = 2 \cdot 78 - 5 \cdot 30.$$

Definisjon 6.9. Vi sier at $a, b \in \mathbb{Z}$ er *innbyrdes primiske* dersom $a \wedge b = 1$.

Korollar 6.10. To heltall $a, b \in \mathbb{Z}$ er innbyrdes primiske hvis og bare hvis det fins $x, y \in \mathbb{Z}$ slik at

$$ax + by = 1.$$

Bevis. Merk at a og b er innbyrdes primiske hvis og bare hvis $1 \in d\mathbb{Z}$, der $d = a \wedge b$. På den andre siden fins det $x, y \in \mathbb{Z}$ slik at $ax + by = 1$ hvis og bare hvis $1 \in \{ax + by : x, y \in \mathbb{Z}\}$. Siden disse to mengdene er like ifølge Proposisjon 6.5, følger konklusjonen. □

Korollar 6.11 (Euklids lemma)**.** La $a, b, c \in \mathbb{Z}$. Dersom $a \mid bc$ og $a \wedge b = 1$, så må $a \mid c$.

Bevis. Vi bruker Korollar 6.10 til å finne $x, y \in \mathbb{Z}$ slik at $ax + by = 1$. I tillegg gir $a \mid bc$ en $q \in \mathbb{Z}$ slik at $aq = bc$. Vi har da at

$$c = c \cdot 1 = c(ax + by) = cax + cby = acx + aqy = a(cx + qy).$$

Dette viser at $a \mid c$. □

Som en anvendelse av teorien vi har utviklet så langt kan vi bevise at ethvert rasjonalt kan skrives på en viss kanonisk form:

Proposisjon 6.12. *For ethvert rasjonalt tall $q \in \mathbb{Q}$ fins det unike heltall $a, b \in \mathbb{Z}$ med $b > 0$ og $a \wedge b = 1$ slik at $q = a/b$.*

Bevis. Først viser vi eksistens. La $q \in \mathbb{Q}$. Vi kan da finne $a, b \in \mathbb{Z}$ med $b \neq 0$ slik at $q = a/b$. La $d = a \wedge b$. Fra Proposisjon 6.5 kan vi da finne $x, y \in \mathbb{Z}$ slik at $d = ax + by$. Om vi lar $k, l \in \mathbb{Z}$ være slik at $kd = a$ og $ld = b$, så får vi at

$$d = d(kx + ly).$$

Dette gir $ax + ly = 1$, altså må $k \wedge l = 1$ ved Korollar 6.10. Vi får nå at

$$q = \frac{a}{b} = \frac{kd}{ld} = \frac{k}{l}.$$

Dersom $l > 0$, er vi nå ferdige. Dersom $l < 0$, kan vi skrive $q = (-k)/(-l)$, der $-l > 0$. Vi er da ferdige i dette tilfellet også.

Så viser vi unikhet. Anta at $a/b = a'/b'$ der $a, b, a', b' \in \mathbb{Z}$, $b \neq 0$, $b' \neq 0$, $a \wedge b = 1$ og $a' \wedge b' = 1$. Vi får da at $ab' = a'b$. Dette gir $b' \mid a'b$ og $b \mid ab'$. Siden $a \wedge b = 1$ og $a' \wedge b' = 1$, gir Korollar 6.10 at $b \mid b'$ og $b' \mid b$. Men siden $b > 0$ og $b' > 0$, er da er eneste mulighet at $b = b'$. Dette gir umiddelbart $a = a'$. □

6.2 Primtall

Som vi har sett er 1 et minste element for delelighetsrelasjonen på $\mathbb{N}$. Om vi ser på $\mathbb{N} \setminus \{1\}$, fins det ikke lenger noen minste elementer. Det fins derimot minimale elementer: Et minimalt element er nå et tall $p \in \mathbb{N} \setminus \{1\}$ slik at $a \mid p$ impliserer $a = p$ for enhver $a \in \mathbb{N} \setminus \{1\}$. Vi ser at dette sammenfaller med følgende definisjon:

Definisjon 6.13. Et naturlig tall $p > 1$ kalles et *primtall* dersom det kun er delelig med 1 og seg selv.

