Diskrete Matematiske Metoder
2. udgave

Jesper Lützen

Juli 2019

Indhold

Forord

Disse noter er skrevet til undervisningen i kurset Diskrete Matematiske Metoder ved Institut for Matematiske Fag, Københavns Universitet. Denne udgave afviger på mange måder fra de tidligere noter med samme navn.

Introduktion

Disse noter har et dobbelt formål: Dels skal de introducere nogle emner i diskret matematik, dels skal de træne læseren i matematisk metode, især beviser.

0.1 Den aksiomatisk-deduktive metode

Mange videnskaber er karakteriseret ved de objekter de omhandler: Botanik handler om planter og astronomi om himmelleger. Matematik er derimod karakteriseret ved sin metode. Det karakteristiske ved matematikken er at dens resultater kræver beviser. Naturligvis argumenterer man også i andre videnskaber, men i matematik er argumenterne eller beviserne mere stringente (dvs. strenge, præcise) end i andre videnskaber. Det er nok en væsentlig grund til at matematiske resultater har vist sig mere langtidsholdbare end resultaterne i andre videnskaber.

En matematisk sætning regnes for sand hvis den kan bevises ved logisk gyldige argumenter ud fra andre sætninger, som man ved er sande. Men disse andre sætninger bør jo så også bevises ud fra endnu andre o.s.v. For at bevisprocessen kan komme i gang, er det derfor klart, at man må begynde med sætninger, som man ikke kræver beviser for, men som man postulerer. Det er de såkaldte aksiomer. Den her beskrevne metode kaldes den aksiomatisk-deduktive metode, fordi den fra aksiomer successivt deducerer (udleder, beviser) nye resultater.

Denne beskrivelse af den matematiske metode rejser to væsentlige problemer: Hvilke aksiomer skal man lægge til grund for matematikken og hvilke argumenter (slutningsregler) skal man acceptere som gyldige? Disse spørgsmål om matematikkens grundlag er emnet for et kursus i matematisk logik og mængdelære. Her vil vi nok opstille regler for korrekte slutninger (argumenter) og vi vil opstille aksiomer for visse dele af matematikken (de naturlige tal, de reelle tal, ækvivalensrelationer og grupper). Men vi vil ikke gå til bunds med grundlagsproblemerne. For eksempel vil vi ikke præcisere slutningsreglerne i mindste detalje, og vi vil ikke føre vore deduktioner tilbage til aksiomerne for mængdelæren, selv om disse aksiomer ligger til grund for den videre aksiomatisering af for eksempel tallene.

Kurset er et håndværkskursus. Vi vil introducere logikken som et værktøj, der bruges til daglig af arbejdende matematikere. Ligeså vil vi introducere

mængder som samlinger af ting uden at kære os om de subtile problemer, der måtte være resultatet af en sådan "naiv" tilgang til mængdelæren. Det er formålet med bogen at læseren skal kunne lære, hvordan han/hun skal læse og selv fremstille beviser for sætninger på et niveau af stringens, som er sædvanligt i matematisk forsknings- og lærebogslitteratur. Til det brug diskuterer vi særligt udbredte bevistyper og -strategier.

0.2 Diskret matematik; hvad er det?

Et andet formål er at introducere og præcicere nogle matematiske begreber, som indgår i mange matematiske sammenhænge: mængder, relationer, funktioner, permutationer, grafer, restklasser, ækvivalensrelationer, ordningsrelationer, grupper, polynomier, de hele og de reelle tal. Disse emner (på nær de reelle tal) hører hjemme i den del af matematikken som kaldes diskret matematik. Vi skal studere disse begreber og vise nogle af deres mange interessante egenskaber. Behandlingen i disse noter kan dog kun betragtes som en kort indledende indføring.

Diskret matematik er ikke betegnelsen for en en slags matematik man dyrker på en særlig taktfuld og afdæmpet måde. Ifølge *Den Store Danske Encyclopædi* betyder diskret, "inden for matematik adskilt eller ikke-kontinuert. En diskret mængde er således en mængde bestående udelukkende af isolerede punkter; en variabel kaldes diskret, hvis den kun kan antage værdier i en diskret mængde". Diskret matematik beskrives i samme værk på følgende måde:

"Diskret matematik, samlebetegnelse for de grene af matematikken, hvor den matematiske analyses kontinuitetsbegreb (jf. kontinuert funktion) ikke spiller en afgørende rolle. Diskret matematik er ikke et afgrænset forskningsområde, men omfatter dele af flere matematiske discipliner, fx grafteori, kombinatorik, logik og algebra. Betegnelsen, der vandt indpas i 1970'erne, bruges bl.a. i forbindelse med datalogiske anvendelser; forskellen mellem diskret og kontinuert kan opfattes som parallel til forskellen mellem digital og analog datarepræsentation."

Om ordet "diskret" forklarer *Ordbog over det danske Sprog* endvidere at det kommer fra det latinske "discretus", som er perfektum participiom af dis - cernere, adskille. Derfor er det ikke overraskende at det i matematik iflg samme ordbog bruges: "om størrelse, hvis dele er adskilt fra hinanden, ell. som kun kan antage en række indbyrdes adskilte talværdier". Den ikke matematiske og mere udbredte brug af ordet kommer egentlig af den oldgermanske betydning: "som har evne til at skelne, skønne". Derfra har det fået betydningen:"forsigtig og beskeden i optræden og tale; taktfuld; hensynsfuld; ofte spec.: som ikke røber hemmeligheder" og den overførte betydning "som ikke er for meget iøjne- ell. iørefaldende; dæmpet; fin".

0.3 Aksiomerne for de reelle tal

Som et eksempel på et (stort) aksiomssystem skal her nævnes aksiomssystemet for de reelle tal.

Definition 1 *De* ***reelle tal*** $\mathbb{R}$ *er en mængde med to kompositionsregler (regneoperationer, regningsarter)* $+$ *og* $\cdot$*, to forskellige tal* 0 *og* 1*, samt en ordningsrelation* $\leqq$*. Desuden findes der til ethvert reelt tal* x *et tal* $-x$*, og til ethvert reelt tal* x *forskelligt fra* 0 *findes der et tal* x^{-1}*. De reelle tal skal desuden opfylde følgende regneregler:*

For vilkårlige reelle tal x, y, z *gælder:*

$$x + y = y + x. \qquad \textit{Den kommutative lov for addition} \tag{1}$$

$$(x + y) + z = x + (y + z)\,. \qquad \textit{Den associative lov for addition} \tag{2}$$

$$x + 0 = 0 + x = x. \qquad \textit{0 er neutralt element for addition} \tag{3}$$

$$x + (-x) = (-x) + x = 0. \qquad -x \textit{ er den additivt inverse til } x \tag{4}$$

$$xy = yx. \qquad \textit{Den kommutative lov for multiplikation} \tag{5}$$

$$(xy)z = x(yz). \qquad \textit{Den associative lov for multiplikation} \tag{6}$$

$$x \cdot 1 = 1x = x. \qquad 1 \textit{ er neutralt element for multiplikation} \tag{7}$$

$$xx^{-1} = x^{-1}x = 1, \ \textit{når} \ x \neq 0. \ x^{-1} \textit{ er multipl. invers til } x \tag{8}$$

$$x(y + z) = xy + xz, \quad (x + y)z = xz + yz. \quad \textit{Den distributive lov} \tag{9}$$

$$x \leq y \textit{ eller } y \leq x. \qquad \textit{Ordningen er total} \tag{10}$$

$$x \leq x. \qquad \leq \textit{ er refleksiv} \tag{11}$$

$$\textit{hvis } x \leq y \textit{ og } y \leq z \textit{ så er } x \leq z. \qquad \leq \textit{ er transitiv} \tag{12}$$

$$\textit{hvis } x \leq y \textit{ og } y \leq x \textit{ så er } x = y. \qquad \leq \textit{ er antisymmetrisk} \tag{13}$$

$$\textit{hvis } x \leq y \textit{ så er } x + z \leq y + z. \qquad \leq \textit{ harmonerer med } + \tag{14}$$

$$\textit{hvis } x \leq y \textit{ og } 0 \leq z, \textit{ så er } xz \leq yz. \qquad \leq \textit{ harmonerer med } \cdot \tag{15}$$

Desuden gælder supremumsegenskaben: enhver ikke tom opadtil begrænset delmængde af de reelle tal har et supremum.

Man kan opfatte ovenstående egenskaber ved de reelle tal på to måder: Enten som en liste af simple egenskaber, som vi har lært i skolen, eller som et aksiomssystem, som fuldstændigt beskriver de reelle tal. Vi skal anlægge det sidstnævnte synspunkt. Det betyder at alle andre sætninger om de reelle tal skal udledes (deduceres) ud fra de ovenstående aksiomer. I kapitel (3) vil vi bevise mange af de basale regneregler for regning med reelle tal ud fra aksiomerne.

Historisk er der ingen vigtige matematiske teorier, som er opstået ved at man er begyndt med aksiomerne. Normalt udvikles en matematisk teori først uformelt. Når teorien så er tilstrækkelig udbygget begynder man ofte at savne et solidt fundament og det fører til en aksiomatisering af teorien. For eksempel opstod ideen om reelle tal som en idé om måltal for geometriske og andre størrelser. Først i midten af 1800-tallet opstod der problemer med dette intuitive

talbegreb især inden for den matematiske analyse. En måde at komme uden om problemerne blev at aksiomatisere teorien. Når en uformel teori aksiomatiseres udvælger man en række af de fundamentale sætninger i teorien og ophøjer dem til aksiomer. Der skal være nok aksiomer til at teoriens sætninger alle kan vises ud fra aksiomerne. Men aksiomerne skal helst være uafhængige, i den forstand at ingen af dem kan bevises ud fra de andre. Desuden må der ikke være modstrid i systemet.

Valget af et aksiomssystem for en uformel teori er ikke entydigt. I det ovennævnte aksiomssyatem har vi for eksempel opskrevet aksiomer for ulighedsrelationen $\leq$. En anden mulighed er at erstatte aksiomerne (10)-(15) med følgende to aksiomer for de positive reelle tal $\mathbb{R}_+$:

Der findes en delmængde $\mathbb{R}_+$ af $\mathbb{R}$ hvorom det gælder:

O1: $\mathbb{R}_+$ er lukket under $+$ og $\cdot$, dvs. for alle $x, y \in \mathbb{R}_+$ gælder:

$$x + y \in \mathbb{R}_+ \quad \text{og} \quad x \cdot y \in \mathbb{R}_+$$

O2: For alle $x, y \in \mathbb{R}$ gælder præcist ét af følgende udsagn:

$$x \in \mathbb{R}_+$$
$$x = 0$$
$$-x \in \mathbb{R}_+.$$

De to ovennævnte aksiomssystemer for de reelle tal er ækvivalente. De giver altså anledning til den samme teori. Det vises ved at bevise at aksiomerne i det ene aksiomssystem kan bevises ud fra aksiomerne i det andet system og vice versa. I kapitel 3 viser vi således aksiomerne O1 og O2 ud fra det førstnævnte aksiomssystem, idet vi som $\mathbb{R}_+$ bruger mængden $\{x \in \mathbb{R} \mid 0 \leq x \wedge x \neq 0\}$. Omvendt, kan aksiomerne (10)-(15) bevises ud fra (1)-(9) samt O1 og O2 når relationen $\leq$ defineres ved

$$x \leq y \Leftrightarrow (y - x) \in \mathbb{R}_+ \cup \{0\}$$

.

Men før vi går i gang med at bevise sætninger om de reelle tal ud fra aksiomerne, skal vi mere generelt se på forskellige bevismetoder og de logiske principper, der ligger til grund for dem.

Kapitel 1

Logik

Dette kapitel omhandler matematiske udsagn og prædikater. I et formelt kursus om logik opstiller man helt præcise regler for hvilke tegnstrenge, der kan tillades i opbygningen af udsagn og prædikater. I disse noter vil vi blot præcisere dagligdags logik.

1.1 Udsagn og prædikater

Definition 2 *Et (matematisk)* ***udsagn*** *er en udtalelse som er enten sand eller falsk.*

Eksempel 3

$$1 < 2 \quad og \quad 1 > 2 \tag{1.1}$$

er begge udsagn. Det første er sandt det andet er falsk. Derimod er

$$1 \int 2 \quad og \quad "matematik\ er\ smukt" \tag{1.2}$$

ikke udsagn.

Notation 4 *Vi betegner normalt udsagn med små bogstaver: $p, q, ...$*

Eksempel 5 *Betragt udtalelsen: $x < 2$. Det er ikke et udsagn, for når vi ikke har fastlagt værdien af x, er det hverken sandt eller falsk. Derimod bliver det et udsagn, når vi tillægger x en bestemt reel værdi. Vi siger da at x er en* ***fri variabel*** *og kalder $x < 2$ for et prædikat i denne variabel.*

Definition 6 *En udtalelse, der indeholder en fri variabel, kaldes et* ***prædikat*** *(eller et åbent udsagn) om elementerne i en given mængde. Det bliver et udsagn, når den frie variabel erstattes med et bestemt element i den givne mængde.*

Bemærkning 7 *Man kan på helt analog måde definere prædikater med flere frie variable. For eksempel er $x^2 > y$ et prædikat i to reelle variable.*

Notation 8 *Vi betegner normalt et prædikat i den variable x med $p(x)$, $q(x)$,.... Prædikater i to variable x og y betegnes med $p(x,y)$, $q(x,y)$, og så videre.*

Bemærkning 9 *Man skriver aldrig lighedstegn mellem prædikater. Hvis forek-sempel $p(x)$ betegner prædikatet $x^3+5x^2+7<3$, kan man skrive*

$$p(x) : x^3+5x^2+7<3$$

*men man kan **ikke** skrive $p(x) = x^3+5x^2+7<3$. Man kunne få brug for at benævne polynomiet x^3+5x^2+7 med et særligt symbol, men så må man bruge et andet symbol end $p(x)$ fx. $P(x)$. Hvis man gør det kan man skrive $P(x) = x^3+5x^2+7$. I så fald er $p(x)$ et prædikat og $P(x)$ er en funktion. Det er vigtigt at sondre mellem prædikater og funktioner!*

Bemærkning 10 *Man skal læse prædikater med omhu. For eksempel ligner prædikatet*

$$\int_0^x e^{2t}dt = 5$$

et prædikat i de to variable x og t. Men her er integrationsvariablen t faktisk bundet og kan ikke tillægges en vilkårlig værdi. Prædikatet er altså et prædikat i den ene frie variable x.

1.2 Sammensatte udsagn

Man kan lave sammensatte udsagn ud fra simple udsagn ved at bruge de logiske **konnektiver** $\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow$. Sandheden af de sammensatte udsagn afhænger alene af sandheden af de indgående simple udsagn.

Definition 11 *Lad p og q være udsagn. Da defineres følgende sammensatte udsagn:*

- Konjunktion: $p \wedge q$ (læses "p og q") er sandt når både p og q er sande og ellers falsk.
- Disjunktion: $p \vee q$ (læses "p eller q") er sandt når enten p eller q eller de begge er sande og falsk når både p og q er falske.
- Negation: $\neg p$ (læses "non p") er sand når p er falsk og falsk når p er sand. I nogle bøger skrives $\sim p$ i stedet for $\neg p$.
- Implikation: $p \Rightarrow q$ (læses "p medfører q" eller "hvis p så q" eller "p kun hvis q") er falsk når p er sand og q er falsk; ellers er det sandt. Med andre ord siger implikationen $p \Rightarrow q$ at når p er sand så er q også sand, og den siger ikke mere end det. Man kan også skrive $q \Leftarrow p$ i stedet for $p \Rightarrow q$. Man kalder p for hypotesen og q for konklusionen.
- Biimplikation (ækvivalens): $p \Leftrightarrow q$ (læses "p er ensbetydende med q" eller "p hvis og kun hvis q") er sand hvis p og q har samme sandhedsværdi.

Sandhedstabeller. Man kan illustrere og præcisere disse definitioner i en tabel, hvori man anfører alle kombinationer af p's og q's sandhedsværdi (s for sand og f for falsk) og de tilhørende sandhedsværdier af de sammensatte udsagn:

p	q	$p \wedge q$	$p \vee q$	$\neg p$	$p \Rightarrow q$	$p \Leftrightarrow q$
s	s	s	s	f	s	s
s	f	f	s	f	f	f
f	s	f	s	s	s	f
f	f	f	f	s	s	s

(1.3)

Mere komplekse sammensatte udsagn. Man kan danne mere komplekse sammensatte udsagn ved at bruge tegnene $\wedge, \vee, \neg, \Rightarrow$ og $\Leftrightarrow$ efter hinanden. For eksempel kan man fra de tre simple udsagn p, q og r danne udsagnet: $(\neg(p \vee q)) \Rightarrow r$. En sandhedstabel for dette udsagn kan fås ved at kombinere informationerne i den ovenstående sandhedstabel:

p	q	r	$p \vee q$	$\neg(p \vee q)$	$(\neg(p \vee q)) \Rightarrow r$
s	s	s	s	f	s
s	s	f	s	f	s
s	f	s	s	f	s
s	f	f	s	f	s
f	s	s	s	f	s
f	s	f	s	f	s
f	f	s	f	s	s
f	f	f	f	s	f

(1.4)

Definition 12 *Et sammensat udsagn, som er falsk for alle sandhedsværdier af de indgående simple udsagn kaldes en* ***modstrid****.*

Eksempel 13 *Det sammensatte udsagn $p \wedge (\neg p)$ er en modstrid. Det ses let af sandhedstabellen:*

p	$\neg p$	$p \wedge (\neg p)$
s	f	f
f	s	f

(1.5)

Definition 14 *Et sammensat udsagn, som er sandt for alle sandhedsværdier af de indgående simple udsagn kaldes en* ***tautologi****.*

Eksempel 15 *Det sammensatte udsagn $((p \Rightarrow q) \wedge (q \Rightarrow p)) \Leftrightarrow (p \Leftrightarrow q)$ er en tautologi. Det ses af nedenstående sandhedstabel:*

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$	$(p \Leftrightarrow q)$	$((p \Rightarrow q) \wedge (q \Rightarrow p)) \Leftrightarrow (p \Leftrightarrow q)$
s	s	s	s	s	s	s
s	f	f	s	f	f	s
f	s	s	f	f	f	s
f	f	s	s	s	s	s

(1.6)

Det her betragtede udsagn $((p \Rightarrow q) \wedge (q \Rightarrow p)) \Leftrightarrow (p \Leftrightarrow q)$ er en tautologi, fordi $((p \Rightarrow q) \wedge (q \Rightarrow p))$ og $(p \Leftrightarrow q)$ er sande for de samme kombinationer af sandhedsværdier af p og q. Man kan da opfatte dem som det samme udsagn, og vi siger at de er logisk ækvivalente. Man kan m.a.o. opfatte $(p \Leftrightarrow q)$ som en forkortelse af $(p \Rightarrow q) \wedge (q \Rightarrow p)$ eller kort skrevet: $\Leftrightarrow$ er en forkortelse for $\Rightarrow \wedge \Leftarrow$.

Notation 16 *Ligesom i almindelig algebra er der konventioner for i hvilken rækkefølge, man skal læse de logiske konnektiver. I et udtryk af formen $xy + z$ skal man foretage multiplikationen før additionen. På samme måde skal $\neg p \wedge q$ læses som $(\neg p) \wedge q$ og ikke som $\neg (p \wedge q)$. Vi siger at $\neg$ er mindst dominerende (skal bruges først) og $\wedge$ er mere dominerende (skal bruges bagefter). I følgende tabel er angivet hvilke af konnektiverne, der dominerer over hvilke:*

mindst dominerende	$\neg$, *negation*	*brug først*
	$\wedge$, *konjunktion;* $\vee$, *disjunktion*	
	$\Rightarrow$, *implikation*	
mest dominerende	$\Leftrightarrow$, *biimplikation*	*brug sidst*

(1.7)

Bemærk, at der ikke er nogen vedtagen rækkefølge for $\wedge$ og $\vee$. Et udtryk af formen $p \wedge q \vee r$ har altså ingen mening, før man sætter parenteser: enten $(p \wedge q) \vee r$ eller $p \wedge (q \vee r)$. Selv i tilfælde, hvor der er en konvention om rækkefølgen af konnektiverne, kan det lette læsningen at sætte parenteser i udtryk for sammensatte udsagn.