Lemma 6.14 (Euklids lemma for primtall)**.** *La p være et primtall og la $a, b \in \mathbb{Z}$. Dersom $p \mid ab$, så gjelder enten $p \mid a$ eller $p \mid b$.*

Bevis. Anta at $p \mid ab$. Dersom $p \mid a$, er beviset ferdig. Dersom p ikke deler a, så må $p \wedge a = 1$. Da gir Korollar 6.10 at $p \mid b$. □

Vi kan bruke lemmaet over til å vise noe artig:

Proposisjon 6.15. *Det fins inget rasjonalt tall q slik at $q^2 = 2$.*

Bevis. Anta for en selvmotsigelse at $q \in \mathbb{Q}$ tilfredsstiller $q^2 = 2$. Ved Proposisjon 6.12 kan vi skrive $q = a/b$ der $a, b \in \mathbb{Z}$, $b \neq 0$, og $a \wedge b = 1$. Vi får da at $a^2/b^2 = 2$, som kan skrives om til

$$a^2 = 2b^2.$$

Denne ligningen gir $2 \mid a^2$. Siden 2 er et primtall, gir Lemma 6.14 at $2 \mid a$. Vi kan dermed finne $k \in \mathbb{Z}$ slik at $2k = a$. Putter vi dette inn i ligningen over, får vi at

$$4k^2 = (2k)^2 = a^2 = 2b^2.$$

Ved å kansellere 2 på begge sider, fås

$$2k^2 = b^2.$$

Dermed har vi at $2 \mid b^2$. Igjen, ved Lemma 6.14, gir dette at $2 \mid b$. Men vi har nå både $2 \mid a$ og $2 \mid b$, som motstrider $a \wedge b = 1$.

Eneste konklusjon er derfor at et slikt rasjonalt tall ikke kan finnes. □

Vi skal nå vise aritmetikkens fundamentalteorem. Beviset bygger på sterk induksjon, som vi ennå ikke har behandlet i pensum.

Proposisjon 6.16 (Sterk induksjon)**.** *La $P(n)$ være et predikat og la $a \in \mathbb{N}$. Anta at følgende gjelder:*

- *$P(a)$ holder.*
- *For alle $n \in \mathbb{N}$ med $n \geq a$ så har vi at*

$$\Big(\forall k \in \mathbb{N}(a \leq k \leq n \;\Rightarrow\; P(k))\Big) \implies P(n+1).$$

Da holder $P(n)$ for alle $n \geq a$.

Bevis. La $Q(n)$ betegne predikatet

$$Q(n): \quad \forall k \in \mathbb{N}\,(a \leq k \leq n+a \implies P(k)).$$

Vi beviser $Q(n)$ for alle $n \in \mathbb{N}$ ved vanlig induksjon.

For å vise $Q(0)$, la $k \in \mathbb{N}$ og anta at $a \leq k \leq a+0$. Dette gir $k = a$. Siden $P(a)$ er antatt å holde, får vi at $P(k)$ holder. Dette viser $Q(0)$.

La nå $n \in \mathbb{N}$ og anta at $Q(n)$ holder. Da får vi at $P(k)$ stemmer for alle $a \leq k \leq a+n$. Dermed gir den andre antagelsen at $P(a+n+1)$. Vi har dermed at $P(k)$ stemmer for alle $a \leq k \neq n+a+1$, hvilket gir at $Q(n+1)$ stemmer.

Dette fullfører induksjonsbeviset. □

Notasjon 6.17. I neste teorem skal vi snakke om lister av tall. La oss være ordentlig presise med hva vi mener når vi snakker om lister av elementer fra en generell mengde A. Gitt $n \in \mathbb{N}$ så definerer vi

$$\mathbb{N}_n = \{k \in \mathbb{N} : k < n\}.$$

Legg merke til at $\mathbb{N}_0 = \emptyset$. En *liste* av lengde n med elementer fra A definerer vi da til å være en funksjon $\mathbb{N}_n \to A$. Dersom f er en slik funksjon, så skriver vi gjerne $a(i) = a_i$ og betegner lista som helhet med $a_0, \ldots, a_{n-1}$. Spesielt er en liste av lengde 0 den tomme funksjonen, som vi tenker på som en tom liste.

Gitt en slik liste $a_0, \ldots, a_{n-1}$ representert ved en funksjon $a\colon \mathbb{N}_n \to A$, så definerer vi

$$\{a_0, \ldots, a_{n-1}\} = \mathrm{Im}(a).$$

Vi definerer produkter av lister av rasjonale tall rekursivt på følgende måte: Dersom a er en tom liste, så er produktet bare 1. Dersom $a_0, \ldots, a_n$ er en liste bestående av $n+1$ tall, så definerer vi

$$a_0 \cdots a_n = (a_0 \cdots a_{n-1})a_n.$$

Teorem 6.18 (Aritmetikkens fundamentalteorem)**.** *La $n \in \mathbb{N}$ $n \geq 1$. Da kan n skrives som et produkt av en liste av primtall. Dette produktet er unikt, opptil endring av rekkefølge på primtallene i lista.*

Bevis. Vi beviser at n kan skrives som et produkt av primtall ved sterk induksjon på n. Grunnsteget er da $n = 1$, som kan skrives som et produkt av en tom liste med primtall.