Øvelse 17 *Sæt parenteser i følgende sammensatte udsagn:*

$$p \vee \neg q \tag{1.8}$$

$$p \Rightarrow q \vee r \tag{1.9}$$

$$p \Rightarrow q \Leftrightarrow r \tag{1.10}$$

$$p \wedge q \Leftrightarrow r \Rightarrow \neg q \tag{1.11}$$

Definition 18 *To sammensatte udsagn p og q kaldes **logisk ækvivalente**, og vi skriver $p \equiv q$, hvis $p \Leftrightarrow q$ er en tautologi.*

Sætning 19 ***Logisk huskeseddel.*** *Det er praktisk at huske følgende logiske ækvivalenser udenad*

$$\neg\neg p \equiv p \ , \tag{1.12}$$

$$p \ \wedge \ q \equiv q \ \wedge \ p \ , \qquad p \ \vee \ q \equiv q \ \vee \ p \ , \tag{1.13}$$

$$(p \ \wedge \ q) \wedge \ r \equiv p \ \wedge (q \ \wedge \ r) \ , \qquad (p \ \vee \ q) \vee \ r \equiv p \ \vee (q \ \vee \ r) \ , \tag{1.14}$$

$$(p \ \wedge \ q) \vee \ r \equiv (p \ \vee \ r) \wedge (q \ \vee \ r) \ , \qquad (p \ \vee \ q) \wedge \ r \equiv (p \ \wedge \ r) \vee (q \ \wedge \ r) \ , \tag{1.15}$$

$$\neg(p \ \wedge \ q) \equiv \ \neg p \ \vee \neg q \ , \qquad \neg(p \ \vee \ q) \equiv \ \neg p \ \wedge \neg q \ , \tag{1.16}$$

$$p \Rightarrow q \ \equiv \ \neg p \ \vee \ q \ , \tag{1.17}$$

$$\neg \, (p \Rightarrow q) \ \equiv \ p \ \wedge \neg \ q \ , \tag{1.18}$$

$$p \Rightarrow q \ \equiv \ \neg q \Rightarrow \neg p \tag{1.19}$$

Bevis. Disse logiske ækvivalenser kan eftervises ved at betragte sandhedstabellerne for udsagnene. ■

Definition 20 *Når $p \Rightarrow q$ er en implikation kaldes implikationen $\neg q \Rightarrow \neg p$ den **kontraponerede** implikation.*

Ifølge (1.19) er en implikation og dens kontraponerede logisk ækvivalente.

Definition 21 *Når $p \Rightarrow q$ er en implikation kaldes $q \Rightarrow p$ den omvendte implikation.*

Øvelse 22 *Vis ved et eksempel, at en implikation og dens omvendte ikke er logisk ækvivalente.*

Bemærkning 23 *For at fremme forståelsen omformer man helst sammensatte udsagn og prædikater så de **så vidt muligt ikke indeholder negationer**. For eksempel vil man om et naturligt tal hellere sige at "x er et lige primtal" end at sige: "x er hverken sammensat eller ulige".*

Øvelse 24 *Vis ved hjælp af reglerne på huskesedlen, at de to prædikater i Bemærkning 23 ovenfor er logisk ækvivalente.*

Øvelse 25 *Vis, at $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ er en tautologi.*

Notation 26 *På grund af ovenstående resultat kan man tillade sig at forkorte udsagnet $(p \Rightarrow q) \wedge (q \Rightarrow r)$ til $p \Rightarrow q \Rightarrow r$.*

1.3 Sammensætning af prædikater

Man kan naturligvis sammensætte prædikater på samme måde som udsagn. Hvis $p(x)$ og $q(x)$ er prædikater om elementerne i mængden M, kan man for eksempel danne prædikatet $p(x) \wedge q(x)$. Når x erstattes af et bestemt element i M, bliver $p(x)$ og $q(x)$ til udsagn, og dermed bliver også $p(x) \wedge q(x)$ til et udsagn.

Konvention. På tilsvarende vis kan man ud fra prædikaterne $p(x)$ og $q(x)$ danne prædikaterne $p(x) \Rightarrow q(x)$ og $p(x) \Leftrightarrow q(x)$. Men her er der en konvention om at læse $p(x) \Rightarrow q(x)$ og $p(x) \Leftrightarrow q(x)$ ikke som prædikater i den frie variabel x, men som udsagnene: "$p(x) \Rightarrow q(x)$ for alle x i M" og "$p(x) \Leftrightarrow q(x)$ for alle x i M". Med denne gængse fortolkning betyder $p(x) \Rightarrow q(x)$ altså: "$q(x)$ er sand for alle de værdier af x, som gør $p(x)$ sand" eller "Hvis $p(x)$ er sand for en værdi af x, så er $q(x)$ sand for den samme værdi af x". På samme vis læses $p(x) \Leftrightarrow q(x)$ altså som udsagnet: "$p(x)$ og $q(x)$ er sande for de samme værdier af x".

Bemærkning 27 *Det kan virke underligt, at man definerer at $p \Rightarrow q$ er sand når både p og q er falske.*

Betragt for eksempel følgende implikationer:

$$2 < 1 \Rightarrow \sin 2 = 10^5. \tag{1.20}$$

"Hvis Wolfgang Amadeus Mozart er præsident i USA, (1.21)

så er månen lavet af grøn ost" (1.22)

I vores almindelige omgang med sproget vil vi nok karakterisere disse udsagn som noget vrøvl, dels fordi hypotesen ikke har noget at gøre med konklusionen, og dels fordi de fire elementære udsagn, implikationerne er sammensat af, alle er falske. Men i matematisk logik er udsagnene sande.

For at forstå hvorfor man har valgt at noget falsk kan medføre både noget falsk og noget sandt, kan vi se på implikationer $p(x) \Rightarrow q(x)$ mellem prædikater, for her svarer konventionen meget bedre til vores umiddelbare dagligdags omgang med sproget. Betragt for eksempel følgende implikation om reelle tal:

$$x > 2 \Rightarrow x^2 > 4 \tag{1.23}$$

Hvis vi skal vise at denne implikation er sand er vores umiddelbare strategi at undersøge x'er som er større end 2 og vise at de har $x^2 > 4$. Da dette er korrekt, slutter vi at implikationen er sand. Vi undersøger slet ikke hvad der sker når x er mindre end eller lig med 2, fordi vi opfatter disse værdier af x som irrelevante for implikationens sandhedsværdi. Denne strategi er korrekt, netop fordi vi har defineret, at $p \Rightarrow q$ er sand, hvis p er falsk (uanset sandhedsværdien af q). Konventionen ovenfor betyder jo, at implikationen $x > 2 \Rightarrow x^2 > 4$ skal læses "$x > 2 \Rightarrow x^2 > 4$ for alle $x \in \mathbb{R}$". Vi burde altså egentligt undersøge alle reelle x, men netop fordi vi har defineret at $x > 2 \Rightarrow x^2 > 4$ er sand for de x, der ikke opfylder $x > 2$, er der ingen grund til at undersøge sådanne x'er. Altså er det nok at undersøge de værdier af x, som gør hypotesen sand.

1.4 Kvantorer

Definition 28 *Ud fra et prædikat $p(x)$ om elementerne i en mængde M kan vi danne to udsagn:*

Udsagnet

$$\forall x \in M : p(x) \tag{1.24}$$

er sandt, netop når $p(x)$ er sand for alle elementerne x i M. Man siger (og skriver): "for alle (eller for ethvert, eller for et vilkårligt) x i M (gælder) $p(x)$".

Udsagnet

$$\exists x \in M : p(x) \tag{1.25}$$

er sandt, netop når der eksisterer (mindst) et element x i M, som gør $p(x)$ sand. Man siger (og skriver): "Der eksisterer et x i M, så $p(x)$".

*Tegnene $\forall$ og $\exists$ kaldes **kvantorer**. $\forall$ kaldes **al-kvantoren** og $\exists$ kaldes **eksistens-kvantoren**.*

Eksempel 29 *Betragt prædikatet $p(x)$: $x^2 \geq 0$. Dette prædikat bliver et sandt udsagn, uanset hvilket reelt tal vi sætter ind på x's plads. Altså er udsagnet $\forall x \in \mathbb{R} : x^2 \geq 0$ sandt. Vi siger at "for alle reelle x gælder $x^2 \geq 0$".*

Eksempel 30 *Udsagnet $\exists x \in \mathbb{R} : x^2 < 1$ er sandt, da der findes et x (for eksempel $x = 0$), som gør prædikatet $x^2 < 1$ sandt. Derimod er $\forall x \in \mathbb{R} : x^2 < 1$ et falsk udsagn, da prædikatet $x^2 < 1$ ikke er sandt for alle $x \in \mathbb{R}$. Det er jo for eksempel falsk for $x = 5$.*

Bemærkning 31 *Når man sætter en kvantor foran den frie variabel i et prædikat i én variabel, får man et udsagn og ikke et prædikat. Variablen er ikke længere fri og kan ikke tillægges forskellige værdier. Man siger da at den variable er bunden.*

Eksempel 32 *Betragt tegnstrengen: $\forall x \in \mathbb{R} : x^2 \geq 0$. Det er ikke et prædikat men et udsagn (som er sandt), og da der står en alkvantor foran x, er dette en bunden variabel.*

Konvention. Den ovennævnte konvention kan nu formuleres som følger: $p(x) \Rightarrow q(x)$ skal normalt fortolkes som udsagnet: $\forall x : p(x) \Rightarrow q(x)$; og $p(x) \Leftrightarrow q(x)$ skal normalt fortolkes som $\forall x : p(x) \Leftrightarrow q(x)$.

Bemærkning 33 *Hvis det er helt klart hvilken mængde variablen x varierer over, kan man udelade at angive denne når man kvantificerer over x. Hvis det for eksempel er klart at vi arbejder med de reelle tal, kan man skrive $\forall x : x^2 \geq 0$*

1.5 Flere kvantorer

Hvis $p(x, y)$ er et prædikat i de to variable x og y, og vi kvantificerer over den ene variabel (f.eks x), så vil resultatet være et prædikat i den anden variabel.

Eksempel 34 *Prædikatet* $\forall x \in \mathbb{R} : x^2 > y$ *er et prædikat i den fri reelle variabel* y*. Derimod er* x *en bunden variabel. Prædikatet er sandt for negative værdier af* y *og falsk for positive værdier af* y*.*

Bemærkning om flere kvantorer. Da $\forall x \in \mathbb{R} : x^2 > y$ er et prædikat i den reelle variabel y, kan vi kvantificere over y. Dermed opnås et udsagn, hvori begge de to variable er bundne. For eksempel kan vi danne udsagnet: $\exists y \in \mathbb{R}(\forall x \in \mathbb{R} : x^2 > y)$. Dette er et sandt udsagn, thi der eksisterer jo et y (for eksempel $y = -1$), som gør prædikatet $\forall x \in \mathbb{R} : x^2 > y$ sandt. Derimod er udsagnet $\forall y \in \mathbb{R}(\forall x \in \mathbb{R} : x^2 > y)$ falsk. Man udelader normalt parentesen og skriver for eksempel $\exists y \in \mathbb{R} \forall x \in \mathbb{R} : x^2 > y$.

Bemærkning om kvantorernes rækkefølge. Det er vigtigt at bemærke at kvantorernes rækkefølge ikke er ligegyldig. For eksempel er udsagnet

$$\forall y \in \mathbb{R} \exists x \in \mathbb{R} : x^2 > y \tag{1.26}$$

sandt, da man altid kan vælge x så stor, at x^2 bliver større end et givet y, uanset hvilken værdi y tillægges. Derimod er udsagnet

$$\exists x \in \mathbb{R} \forall y \in \mathbb{R} : x^2 > y \tag{1.27}$$

falsk. Det er jo ikke muligt at finde et x, så x^2 bliver større end alle reelle tal y.

Der er dog nogle tilfælde, hvor man gerne må bytte om på kvantorerne:

Sætning 35 *Lad* $p(x, y)$ *være et prædikat i de frie variabel* x *og* y*. Der gælder følgende implikationer:*

$$(\exists x \ \exists y : \ p(x, y)) \quad \Leftrightarrow \quad (\exists y \ \exists x : \ p(x, y)) \ , \tag{1.28}$$

$$(\forall x \ \forall y : \ p(x, y)) \quad \Leftrightarrow \quad (\forall y \ \forall x : \ p(x, y)) \ , \tag{1.29}$$

samt

$$(\exists x \ \forall y : \ p(x, y)) \quad \Rightarrow \quad (\forall y \ \exists x : \ p(x, y)) \ . \tag{1.30}$$

Formuleres de to første i ord, er de intuitivt klare. Det gælder også den tredie regel: Antag, at der findes x (kald et sådant x_0), således at der for alle y gælder $p(x_0, y)$. Da vil der for ethvert y findes x, (for eksempel det førnævnte x_0), så $p(x_0, y)$.

Bemærkning 36 *Udsagnet* $(\forall y \ \exists x : \ p(x, y)) \Rightarrow (\exists x \ \forall y : \ p(x, y))$ *er derimod ikke i almindelighed sandt:*

Eksemplet i ovenstående bemærkning giver et modeksempel. Som et andet simpelt modeksempel kunne man eksempelvis lade $p(x, y)$ være prædikatet $x^2 = y$ hvor de frie variable x og y tillades at løbe over de positive reelle tal $\mathbb{R}_+$. I så fald er udsagnet $\forall y \ \exists x : x^2 = y$ sandt: Det siger blot, at ethvert positivt reelt tal har en positiv kvadratrod. Men udsagnet $\exists x \ \forall y : x^2 = y$ er jo klart falsk: Der findes naturligvis intet positivt reelt tal x, hvis kvadrat er lig ethvert positivt reelt tal y.

Eksempel 37 *Punktvis og uniform kontinuitet:*

De ovennævnte eksempler på at kvantorer ikke kan ombyttes er legetøjseksempler. Her skal nævnes et tilfælde, hvor problemet bliver akut i en vigtig matematisk sammenhæng. Lad den reelle funktion f være defineret på en delmængde M af $\mathbb{R}$. Som bekendt siges f da at være kontinuert i punktet $x_0 \in M$, hvis

$$\forall \epsilon \in \mathbb{R}_+ \exists \delta \in \mathbb{R}_+ \forall x \in M : |x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon \tag{1.31}$$

Endvidere siges f at være **(punktvis) kontinuert** i M, hvis den er kontinuert i alle punkter $x_0 \in M$, dvs. hvis

$$\forall x_0 \in M \forall \epsilon \in \mathbb{R}_+ \exists \delta \in \mathbb{R}_+ \forall x \in M : |x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon \tag{1.32}$$

I følge ovenstående regler har vi lov til at bytte om på de to første alkvantorer i denne definition. Men hvad hvis vi flytter $\forall x_0 \in M$ helt hen efter $\exists \delta \in \mathbb{R}_+$? Så fås følgende betingelse på f:

$$\forall \epsilon \in \mathbb{R}_+ \exists \delta \in \mathbb{R}_+ \forall x_0 \in M \forall x \in M : |x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon \tag{1.33}$$

Hvis f opfylder dette kaldes den pr. definition **uniformt kontinuert** på mængden M. Det følger af (1.30) at hvis en funktion er uniform kontinuert på en mængde M, så er den også punktvis kontinuert. Derimod er $f(x) = 1/x$ defineret på intervallet $]0, 1]$ et eksempel på en funktion, som er punktvis kontinuert men ikke uniform kontinuert. En hovedsætning siger dog, at på en lukket og begrænset mængde er uniform kontinuitet det samme som punktvis kontinuitet.

Øvelse 38 *Argumenter for at $f(x) = 1/x$ defineret på intervallet $]0, 1]$ ikke er uniformt kontinuert. Det bliver måske lettere at finde på argumentet, når du har læst afsnittet om uligheder og numerisk værdi.*

Sætning 39 ***Logisk huskeseddel fortsat.*** *Man har følgende regler:*

$$\neg(\forall x \ : \ p(x)) \ \equiv \ \exists x \ : \ \neg p(x) \ , \qquad \neg(\exists x \ : \ p(x)) \ \equiv \ \forall x \ : \ \neg p(x) \ . \tag{1.34}$$

Disse tillader negation af længere strenge med al– og/eller eksistenskvantorer. Eksempelvis:

$$\neg(\forall x \ \exists y \ \forall z \ : \ p(x, y, z)) \ \equiv \ \exists x \ \forall y \ \exists z \ : \ \neg p(x, y, z) \ . \tag{1.35}$$

Endelig gælder følgende regel, hvis $p(x)$ er et prædikat og q et udsagn:

$$(\forall x \ : \ p(x)) \wedge q \ \equiv \ \forall x \ : \ p(x) \wedge q \ , \tag{1.36}$$

samt de tilsvarende, der fås hvis $\wedge$ og/eller $\forall$ udskiftes med $\vee$ hhv. $\exists$.

1.6 Om brug af udsagn og prædikater

Når der i en matematisk tekst står et udsagn, betyder det da "dette udsagn er sandt" eller betyder det "her står et udsagn, som kan være sandt eller falsk"? Det korte svar på spørgsmålet er, at det afhænger af sammenhængen. I en tekst om logik vil der ofte stå udsagn, som kan være sande eller falske. For eksempel har vi ovenfor skrevet forskellige udsagn uden at implicere at de var sande. Når man derimod formulerer en sætning i matematik, er meningen at udsagnet i sætningen er sand. Nedenfor formuleres for eksempel De Morgan's love og meningen er naturligvis, at disse er sande.

Man kan sige noget lignende om prædikater. Når man skriver $x > 2$, kan man mene: Her står et prædikat i den reelle variable x. Men oftere mener man "x er et reelt tal, som gør prædikatet $x > 2$ sandt".

Denne usystematiske brug af udsagn i matematik giver sjældent anledning til forvirring. Men jeg vil dog fremhæve en argumentationsform, hvor der ofte opstår forvirring: Hvis der midt i et matematisk bevis står en implikation f.eks. $p \Rightarrow q$, så betyder det at følgende udsagn er sandt: "Hvis p er sand da er q sand". Det betyder *ikke* "Da p er sand er også q sand". Hvis man vil sige at p er sand, må man skrive det eksplicit. Lad os se på et eksempel:

Sætning: Hvis et kvadrat har en side, der er større end 2 så er dets areal større end 4.

En udbredt fejlagtig præsentation af beviset går på følgende vis: Hvis siden i kvadratet kaldes x, er $x > 2$. Da $x > 2$ gælder at

$$x > 2 \Rightarrow x^2 > 4, \tag{1.37}$$

hvorfor arealet $x^2 > 4$.

Forfatteren af argumentet mente nok følgende slutning (det, der står i parenteserne behøver man ikke skrive. Det kan underforstås): "Da $x > 2$ (er sand) er $x^2 > 4$ (sand)". Men når forfatteren skriver at $x > 2 \Rightarrow x^2 > 4$ "gælder" så betyder det bare, at *hvis* $x > 2$ (er sand) *så* er $x^2 > 4$ (sand). Men dette udsagn er sandt uanset værdien af $x \in \mathbb{R}$. Der er derfor ikke nogen grund til at skrive, at *da* $x > 2$ *så* gælder $x > 2 \Rightarrow x^2 > 4$. Og argumentet er slet ikke færdigt når vi har udledt at $x > 2 \Rightarrow x^2 > 4$ for det betyder jo ikke at $x^2 > 4$ er sandt, sådan som vi skulle konkludere i beviset.