Vi lar nå $n \in \mathbb{N}$ være et vilkårlig naturlig tall større enn eller lik 2, og antar at alle naturlige tall $1 \leq m < n$ kan skrives som produkt av primtall. Dersom n allerede er et primtall, er beviset

ferdig. Dersom dette ikke er tilfellet, er n per definisjon delelig med et tall som hverken er 1 eller n, så vi kan skrive $n = ab$ der $a, b \in \mathbb{N}$ og $1 < a < n$, $1 < b < n$ (ved Proposisjon 6.4 (v)). Induksjonsantagelsen gir nå at a og b kan skrives som produkt av primtall. Men da er også $n = ab$ et produkt av primtall.

Så viser vi entydighet. Vi beviser ved induksjon på $m \in \mathbb{N}$ følgende utsagn: For alle $n \in \mathbb{N}$, alle primtall $p_0, \dots, p_{m-1}$, og alle primtall $q_0, \dots, q_{n-1}$, så vil

$$p_0 \cdots p_{m-1} = q_0 \cdots q_{n-1},$$

implisere at $m = n$ og at det fins en bijeksjon $\sigma \colon \mathbb{N}_m \to \mathbb{N}_n$ slik at $p_i = q_{\sigma(i)}$ for alle $1 \leq i \leq m$.

For $m = 0$ får vi at $1 = q_0 \cdots q_{n-1}$. Dette impliserer at $n = 0$, for primtall må være ulik 1 per definisjon. Dermed er den tomme funksjonen $\mathbb{N}_0 \to \mathbb{N}_0$ bijeksjonen vi er ute etter.

La nå $m \in \mathbb{N}$ og anta at utsagnet stemmer for m. La så $n \in \mathbb{N}$, la $p_0, \dots, p_m$ være primtall, la $q_0, \dots, q_{n-1}$ være primtall, og anta at

$$p_0 \cdots p_m = q_0 \cdots q_{n-1}.$$

Vi får at $p_m \mid q_0 \cdots q_{n-1}$, så da kan spesielt ikke produktet være tomt, for dette ville implisert $p_m = 1$. Det fins dermed en $n' \in \mathbb{N}$ slik at $n' + 1 = n$. Ved Lemma 6.14 fins det en $j \in \mathbb{N}_n$ slik at $p_m = q_j$. Definer en bijeksjon $\tau \colon \mathbb{N}_n \to \mathbb{N}_n$ ved $\tau(j) = n'$, $\tau(n') = j$, og $\tau(i) = i$ for $i \neq j$ og $i \neq n'$. Skriv i tillegg $r_i = q_{\tau(i)}$ for hver $i \in \mathbb{N}_{m'+1}$. Vi har da at

$$p_0 \cdots p_m = r_0 \cdots r_{n'}.$$

og at $p_m = r_{n'}$. Kansellerer vi denne felles faktoren på begge sider, får vi at

$$p_0 \cdots p_{m-1} = r_0 \cdots r_{n'-1}.$$

Ved induksjonshypotesen er $m = n'$ og fins en bijeksjon $\sigma \colon \mathbb{N}_m \to \mathbb{N}_m$ slik at $p_i = r_{\sigma(i)}$ for alle $i \in \mathbb{N}_m$. La oss utvide σ til en bijeksjon $\mathbb{N}_{m+1} \to \mathbb{N}_{m+1}$ som vi også betegner med σ, hvor $\sigma(m) = m$. Sett deretter $\sigma' = \tau \circ \sigma$. Da er σ' en bijeksjon og $p_i = q_{\sigma'(i)}$ for alle $i \in \mathbb{N}_{m+1}$. Dette fullfører beviset. □

Vi konkluderer med Euklids bevis for uendeligheten av primtall. Vi har ikke ennå formelt definert hva en uendelig mengde er, så vi formulerer resultatet på en litt annerledes måte.