Vi kan dog fra $x > 2$ og $x > 2 \Rightarrow x^2 > 4$ slutte at $x^2 > 4$ (modus ponens, se senere). Men det bliver meget tungt at bruge pile i sådanne tilfælde. Det er derfor ofte sikrest og mest elegant at undgå brug af pile.

Hovedreglen synes at være at når der står et længere sammensat udsagn i en matematisk tekst, så mener vi, at dette udsagn er sandt, men vi mener *ikke* at de simplere udsagn, som indgår i det sammensatte udsagn er sande. Når vi skriver $p \Rightarrow q$ så mener vi (ofte) at det er sandt, at hvis p er sand, så er q også sand. Men det betyder ikke at vi mener at p er sand (og derfor også q er sand).

Tilsvarende, når vi om en funktion der er kontinuert i a skriver at

$$\forall \epsilon > 0 \exists \delta > 0 : |x - a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon \tag{1.38}$$

så mener vi naturligvis at hele dette sammensatte udsagn er sandt, men vi mener *ikke* at udsagnet $|x-a|<\delta$ er sandt. Hvis vi derfor vil antage dette i et bevis, må vi eksplicit sige det: "Lad $|x-a|<\delta$".

1.7 Definitioner

Definitioner er sætninger som fortæller, hvad ord eller tegn betyder. I modsætning til aksiomerne indeholder definitionerne ikke egentlig ny information om den matematiske teori, og i modsætning til sætningerne kræver de ikke noget bevis. I det foregående kapitel så vi eksempler på definitioner inden for teorien for hele tal. Her følger et par andre definitioner vi får brug for i det følgende:

Definition 40 *Et helt tal x kaldes **lige**, hvis der findes et helt tal n så $x=2n$.*

Definition 41 *Et helt tal kaldes **ulige**, hvis det ikke er lige.*

Bemærkninger om definitioner. I formuleringen af definitionerne indgår der ordet "hvis". Der burde egentlig stå "hvis og kun hvis". Den første definition skal for eksempel ikke blot betyde at tal af formen $2n$ er lige, men også at tal, der ikke er af denne form, ikke er lige. Der er dog tradition for kun at skrive "hvis" i definitioner.

Selv om man i matematikken ofte benytter ord, som også har en dagligdags betydning betyder de i matematik kun det, som er specificeret i definitionen. For eksempel har ordene "grænse" og "kontinuitet" i matematikken en betydning, som kun til en vis grad stemmer overens med den dagligdags betydning af ordene. Det er naturligvis vigtigt at danne sig intuitive billeder af hvad de matematiske ord og begreber dækker, men i sidste ende er det kun definitionerne, der bestemmer betydningen af begreberne og ordene. Man kan for eksempel have en intuitiv fornemmelse af, at kontinuitet af en funktion betyder, at dens graf hænger sammen, og det er også en nyttig intuition. Men man kan blive snydt af den. For eksempel kan den vildlede en til at tro, at funktionen f defineret ved

$$f(x)=\left\{\begin{array}{c}\sin\frac{1}{x}\text{ for }x\neq 0\\ 0\text{ for }x=0\end{array}\right\} \tag{1.39}$$

er kontinuert i 0. Men definitionen af kontinuitet afgør, at funktionen er diskontinuert i 0.

Bemærk også at definition af et matematisk begreb ikke sikrer, at der i teorien eksisterer et objekt af den slags som defineres. Eksistens må etableres ud fra aksiomerne i teorien. For eksempel kan man godt definere, at et lige primtal større end 2 kaldes et stor-lige primtal. Der er dog ingen naturlige tal som er stor-lige primtal. Ligeså kan man godt i euklidisk geometri definere en retvinklet femkant som en femkant med fem rette vinkler. Det viser sig bare at sådanne femkanter ikke findes. Omvendt, når man har defineret et kvadrat som en firkant med fire rette vinkler og fire lige store sider, så må man først bruge sådanne firkanter i sin teori, når man har vist deres eksistens, uanset hvor intuitivt det kan synes, at der findes kvadrater.

Når et lighedstegn bruges til at definere et matematisk objekt skrives ofte $:=$. For eksempel kan man skrive at intervallet $[a, \infty[$ defineres som

$$[a, \infty[:= \{x \in \mathbb{R} \mid a \leq x\}. \tag{1.40}$$

Når en biimplikationspil bruges til at definere et udsagn eller et prædikat, skriver man ofte $\overset{def}{\Leftrightarrow}$ eller $\dot{\Leftrightarrow}$. For eksempel kunne vi formulere definitionen af relationen $<$ som følger:

$$x < y \overset{def}{\Leftrightarrow} (x \leq y) \wedge x \neq y \tag{1.41}$$

1.8 Opgaver

1. Opskriv sandhedstabeller for følgende sammensatte udsagn:

$$(p \vee \neg q) \wedge (\neg p \vee q) \quad \text{og} \quad (p \vee q) \wedge (\neg p \vee \neg q) \tag{1.42}$$

2. Hvilke af følgende sammensatte udsagn er logisk ækvivalente?

$$p \Rightarrow q, \;\; q \Rightarrow p, \;\; \neg(p \Rightarrow q), \tag{1.43}$$

$$p \Rightarrow \neg q, \;\; \neg p \Rightarrow q, \;\; \neg p \Rightarrow \neg q. \tag{1.44}$$

3. Vis at følgende sammensatte udsagn er en tautologi:

$$(p \Rightarrow q) \vee (\neg p \Rightarrow q) \tag{1.45}$$

4. Skriv følgende udsagn ved brug af kvantorer:
(a) Ligningen $x^3 = 7$ har mindst en rod.
(b) Ligningen $x^2 - 2x - 5 = 0$ har ingen rational rod.
(c) Enhver ligning af formen $x^3 = a$ har en rod.
(d) Der findes ingen ligninger af formen $x^n = a$, der ikke har rødder.
(e) Der findes intet helt tal, som er større end alle andre hele tal.

5. Lad $p(x)$ og $q(x)$ være prædikater om elementerne i en mængde M.
Er følgende udsagn logisk ækvivalente?
(a) $\forall x \in M : p(x) \wedge q(x)$ og $(\forall x \in M : p(x)) \wedge (\forall x \in M : q(x))$
(b) $\forall x \in M : p(x) \vee q(x)$ og $(\forall x \in M : p(x)) \vee (\forall x \in M : q(x))$
(c) $\exists x \in M : p(x) \vee q(x)$ og $(\exists x \in M : p(x)) \vee (\exists x \in M : q(x))$
(d) $\exists x \in M : p(x) \wedge q(x)$ og $(\exists x \in M : p(x)) \wedge (\exists x \in M : q(x))$

6. Lad det være givet, at Kurt kun spiser is, når solen skinner. Lad $p(t)$ og $q(t)$ være følgende prædikater:
$p(t)$: Solen skinner til tidspunktet t.
$q(t)$: Kurt spiser en is til tidspunktet t.
Hvilken implikation gælder mellem $p(t)$ og $q(t)$.

7. Bestem de kontraponerede til følgende udsagn. Brug positiv udtryksmåde hvis det er muligt.

(a) Hvis $x < 0$, så er $x^2 > 0$.
(b) Hvis $x \neq 0$, så eksisterer der et y så $xy = 1$.
(c) Hvis x er et lige helt tal, så er x^2 et lige helt tal.
(d) Hvis $x + y$ er ulige og $y + z$ er ulige, så er $x + z$ lige
(e) Hvis f er et polynomium af ulige grad, så har f mindst én reel rod.

8. Bevis nogle af de logiske ækvivalenser i Sætning 19, ved at opskrive sandhedstabeller.

9. Giv et eksempel på en sand implikation, hvis omvendte implikation er sand, og én hvor den omvendte implikation er falsk.

10. Neger følgende udsagn:

(a) $x > 0$ og x er rational.
(b) l er enten parallel med m, eller også er l lig med m. (l, m er linjer)

11. Opskriv med kvantorer hvad det betyder at en reel funktion ikke er kontinuert i punktet a. (neger (1.38))

Kapitel 2

Beviser

En matematisk teori består af en række udsagn (spilleregler) kaldet *aksiomerne,* som man regner for sande i teorien, og hvorfra man beviser "sætninger", det vil sige andre udsagn, som er sande i teorien. Vi skal i dette afsnit se på, hvordan man beviser sætninger. Lad os først formalisere bevisbegrebet lidt mere:

2.1 Gyldige slutninger (deduktioner).

Hvis $p_1, p_2, \ldots, p_n$ og q er udsagn, siger vi, at q *kan sluttes af* $p_1, p_2, \ldots, p_n$, eller at vi har en *gyldig slutning (en deduktion) af* q *fra udsagnene* $p_1, p_2, \ldots, p_n$, såfremt:

$$(p_1 \wedge \ldots \wedge p_n) \Rightarrow q \text{ er en tautologi} \tag{2.1}$$

Her er nogle vigtige eksempler på gyldige slutninger:

$$\text{Af } (p \Rightarrow q \text{ og } p) \text{ kan } q \text{ sluttes} \quad \text{(Modus ponens).} \tag{2.2}$$

$$\text{Af } (p \Rightarrow q \text{ og } \neg q) \text{ kan } \neg p \text{ sluttes} \quad \text{(Modus tollens).} \tag{2.3}$$

$$\text{Af } (p \vee q \text{ og } \neg p) \text{ kan } q \text{ sluttes} \quad \text{(Disjunktiv syllogisme).} \tag{2.4}$$

$$\text{Af } (p \Rightarrow q \text{ og } q \Rightarrow r) \text{ kan } p \Rightarrow r \text{ sluttes} \quad \text{(Hypotetisk syllogisme).} \tag{2.5}$$

$$\text{Af } (p \vee q \text{ og } p \Rightarrow r \text{ og } q \Rightarrow r) \text{ kan } r \text{ sluttes} \quad \text{(Dilemma).} \tag{2.6}$$

Øvelse: Vis ved brug af sandhedstabeller at disse slutninger er gyldige.