Teorem 6.19. *La $n \in \mathbb{N}$ og la $p_0, \dots, p_{n-1}$ være en liste av primtall. Da fins det et primtall q slik at $q \notin \{p_0, \dots, p_{n-1}\}$.*

Bevis. Definer $P = p_0 \cdots p_{n-1}$ og $N = P + 1$. Da er $N > 1$, så ved Teorem 6.18 fins det et primtall q som deler N. Dersom vi hadde hatt $q \in \{p_0, \dots, p_{n-1}\}$, si $q = p_i$ for en indeks $i \in \mathbb{N}_n$, så ville både $q \mid P$ og $p \mid N$, så ved Proposisjon 6.4 (iv) må

$$q \mid (N - P) = 1.$$

Dette gir $q = 1$, en selvmotsigelse. Vi konkluderer med at $q \notin \{p_0, \dots p_{n-1}\}$. □

6.3 Kongruensregning

Definisjon 6.20. La $n \in \mathbb{N} \setminus \{0\}$. Vi sier at to tall $a, b \in \mathbb{Z}$ er *kongruente modulo n* dersom

$$n \mid (a - b).$$

Dersom dette er tilfellet skriver vi $a \equiv b \pmod{n}$.

For eksempel er $2 \equiv 14 \pmod 2$, siden $14 - 2 = 12$ som er delelig med 12.

Lemma 6.21. *La $a, n \in \mathbb{Z}$ der $n > 0$. Da er a kongruent modulo n med nøyaktig ett av tallene i $\mathbb{N}_n = \{k \in \mathbb{N} : k < n\}$.*

Bevis. Ved Teorem 6.1 fins det unike $q, r \in \mathbb{Z}$ med $0 \leq r < n$ slik at $a = qn + r$. Denne ligningen gir $qn = a - r$, altså $a \equiv r \pmod n$. Dersom $a \equiv r' \pmod n$ der $r' \in \mathbb{N}_n$, har vi at $n \mid a - r'$, så det fins $q' \in \mathbb{Z}$ slik at $nq' = a - r'$. Dette gir $a = nq' + r'$ der $0 \leq r' < n$, så unikheten av r gir $r = r'$. Dette fullfører beviset. □

Proposisjon 6.22. *Kongruens modulo n er en ekvivalensrelasjon.*

Bevis. Refleksitivet: Siden $n \mid 0 = (a - a)$ for alle $a \in \mathbb{Z}$, har vi at $a \equiv a \pmod n$.

Symmetri: Anta at $a \equiv b \pmod n$. Da får vi at $n \mid (a - b)$, som gir $n \mid -(a - b) = b - a$. Dermed har vi $b \equiv a \pmod n$.

Transitivitet: Anta at $a \equiv b \pmod n$ og $b \equiv c \pmod n$. Dette gir $n \mid (a - b)$ og $n \mid (b - c)$. Fra dette følger det at

$$n \mid ((a - b) + (b - c)) = (a - c),$$

som gir $a \equiv c \pmod n$. □

Definisjon 6.23. Vi betegner kvotientmengden av $\mathbb{Z}$ med kongruens modulo n for $\mathbb{Z}_n$.

Proposisjon 6.24. *La $a, a', b, b' \in \mathbb{Z}$. Dersom $a \equiv a' \pmod n$ og $b \equiv b' \pmod n$, så gjelder*

$$\begin{aligned} a + b &\equiv a' + b' \pmod n, \\ ab &\equiv a'b' \pmod n. \end{aligned}$$

Videre utgjør $(\mathbb{Z}_n, +, \cdot, [0], [1])$ en kommutativ ring med de induserte binæroperasjonene

$$\begin{aligned} [a] + [b] &= [a + b], \\ [a][b] &= [ab], \end{aligned}$$

for $a, b \in \mathbb{Z}$.

Bevis. Anta at $a \equiv a' \pmod n$ og $b \equiv b' \pmod n$. Dette gir $n \mid (a - a')$ og $n \mid (b - b')$. Vi får da fra Proposisjon 6.4 (iv) at

$$n \mid (a - a') + (b - b') = (a + b) - (a' + b'),$$

altså $a + b \equiv a' + b' \pmod n$. I tillegg får vi fra Proposisjon 6.4 (iv) at

$$n \mid (a - a')b + a'(b - b') = ab - a'b',$$

som gir $ab \equiv a'b' \pmod n$.

Det er rett fram å sjekke at den resulterende kvotientmengden utgjør en kommutativ ring med de induserte binæroperasjonene. Vi overlater det som en oppgave. □

Følgende eksempel viser hvordan kongruensregning kan være nyttig.