2.2 Beviser

Et **bevis** for et udsagn q består af en kæde af udsagn $p_1, p_2, \ldots, p_n$, således at:

- $p_n = q$

- For hvert $i = 1, \ldots, n$ er udsagnet p_i enten et aksiom i vores teori, eller et tidligere bevist udsagn, eller fremgår ved en *gyldig slutning* af udsagnene $p_1, \ldots, p_{i-1}$.

Når et udsagn er blevet bevist, er det blevet en såkaldt "sætning" (teorem, proposition) i teorien.

2.3 Direkte beviser

De fleste matematiske sætninger er af formen: "Hvis ... så ...", altså af formen $p \Rightarrow q$ eller $p(x) \Rightarrow q(x)$. Som understreget ovenfor er der i sådan en sætning en gemt alkvantor, så sætningen er af formen $\forall x \in M : p(x) \Rightarrow q(x)$. Som vi også gjorde opmærksom på i forrige kapitel bevises en sådan sætning ved at vise, at $q(x)$ er sand for alle de x som gør $p(x)$ sand. Vi behøver altså ikke kære os om de x som gør $p(x)$ falsk, men selv da kan der jo være uendeligt mange x'er at checke. Lad os for eksempel se på sætningen:

Sætning 42 *Kvadratet på et lige tal er lige.*

Bemærkning. For at se at denne sætning er af formen $p(x) \Rightarrow q(x)$, kan vi skrive den på den mindre elegante form: "Hvis x er et lige tal, så er x^2 et lige tal". For at bevise sætningen skal vi altså checke, alle lige tal og kontrollere, at deres kvadrat er lige. Vi kunne så begynde forfra: $2^2 = 4$ er lige, $4^2 = 16$ er lige,..., men vi ville aldrig blive færdige. I stedet bruger vi fleksibiliteten i bogstavregningen, som tillader os at behandle alle lige tal på én gang. Vi antager blot, at x er et lige tal, og viser ud fra definitionen af lige tal og de kendte regneregler for hele tal, at x^2 er lige. Vi opererer altså med x, som om det var et bestemt tal , men er omhyggelige med kun at bruge de egenskaber, som alle lige tal har. Beviset kan forløbe således:

Bevis for Sætning 42 Lad x være et lige tal. Bestem et helt tal n så $x = 2n$. Dette er muligt ifølge definitionen af et lige tal. Ifølge regnereglerne for hele tal gælder da, at $x^2 = (2n)^2 = 2^2n^2 = 2(2n^2)$. Da $2n^2$ er et helt tal, er x^2 altså af formen $2m$ for et helt tal m og er derfor lige. QED.

Bemærkninger. Bemærk at beviset begynder med ordene "Lad x være et lige tal". Sådan begynder et typisk direkte bevis med at "lade" hypotesen være sand. Det er bedre end at starte med ordene "for alle", fordi vi efter ordet "lad" kan operere med x, som om det er et bestemt helt tal. Ligeså er det også bedre at skrive "bestem et helt tal n så $x = 2n$" end at skrive "da eksisterer et helt tal n så $x = 2n$", fordi vi efter at have "bestemt" n, kan operere med det som med en kendt størrelse.

Beviset slutter med bogstaverne QED. Det er en forkortelse for det latinske "quod erat demonstrandum", som betyder: hvad der skulle bevises. Det er dog også blevet almindeligt at slutte beviser med en firkant.

Bemærk også at beviset ikke bruger pile. Man kunne måske fristes til at skrive beviset på følgende vis: Da x er et lige tal, kan vi bestemme et helt tal n

så $x = 2n$. Derfor gælder at

$$x^2 = (2n)^2 \tag{2.7}$$
$$\Rightarrow x^2 = 2^2 n^2 \tag{2.8}$$
$$\Rightarrow x^2 = 2(2n^2). \tag{2.9}$$

Men som bemærket ovenfor ville det være forkert. Implikationerne gælder jo altid og ikke *fordi* $x = 2n$. Og når man som her kun regner på den ene side af lighedstegnet, er det meget mere elegant at skrive udregningen med en række lighedstegn, som vi gjorde i beviset: $x^2 = (2n)^2 = 2^2 n^2 = 2(2n^2)$.

Bemærkning. Ifølge den ovenstående forklaring af hvad et bevis er, skulle ovenstående bevis bestå af gyldige slutninger ud fra aksiomerne og de allerede beviste sætninger i teorien. Faktisk består beviset i gyldige slutninger ud fra 1. definitionen af et lige tal og 2. aksiomer og sætninger i teorien for aritmetikken for de hele tal. I Kapitel 4 vil vi komme nærmere ind på aksiomerne for de hele tals aritmetik. Det er i øvrigt karakteristisk for megen matematik, at den tager sit udgangspunkt i en ikke helt formaliseret teori.

Bemærkning. En sætning, der udsiger at $q(x)$ gælder for alle elementer x i en given mængde M, er et specialtilfælde af ovenstående. I sådanne beviser begynder man med at "lade" $x \in M$ og fortsætter da med logiske slutninger, som gælder for alle $x$er i M.

Sætning 43 *For alle $x \in \mathbb{R}$ gælder at $0 \cdot x = 0$*

Bemærkning: Man kunne tro at det var trivielt rigtigt. Men det skal jo bevises ud fra aksiomerne for de reelle tal (Definition 1). Og i aksiomssystemet er 0 jo karakteriseret ved, at det er et neutralt element for addition. Det vi her skal vise, handler derimod om, hvordan 0 virker ved multiplikation. For at bevise sætningen er det derfor klart, at vi skal bruge den distributive lov (9), som er det eneste aksiom, der knytter addition sammen med multiplikation.
Bevis. Lad $x \in \mathbb{R}$. Først bemærker vi at $0+0 = 0$. Det følger af (3). Så slutter vi fra den distributive lov at

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

Lægges nu $-(0 \cdot x)$ til på begge sider fås det ønskede:

$$0 = 0{\cdot}x + (-(0{\cdot}x)) = (0{\cdot}x + 0{\cdot}x) + (-(0{\cdot}x)) = 0{\cdot}x + (0{\cdot}x + (-(0{\cdot}x))) = 0{\cdot}x + 0 = 0{\cdot}x$$

Overvej præcist hvilke aksiomer der benyttes i hvert lighedstegn! ■

Bemærkning 44 *Der gælder følgende logiske ækvivalens:*

$$(p \vee q) \equiv (\neg p \Rightarrow q).$$

(opskriv en sandhedstabel!) Derfor kan man vise udsagnet $p \vee q$ ved at vise $\neg p \Rightarrow q$. Ligeså kan man vise $p \vee q \vee r$ ved at vise $(\neg p \wedge \neg q) \Rightarrow r$. Det vil vi benytte os af i beviset for Sætning 77.

Ligeså gælder følgende logiske ækvivalens:

$$(p \Rightarrow (q \vee r)) \equiv ((p \wedge \neg q) \Rightarrow r).$$

Bevis dette enten ved at opskrive en sanhedstabel, eller ved at udlede ækvivalensen ud ækvivalenserne i den logiske huskeseddel. Man kan altså bevise udsagnet $(p \Rightarrow (q \vee r))$ *ved at bevise* $((p \wedge \neg q) \Rightarrow r)$.

Sætning 45 ***Nul-reglen:*** *Lad* x, y *være reelle tal. Hvis* $x \cdot y = 0$*, så er enten* $x = 0$ *eller* $y = 0$.

Bevis. Med logiske tegn kan sætningen skrives $(x \cdot y = 0) \Rightarrow (x = 0 \vee y = 0)$. Ifølge foregående bemærkning kan vi bevise sætningen ved at vise at $((x \cdot y = 0) \wedge (x \neq 0)) \Rightarrow (y = 0)$ Antag derfor at $x \cdot y = 0$ og at $x \neq 0$. Vi skal så vise at $y = 0$. Men det ses let ved at gange ligheden $x \cdot y = 0$ på begge sider med x^{-1} (som jo eksisterer, da $x \neq 0$):

$$y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0.$$

Overvej igen hvilke aksiomer der bruges i hvert lighedstegn. ■

2.4 Modeksempler.

Vi har ovenfor set hvordan man kan vise at et "hvis...så..." udsagn er sandt, altså er en sætning i en bestemt matematisk teori. Hvordan kan man da indse at et sådant udsagn er falsk? Jo, et udsagn af formen $(\forall x :)p(x) \Rightarrow q(x)$ er jo kun sandt, hvis alle x der gør hypotesen $p(x)$ sand også gør konklusionen $q(x)$ sand. Vi viser altså at udsagnet er falsk, hvis vi bare finder et eneste x, som gør $p(x)$ sand, men som gør $q(x)$ falsk. Et sådant x kaldes et **modeksempel**.

Eksempel 46 *For at modbevise udsagnet "For alle naturlige tal* n *er* $n^2 > n$*" er det nok at bemærke at* 1 *er et naturligt tal, medens udsagnet "*$1^2 > 1$*" er falsk. Tallet* 1 *er altså et modeksempel.*

2.5 Formodninger og deres behandling.

I lærebøger som denne er opgaverne ofte formuleret som: "Bevis ..." eller "Find et modeksempel mod ..." For den kreative matematiske forsker er situationen mere kompliceret. Han eller hun vil ofte have en intuitiv formodning om, at et bestemt udsagn $p(x) \Rightarrow q(x)$ er en sætning i den teori han eller hun arbejder med. For at afgøre sagen vil matematikeren først prøve at finde et bevis for udsagnets sandhed. Hvis det mislykkes, vil bevisforsøgene måske have afdækket nogle mulige modeksempler. Disse vil så blive prøvet af. Hvis de viser sig at være modeksempler, er sagen klar: udsagnet er ikke en sand sætning. Hvis det derimod viser sig, at eksemplerne alligevel ikke er modeksempler, så vil matematikeren nok endnu en gang prøve at finde et bevis osv. Hvis denne dialektiske proces ender med et bevis, er udsagnet blevet en sætning i teorien.