Eksempel 6.25. Et kvadrattall er et tall på formen n^2 der $n \in \mathbb{N}$. La oss se hvilke mulige kvadrattall vi kan få modulo 3. Fra Lemma 6.21 vet vi at alle tall er kongruente med enten 0, 1 eller 2 modulo 3. I hvert av disse tilfellene gir Proposisjon 6.24 at

$$\begin{aligned} n \equiv 0 \pmod 3 &\implies n^2 \equiv 0^2 = 0 \pmod 3, \\ n \equiv 1 \pmod 3 &\implies n^2 \equiv 1^1 = 1 \pmod 3, \\ n \equiv 2 \pmod 3 &\implies n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3. \end{aligned}$$

Dette viser at alle kvadrattall må være kongruente med 0 eller 1 modulo 3. Muligheten 2 modulo 3 er altså utelatt.

Dette kan brukes på uventet vis. La oss betrakte ligningen

$$x^2 - 3y^2 = 2.$$

Det viser seg at denne ligningen ikke har noen heltallsløsninger, og en nyttig bevisstrategi er å vise at den ikke engang har noen løsninger i ringen $\mathbb{Z}_3$, eller "modulo 3": Antar vi at vi har en heltallsløsning gitt ved x og y, vil spesielt

$$x^2 - 3y^2 \equiv 2 \pmod 3.$$

Men Proposisjon 6.24 gir at $x^2 - 3y^2 \equiv x^2 - 0 \cdot y^2 = x^2 \pmod 3$. Videre vet vi at et kvadrattall kun kan være kongruent med 0 eller 1 modulo 3, så venstresiden av ligningen vil alltid gi 0 eller 1 modulo 3. Dermed kan den ikke være lik høyresiden, som er 2.

Proposisjon 6.26. *La $n \in \mathbb{N}$, $n \geq 1$. Da er følgende ekvivalent:*

(i) $\mathbb{Z}_n$ *er et integritetsområde.*
(ii) $\mathbb{Z}_n$ *er en kropp.*
(iii) n *er et primtall.*

Bevis. $(i) \Rightarrow (iii)$: Vi viser den kontrapositive implikasjonen. Anta at n ikke er et primtall. Vi kan da skrive $n = ab$ der $a, b \in \mathbb{Z}$ og $1 < a < n$ og $1 < b < n$. Det følger at $[a] \neq [0]$, $[b] \neq [0]$, og $[a][b] = [ab] = [n] = [0]$ i $\mathbb{Z}_n$. Dermed er $\mathbb{Z}_n$ ikke et integritetsområde.

$(iii) \Rightarrow (ii)$: La p være et primtall. La $[a] \in \mathbb{Z}_p$, $[a] \neq [0]$. Vi kan da anta at $1 \leq a < p$. Det følger at $a \wedge p = 1$, så ved Korollar 6.10 kan vi finne $x, y \in \mathbb{Z}$ slik at $az + py = 1$. Dermed har vi at

$$[1] = [az + py] = [a][z] + [p][y] = [a][z].$$

Vi har med andre ord funnet en invers til $[a]$ i $\mathbb{Z}_p$, som viser at $\mathbb{Z}_p$ er en kropp.

$(ii) \Rightarrow (i)$: Enhver kropp er et integritetsområde, så denne implikasjonen gjelder generelt. □

Kapittel 7

Reelle tall

I dette kapittelet skal vi se på en aksiomatisk framstilling samt en konstruksjon av de reelle tallene fra de rasjonale tallene. Dette dekkes i [1, Kapittel 8]. Mesteparten av dette kapittelet skal vi derimot utelate; vi ser i hovedsak på delkapitlene 8.1 og 8.7. Vi skal også se på en annen konstruksjon av de reelle tallene enn den som presenteres i [1, s. 8.7].

7.1 Dedekind-kompletthet

Vi skal snakke om totalt ordnede ringer i denne seksjonen, som vi tidligere definerte som sekstupler $(A, +, \cdot, 0, 1, \leq)$. Vi skal nå forenkle notasjonen vår litt og kalle simpelthen A selv en totalt ordnet ring, der resten av strukturen er implisitt tatt med.

Definisjon 7.1. Vi sier at en totalt ordnet ring A er *Dedekind-komplett* dersom følgende holder: Enhver ikke-tom, oppad begrenset delmengde av A har en minste øvre skranke (altså et supremum). Videre kaller vi en Dedekind-komplett totalt ordnet kropp for en *reell kropp*.

Merk at i en totalt ordnet ring A, så holder det at $x \in A$ er en øvre skranke for en mengde $U \subseteq A$ hvis og bare hvis $-x$ er en nedre skranke for $-U$. Det følger at A er Dedekind-komplett hvis og bare hvis enhver ikke-tom, nedad begrenset delmengde av A har et infimum.