Hvis processen ender med et modeksempel er udsagnet falsk. Hvis det er falsk, kan matematikeren vælge at vende sig mod andre ting eller prøve at modificere udsagnet, så eksemplet ikke længere er et modeksempel. Hvis det sidste lykkes fortsætter den dialektiske afprøvningsproces med det nye udsagn. Hvis afprøvningsprocessen ender uden at der er fundet modeksempler eller beviser, må udsagnet forblive en formodning. Hvis udsagnet er særligt interessant og genstridigt kan det blive en berømt formodning som for eksempel

Goldbachs formodning: Ethvert lige tal større end to er sum af to primtal.

2.6 Bevis ved kontraposition.

Hvis man skal vise $p \Rightarrow q$, er det nogle gange simplere at vise det kontraponerede udsagn $\neg q \Rightarrow \neg p$. I så fald er man færdig, for af $\neg q \Rightarrow \neg p$ kan man slutte $p \Rightarrow q$, da disse udsagn er logisk ækvivalente (se den logiske huskeseddel).

Sætning 47 *Hvis x^2 er ulige, så er x ulige.*

Bevis. Beviset føres ved kontraposition: Lad x være lige. Vi skal da vise at x^2 er lige. Det følger af Sætning 42. ■

Sætning 48 *Kvadratet på et ulige tal er ulige. Eller sagt anderledes: Hvis x er ulige, så er x^2 ulige.*

Bevisskitse. Da et ulige tal er defineret som et tal, der ikke er lige, er det nærliggende at forsøge at lave et bevis ved kontraposition, altså at bevise det kontraponerede udsagn:.

Sætning 49 *Hvis x^2 er lige, er x lige.*

Bevis. Antag at x^2 er lige. Da går 2 op i $x^2 = xx$. Da 2 er et primtal følger det af sætning 141, som vi vil vise senere, at 2 går op i x hvorfor x er lige. ■

Alternativ bevisskitse. Man kunne fristes til at bevise Sætning 48 direkte ved at bruge, at ulige tal er tal af formen $2n + 1$ for et naturligt tal n. Men da vi har defineret et ulige tal til at være et tal der ikke er lige, kan vi ikke bruge denne anden karakterisering af ulige tal, før vi har bevist, at den er ækvivalent med definitionen. Det vil vi gøre nedenfor (Sætning 54)

Øvelse 50 *Gennemfør beviset for Sætning 48 på grundlag af den alternative karakterisering af et ulige tal.*

Senere i bogen kommer vi til at bevise mange mere interessante sætninger ved kontraposition. Se for eksempel Sætning 127.

2.7 Bevis ved modstrid.

Hvis man vil vise at et udsagn q er sandt, kan man gøre det ved at antage, at udsagnet er falsk (altså at $\neg q$ sand) og så vise at det fører til modstrid. Intuitivt er det jo klart, at hvis vi opnår en modstrid må vi have antaget noget falsk. $\neg q$ er altså falsk, hvorfor q er sand. Mere formelt kan bevismetoden beskrives således:

Man ønsker at bevise et udsagn q. Kan man bevise:

$$\neg q \Rightarrow (p \ \wedge \neg p) \ , \tag{2.10}$$

for et eller andet udsagn p, er man færdig: For det checkes let, at:

$$q \ \equiv \ (\neg q \Rightarrow (p \ \wedge \neg p)) \ , \tag{2.11}$$

hvorfor q kan sluttes af $\neg q \Rightarrow (p \ \wedge \neg p)$.

2.7.1 Eksempler på beviser ved modstrid:

Sætning 51 *Tallet* 0 *har intet multiplikativt inverst element i* $\mathbb{R}$.

Bevis. Antag nemlig at e er multiplikativt inverst til 0. Ifølge definitionen af den multiplikative inverse gælder at $0 \cdot e = 1$ og ifølge Sætning 43 gælder at $0 \cdot e = 0$. Men det er umuligt, da vi har forudsat at 0 og 1 er forskellige. ■

Bemærkning 52 *Det er dette faktum, som vi normalt omtaler med følgende vending: "Man kan ikke dividere med* 0 *".*

Sætning 53 $\sqrt{2}$ *er irrational.*

Bevis. Lad mig først minde om at et reelt tal kaldes rationalt, hvis det kan skrives som en brøk mellem to hele tal. Hvis et reelt tal ikke er rationalt, kaldes det irrationalt.

Vi viser sætningen ved et modstridsargument[1]. Antag altså at $\sqrt{2}$ ikke er irrational, dvs. at $\sqrt{2}$ er rational. Bestem da hele tal m, n så $\sqrt{2} = \frac{m}{n}$. Vi kan antage at vi har forkortet brøken så meget som muligt, så intet helt tal går op i både m og n (se evt. Sætning 149). Det følger da af definitionen af $\sqrt{2}$ at

$$2 = (\sqrt{2})^2 = (\frac{m}{n})^2 = \frac{m^2}{n^2} \tag{2.12}$$

hvorfra vi slutter at

$$m^2 = 2n^2 \tag{2.13}$$

I følge definitionen på lige tal betyder dette, at m^2 er lige, hvorfor m ifølge Sætning 49 selv er lige. Altså findes et naturligt tal p så $m = 2p$. Men så får vi fra (2.13), at

$$2^2 p^2 = (2p)^2 = m^2 = 2n^2, \tag{2.14}$$

[1] Det er faktisk det ældste modstridsbevis i matematikkens historie. Det går nok tilbage til pythagoræerne omkring 430 f.Kr.

hvoraf

$$2p^2 = n^2. \tag{2.15}$$

Heraf ses, at n^2 er lige og derfor iflg. Sætning 49, at n er lige og altså af formen $2q$ for et naturligt tal q. Men det betyder at 2 går op i både m og n, i modstrid med at vi havde antaget, at de ikke havde nogen fælles divisorer. Altså har antagelsen om at $\sqrt{2}$ var rational ført til en modstrid, og vi slutter at $\sqrt{2}$ er irrational. ■

Sætning 54 *Et helt tal x er ulige, hvis og kun hvis der findes et helt tal n så $x = 2n + 1$.*

Bevis. Vi skal vise

$$x \text{ er ulige} \Leftrightarrow \exists n \in \mathbb{Z} : x = 2n + 1 \tag{2.16}$$

Vi viser først $\Rightarrow$: Dette gør vi ved et direkte bevis. Antag altså at x er ulige, dvs at det ikke er lige. Vi skal vise at x kan skrives på formen $2n + 1$ for et n i $\mathbb{Z}$. Bestem det største hele tal m så $2m < x$.[2] Da er

$$2m < x \leq 2(m + 1). \tag{2.17}$$

Men da x er ulige, er x pr. definition ikke lige, og altså ikke lig med $2(m + 1)$. Altså er

$$2m < x < 2(m + 1) = 2m + 2, \tag{2.18}$$

og da $2m + 1$ er det eneste hele tal mellem $2m$ og $2m + 2$, har vi at $x = 2m + 1$.

Dernæst viser vi $\Leftarrow$: Igen begynder vi beviset som et direkte bevis: Vi antager altså at $x = 2n + 1$ og $n \in \mathbb{Z}$ og skal vise at x er ulige. Vi skal altså vise at x ikke er lige. Det gør vi ved modstrid. Antag altså at x er lige, dvs. kan skrives $x = 2m$ for $m \in \mathbb{Z}$. Men så får vi

$$2n + 1 = x = 2m, \tag{2.19}$$

hvoraf

$$1 = 2(m - n). \tag{2.20}$$

Heraf ses at 2 går op i 1; men vi ved at 2 ikke går op i 1. Altså har vi sluttet os til en modstrid og kan derfor konkludere, at x ikke er lige, altså at x er ulige. ■

Vi kommer til at møde mange modstridsbeviser i det følgende, fx. beviset for at der findes uendeligt mange primtal (Sætning 144)

Notation 55 *Beviser ved kontraposition og ved modstrid kaldes ofte **indirekte beviser**.*

[2] På dette sted vil vi uden bevis bruge at et sådant største tal findes. Det følger af supremumsegenskaben ved de reelle tal.

2.8 Beviser delt op i tilfælde.

I nogle beviser kan det være nødvendigt eller bekvemt at dele op i forskellige tilfælde.

Sætning 56 *Udsagnet* $(p \vee q) \Rightarrow r$ *er ækvivalent med udsagnet*

$$(p \Rightarrow r) \wedge (q \Rightarrow r).$$

Bevis. Lav en sandhedstabel. ■

Det betyder at man kan bevise $p \vee q \Rightarrow r$ ved at bevise $p \Rightarrow r$ og $q \Rightarrow r$.

Eksempel 57 *Hvis* n *er et naturligt tal, er* $n^2 + n$ *et lige tal.*

Bevis. Ifølge Definition 41 er ethvert naturligt tal enten lige eller ulige. Derfor kan sætningen omformes til:

$$((n \text{ lige}) \vee (n \text{ ulige})) \Rightarrow (n^2 + n) \text{ lige}. \tag{2.21}$$

Det kan vi altså vise ved at bevise

$$((n \text{ lige}) \Rightarrow (n^2 + n) \text{ lige}) \wedge \ ((n \text{ ulige}) \Rightarrow (n^2 + n) \text{ lige}). \tag{2.22}$$

Først beviser vi at $(n \text{ lige}) \Rightarrow (n^2 + n)$ lige. Antag altså at n er lige. Ifølge Definition 40 betyder det at vi kan finde et $m \in \mathbb{N}$ så $n = 2m$ (overvej). Men så er

$$n^2 + n = (2m)^2 + 2m = 2(2m^2 + m), \tag{2.23}$$

og da $2m^2 + m \in \mathbb{N}$, er $n^2 + n$ altså et lige tal i dette tilfælde.