Eksempel 7.2. Heltallene $\mathbb{Z}$ er Dedekind-komplett som en totalt ordnet ring: Vi viste i Proposisjon 5.55 at enhver ikke-tom, oppad begrenset delmengde av $\mathbb{Z}$ har et største element, som da spesielt er et supremum.

Eksempel 7.3. De rasjonale tallene $\mathbb{Q}$ utgjør ikke en rell kropp. Dette skal vi vise nå:

Definer

$$A = \{x \in \mathbb{Q} : x \geq 0,\ x^2 < 2\}.$$

Da gjelder følgende:

- A er ikke-tom, for $1 \in A$ siden $1 \geq 0$ og $1^2 = 1 < 2$.
- A er oppad begrenset, for 2 er en øvre skranke: Dersom vi hadde hatt $x \in A$ og $x > 2$, ville $x^2 > 2^2 = 4$, som motstrider at $x^2 < 2$.

Vi påstår derimot at A ikke har noe supremum. For å se dette antar vi for en selvmotsigelse at $s \in \mathbb{Q}$ er supremum for A. Vi setter nå

$$t = \frac{2s + 2}{s + 2}.$$

En utregning viser at

$$t - s = \frac{2 - s^2}{s + 2}, \quad t^2 - 2 = 2 \cdot \frac{s^2 - 2}{(s+2)^2}.$$

Vi deler nå inn i tre tilfeller:

- Dersom $s^2 < 2$, så gir identitetene over at $t - s > 0$ og $t^2 - 2 < 0$, altså er $t > s$ og $t^2 < 2$. Dermed er $t \in A$ og t er større enn s. Det motstrider at s er en øvre skranke for A.
- Dersom $s^2 > 2$, så gir identitetene istedet at $t - s < 0$ og $t^2 - 2 > 0$, altså er $t < s$ og $t^2 > 2$. Dermed har vi for enhver $x \in A$ at $x^2 < 2 < t^2$, og siden $x, t \geq 0$, gir dette $x < t$. Dette viser at t er en øvre skranke for A, men da motstrider $t < s$ at s er minste øvre skranke for A.
- Dersom $s^2 = 2$, får vi en selvmotsigelse fra Proposisjon 6.15.

Uansett ender vi opp med en selvmotsigelse. Konklusjonen blir da at $\mathbb{Q}$ ikke kan være en reell kropp.

Merknad 7.4. Dersom F er en reell kropp, kunne vi ha gjort nøyaktig samme argument som i Eksempel 7.3 for å vise at $s = \sup A$, som per antagelse eksisterer, må tilfredsstille $s^2 = 2$. Dette er en vanlig måte å konstruere kvadratroten av to på.

Gitt en reell kropp F og et element $x \in F$, så definerer vi $n \cdot x$ for $n \in \mathbb{N}$ rekursivt ved

$$\begin{aligned} 0 \cdot x &= 0, \\ (n+1) \cdot x &= n \cdot x + x, \qquad n \in \mathbb{N}. \end{aligned}$$

Dersom $x \geq 0$ er da $n \cdot x \geq 0$ for alle $n \in \mathbb{N}$, og dersom $x > 0$ er $n \cdot x > 0$ for alle $n \geq 1$ (vis disse ulikhetene ved induksjon). Videre kan en vise at

$$n \cdot x = (n \cdot 1)x, \qquad n \in \mathbb{N},$$

ved induksjon.

Dersom $k \in \mathbb{Z}$, si $k = n_1 - n_2$ der $n_1, n_2 \in \mathbb{N}$, så definerer vi

$$k \cdot x = n_1 \cdot x - n_2 \cdot x.$$

(Sjekk at dette er veldefinert!) Vi merker oss da at $x \geq 0$ og $k \leq l$ impliserer $k \cdot x \leq l \cdot x$, og dersom $x > 0$ og $k < l$ gjelder $k \cdot x < l \cdot x$. Spesielt har vi at $n \cdot x \neq 0$ dersom $n \neq 0$ og $x \neq 0$, så for et rasjonalt tall $q \in \mathbb{Q}$, si $q = k/l$ med $k, l \in \mathbb{Z}$ og $l \neq 0$, kan vi definere

$$q \cdot x = (k \cdot 1)(l \cdot 1)^{-1} x.$$

Proposisjon 7.5. *La F være en reell kropp. Da er funksjonen $\iota \colon \mathbb{Q} \to F$ gitt ved*

$$\iota(q) = q \cdot 1, \quad q \in \mathbb{Q}$$

injektiv og tilfredsstiller følgende for alle $q, r \in \mathbb{Q}$ og $x \in F$:

$$\begin{aligned} \iota(q + r) &= \iota(q) + \iota(r), \\ \iota(qr) &= \iota(q)\iota(r), \\ \iota(1) &= 1, \\ \iota(qr) \cdot x &= \iota(q) \cdot (\iota(r) \cdot x), \\ q \leq r &\iff \iota(q) \leq \iota(r). \end{aligned}$$

Bevis. Oppgave. □

Vi bruker injeksjonen i Proposisjon 7.5 til å anse $\mathbb{Q}$ som allerede sittende inne i F. Dermed tillater vi oss å skrive for eksempel $x-1/2$ der $x \in F$, der det er underforstått at $1/2 = \iota(1/2) = (1+1)^{-1}$.

Lemma 7.6. *La F være en reell kropp. Da holder følgende:*

(i) (Archimedes' egenskap) For alle $x, y \in F$ med $x > 0$ og $y > 0$ fins en $n \in \mathbb{N}$ slik at

$$n \cdot x > y.$$

(ii) For alle $x, y \in F$ med $x < y$ fins en $q \in \mathbb{Q}$ slik at

$$x < q < y.$$

Bevis. (i) Anta for en selvmotsigelse at mengden

$$A = \{n \cdot 1 : n \in \mathbb{N}\}$$

er oppad begrenset. Siden den er ikke-tom, gir Dedekind-kompletthet at den har et supremum $s = \sup A$. Siden $s - 1 < s$, kan ikke $s - 1$ være en øvre skranke for A. Det følger at det fins $n \in \mathbb{N}$ slik at $n \cdot 1 > s - 1$. Dette gir $s < n \cdot 1 + 1 = (n + 1) \cdot 1$, som motstrider at s er en øvre skranke for A. Vi konkluderer med at A ikke er oppad begrenset.

Spesielt kan ikke y/x være en øvre skranke for A, så det fins $n \in \mathbb{N}$ slik at $n \cdot 1 > y/x$. Dette gir $n \cdot x > y$.

(ii) La $x, y \in F$ med $x < y$. Ved (i) kan vi velge $n \in \mathbb{N}$ slik at $n \cdot (y - x) > 1$, altså $x + 1/n < y$. La m være det minste heltallet som er større enn $n \cdot x$, altså det minste elementet i mengden $\{m \in \mathbb{Z} : m \cdot 1 > n \cdot x\}$ (dette eksisterer ved versjonen av velordningsprinsippet i Proposisjon 5.55 (ii)). Vi har da at $m > n \cdot x$ og $m - 1 \leq n \cdot x$. Førstnevnte gir $x < m/n$, og sistnevnte gir at

$$m/n \leq x + 1/n < y.$$

Dermed tilfredsstiller $q = m/n$ egenskapen vi søker. □

Vi er nå klare til å skissere beviset av følgende resultat:

Teorem 7.7. *La F og F' være Dedekind-komplette totalt ordnede kropper. Da fins det en unik funksjon $\phi\colon F \to F'$ slik at følgende holder:*

(i) $\phi(x + y) = \phi(x) + \phi(y)$ *for alle* $x, y \in F$.
(ii) $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ *for alle* $x, y \in F$.
(iii) $\phi(1_F) = 1_{F'}$.

Videre er ϕ en bijeksjon, og den bevarer ordningene i følgende forstand:

$$x \leq y \quad \Longleftrightarrow \quad \phi(x) \leq \phi(y), \qquad x, y \in F.$$

Bevis. Vi deler beviset inn i fem steg.

Steg 1: La først F og F' være reelle kropper, og la $\iota\colon \mathbb{Q} \to \perp$ og $\iota'\colon \mathbb{Q} \to F'$ betegne inklusjonene av $\mathbb{Q}$ inn i henholdsvis F og F' fra Proposisjon 7.5. La $x \in F$ og definer

$$A_x = \{\iota'(q) \ : \ q \in \mathbb{Q},\ \iota(q) < x\} \subseteq F'.$$

Vi påstår at A_x er ikke-tom og oppad begrenset: Vi kan finne en $q \in \mathbb{Q}$ slik at $\iota(q) < x$ fra Lemma 7.6, og da er $\iota'(q) \in A_x$. Videre, la $r \in \mathbb{Q}$ med $x < \iota(r)$ fra Lemma 7.6. Dersom $q \in \mathbb{Q}$ tilfredsstiller $\iota(q) < x$, så får vi $\iota(q) < \iota(r)$, som gir $q < r$ fra egenskapene til ι. Dermed er $\iota'(q) < \iota'(r)$. Dette viser at A_x er oppad begrenset av $\iota'(r)$.

Definer nå en funksjon $\phi\colon F \to F'$ ved

$$\phi(x) = \sup A_x, \qquad x \in F.$$

Merk at denne mengden er begrenset ovenifra av x og ikke-tom ved Lemma 7.6. Vi merker oss at $\phi(q) = q$ for alle $q \in \mathbb{Q}$. Spesielt gjelder $\phi(1_F) = 1_{F'}$. Beviset for egenskap (i) og (ii) overlater vi som en oppgave.

Steg 2: Her viser vi at dersom $\phi'\colon F \to F'$ tilfredsstiller egenskapene (i) og (iii), så må $\phi'(q) = q$ for alle $q \in \mathbb{Q}$.

Vi merker oss først at (i) gir $\phi'(n \cdot 1) = n \cdot \phi'(1) = n \cdot 1$ for alle $n \in \mathbb{N}$. Fra egenskap (i) må ϕ' nødvendigvis bevare additive inverser, og da følger det fra definisjonen av $k \cdot 1$ for $k \in \mathbb{Z}$ at $\phi'(k \cdot 1) = k \cdot \phi'(1) = k \cdot 1$. Til slutt lar vi $q = k/l$ være et rasjonalt tall der $k, l \in \mathbb{Z}$ og $l \neq 0$, og observerer at

$$l \cdot \phi'(q \cdot 1) = \phi'(k \cdot 1) = k \cdot 1 = l \cdot (q \cdot 1).$$

Siden $l \neq 0$ kan vi konkludere med at $\phi'(q \cdot 1) = q \cdot 1$.

Steg 3: Her viser vi at dersom $\phi'\colon F \to F'$ tilfredsstiller egenskapene (i), (ii), og (iii), så må ϕ' ha egenskapen

$$x \leq y \implies \phi'(x) \leq \phi'(y), \qquad x, y \in F.$$

Anta først at $x \geq 0$. Ved en generalisering av beviset i Merknad 7.4 fins $t \in F$ slik at $t^2 = x$. Vi får da ved å bruke egenskap (ii) at

$$\phi'(x) = \phi'(t)^2 \geq 0$$

siden kvadrater alltid er ikke-negative, se Proposisjon 5.54 (iii).

Mer generelt, dersom $x \leq y$, har vi $y - x \geq 0$, så $\phi(y - x) \geq 0$ ved det vi nettopp viste. Men da gir egenskap (i) at $\phi(y) - \phi(x) \geq 0$, altså $\phi(x) \leq \phi(y)$.

Steg 4: Her viser vi at dersom $\phi'\colon F \to F'$ tilfredsstiller egenskapene (i), (ii) og (iii), så må $\phi' = \phi$ fra Steg 1. La $x \in F$. Dersom $\phi(x) < \phi'(x)$, kan vi finne $q \in \mathbb{Q}$ ved $\phi(x) < q < \phi'(x)$ ved Lemma 7.6 (ii). Dersom $x \geq q$, får vi at $\phi(x) \geq \phi(q) = q > \phi(x)$, en selvmotsigelse. Dersom $x \leq q$, får vi at $\phi'(x) \leq \phi'(q) = q < \phi'(x)$, en selvmotsigelse. Antagelsen $\phi(x) > \phi'(x)$ gir tilsvarende en selvmotsigelse. Vi konkluderer derfor med at $\phi(x) = \phi'(x)$. Dette viser at $\phi = \phi'$.

Steg 5: Her viser vi at ϕ må være en bijeksjon. Ved å bytte rollene til F og F' i Steg 1 får vi en funksjon $\psi\colon F' \to F$ som har egenskapene (i), (ii) og (iii) i teoremet. Da må komposisjonene $\psi \circ \phi\colon F \to F$ og $\phi \circ \psi\colon F' \to F'$ ha alle egenskapene i teoremet. Ved entydigheten får vi dermed at $\psi \circ \phi = \mathrm{id}_F$ og $\phi \circ \psi\colon \mathrm{id}_{F'}$, siden identitetsfunksjonene også har alle disse egenskapene. Siden ϕ er injektiv, holder nå spesielt ekvivalensen

$$x \leq y \quad \iff \quad \phi(x) \leq \phi(y), \qquad x, y \in F.$$

Dette fullfører beviset. □