Dernæst beviser vi at $(n \text{ ulige}) \Rightarrow (n^2 + n)$ lige. Antag altså at n er ulige. Så findes der ifølge Sætning 54 et $m \in \mathbb{N} \cup \{0\}$ så $n = 2m + 1$. Men så er

$$n^2 + n = (2m + 1)^2 + (2m + 1) = 2(2m^2) + 2(2m) + 1 + 2m + 1 \tag{2.24}$$

$$= 2(2m^2 + 3m + 1), \tag{2.25}$$

og da $2m^2 + 3m + 1 \in \mathbb{N}$ er $n^2 + n$ altså også lige i dette tilfælde.

Vi har altså bevist (2.22) og dermed sætningen. ■

Øvelse 58 *Brug den samme teknik til at bevise følgende sætning:*

Sætning 59 *Hvis* n *er et naturligt tal, så går* 4 *op i enten* n^2 *eller* $n^2 - 1$.

2.9 Eksistenssætninger

En særlig slags sætninger er de, der udsiger eksistensen af et objekt med bestemte egenskaber, altså sætninger af formen:

$$\exists x \in M : p(x) \tag{2.26}$$

Sådanne sætninger kaldes eksistenssætninger.

Man skulle tro at eksistenssætninger var lettere at vise end sætninger af formen $p(x) \Rightarrow q(x)$, hvor man jo skal undersøge om $q(x)$ er sand ikke bare for ét x, men for alle x som opfylder $p(x)$. Almindeligvis er eksistenssætninger dog sværere at vise end universelle udsagn i den forstand, at de kræver mere kreativitet. Et eksistensbevis falder nemlig oftest i to dele. Først finder man en kandidat x_0, og dernæst beviser man at $p(x_0)$ er sand. Den sidste del af beviset går ofte ret let. Her følges logikkens sædvanlige regler. Derimod er der ingen faste regler for, hvordan man finder en kandidat. Det er aldeles ligegyldigt, hvordan det sker. Det kan ske ved et inspireret gæt eller ved en mere systematisk undersøgelse. Og man behøver i beviset ikke fortælle, hvordan kandidaten er fundet. Så længe man efterfølgende kan vise at kandidaten x_0 opfylder det ønskede ($p(x_0)$), er beviset i hus.

2.9.1 Eksempler på eksistenssætninger

Sætning 60 *Der findes et naturligt tal x så $x = x^2$.*

Bevis. Betragt tallet 1. Da 1 er et naturligt tal og $1 = 1^2$, er sætningen vist. ■

Sætning 61 *Der eksisterer en rational rod i polynomiet $P(x) = x^4 - 2x^3 - 3x^2 + 5x + 2$.*

Bevis. Da 2 er et rationalt tal, og $P(2) = 2^4 - 2 \cdot 2^3 - 3 \cdot 2^2 + 5 \cdot 2 + 2 = 0$ er 2 en rational rod i P. ■

Bemærkning. Hvor universelle udsagn modbevises ved at finde et modeksempel (altså ved at løse et eksistensproblem), vil eksistensudsagn modbevises ved at bevise et universelt udsagn. Negationen af udsagnet $\exists x \in M : p(x)$ er jo udsagnet $\forall x \in M : \neg p(x)$.

Bemærkning: En eksistenssætning $\exists x \in M : p(x)$ udtaler sig ikke om, hvor mange elementer i M, der opfylder $p(x)$. Den siger blot at der mindst er et. Hvis man vil vise, at der højst er et, skal man vise en entydighedssætning.

Bemærkning. De beviser vi har omtalt ovenfor er *konstruktive* i den forstand, at de ikke bare fortæller at der findes et objekt med de ønskede egenskaber, men også angiver et sådant objekt. Eksistenssætninger kan dog også bevises ikke-konstruktivt.

2.9.2 Ikke-konstruktive beviser

Hvis et eksistensbevis godtgør at der eksisterer et objekt med givne egenskaber uden at fortælle, hvilket objekt der er tale om, så siges beviset at være ikke-konstruktivt.

Eksempel 62 *Ligningen*

$$x^3 + 2x^2 + x + 7 = 0 \tag{2.27}$$

har en reel løsning.

Bevis. Polynomiet $P(x) = x^3+2x^2+x+7$ er en kontinuert funktion af x på hele den reelle akse. Da $P(1) > 0$ og $P(-10) < 0$ ved vi fra mellemværdisætningen (Skjæringssætningen 5.2.1 i Lindstrøm), at der findes et reelt tal $x_0 \in]-10, 1[$, så $P(x_0) = 0$. Dette x_0 er altså en rod i ligningen. ■

Eksempel 63 *Der findes et naturligt tal n som er større end e^{100}.*

Bevis. Vi vil føre beviset ved modstrid. Antag derfor, at alle naturlige tal er mindre eller lig med e^{100}. Vi vil senere vise, at det fører til modstrid, så vi slutter, at der er et naturligt tal større end e^{100}. ■

Beviserne i de to sidste eksempler er ikke-konstruktive, idet de ikke fortæller hvilket tal der opfylder det ønskede.

Et mere interessant og berømt ikke konstruktivt bevis er det følgende:

Sætning 64 *Der findes irrationale tal x og y så at x^y er rational.*

Bevis. Vi ved fra sætning 53 at $\sqrt{2}$ er irrational. Betragt nu $\sqrt{2}^{\sqrt{2}}$. Der er to muligheder:

1. $\sqrt{2}^{\sqrt{2}}$ kan være rational. I så fald har vi fundet to irrationale tal nemlig $x = \sqrt{2}$ og $y = \sqrt{2}$ så x^y er rational.

2. Eller $\sqrt{2}^{\sqrt{2}}$ er irrational. Men da kan vi betragte $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$. Dette tal er nemlig rationalt da

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\cdot\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2. \tag{2.28}$$

   Altså har vi også i dette tilfælde fundet to irrationale tal nemlig $x = \left(\sqrt{2}^{\sqrt{2}}\right)$ og $y = \sqrt{2}$ så x^y er rational.

■

Vi har altså i begge tilfælde fundet et x og et y med den ønskede egenskab, men da vi ikke har bevist hvorvidt $\sqrt{2}^{\sqrt{2}}$ er rational eller irrational, ved vi altså ikke hvilket par der er det rigtige. Eksistensbeviset er altså ikke-konstruktivt[3].

Man kan også lave ikke-konstruktive eksistensbeviser ved at argumentere indirekte: Betragt eksistenssætningen $\exists x \in M : p(x)$ (hvor $p(x)$ er et prædikat i variablen $x \in M$). Vi kan da indirekte bevise, at sætningen er sand, idet vi beviser, at dens negation $\forall x \in M : \neg p(x)$ fører til modstrid. I dette tilfælde giver beviset altså et eksistensbevis uden at give en ide til, hvordan vi finder et objekt x, som opfylder det ønskede $p(x)$. Normalt foretrækker man konstruktive eksistensbeviser netop fordi man så ved, hvordan man finder det eksisterende objekt.

[3] Det følger faktisk af Gelfond-Schneiders sætning (1934) at det er det andet tilfælde, som er sandt.

2.10 Entydighedssætninger

Entydighedssætninger er sætninger der udsiger, at der højst er et objekt med bestemte egenskaber, altså sætninger af formen:

$$\text{Der findes højst ét } x \in M \text{ så } p(x) \tag{2.29}$$

En sådan entydighedssætning kan vises ved at udlede nogle konsekvenser fra $p(x)$ som fastlægger x entydigt.

Bemærkning 65 *En anden meget brugt metode til at bevise at der højst findes ét $x \in M$ så $p(x)$, er at antage, at x og y begge har egenskaben p og derfra udlede at $x = y$. Udtrykt mere formelt bevises entydigheden ved at vise at for $x, y \in M$ gælder:*

$$(p(x) \wedge p(y)) \Rightarrow (x = y). \tag{2.30}$$

2.10.1 Eksempler på entydighedssætninger

Sætning 66 *Hvis q er et positivt rationalt tal da findes højst ét positivt rationalt tal x så*

$$x^2 + x = q. \tag{2.31}$$

Bevis. Antag at x og y er to positive rationale tal, som opfylder at

$$x^2 + x = y^2 + y = q. \tag{2.32}$$

Det følger af aksiomerne for regning med de rationale tal, at funktionen x^2+x er voksende på de positive rationale tal (dette vil vi ikke bevise). Fra $x^2+x = y^2+y$ kan vi derfor slutte at $x = y$. ■

Bemærk at sætningen i lighed med alle andre entydighedssætninger ikke udtaler sig om, hvorvidt der *eksisterer* positive rationale løsninger til ligningen (2.31). Entydighedssætningen siger blot, at *hvis* der findes en positiv rational løsning, er der kun én. Hvis $q = 2$, er det let at se at $x = 1$ er en positiv rational løsning, og sætningen siger derfor at der ikke er andre. Hvis $q = 1$, findes der derimod ingen rationale løsninger (prøv bare at løse ligningen $x^2 + x = 1$).

Sætning 67 *I de reelle tal er det additive neutralellement 0 entydigt bestemt. Sagt på en anden måde: Der er kun et tal med egenskaben (3)*

Bevis. Antag nemlig at n_1 og n_2 er additive neutralelementer. Da gælder:

$$n_1 = n_1 + n_2 = n_2$$

Det første lighedstegn følger af at n_2 er et additivt neutralelement og det andet lighedstegn følger af at n_1 et additivt neutralelement. Dermed er det vist at det additive neutralelement er entydigt bestemt. ■

Øvelse 68 *Vis, at også det multiplikative neutralelement i $\mathbb{R}$ er entydigt bestemt.*

Sætning 69 *For alle reelle tal x, y (med $y \neq 0$) er de inverse $(-x)$ og y^{-1} entydigt bestemt.*

Bevis. Antag at a og b er multiplikativt inverse til y. Så gælder:

$$a = a \cdot 1 = a \cdot (y \cdot b) = (a \cdot y) \cdot b = 1 \cdot b = b$$

Der er altså kun et tal. som er multiplikativt inverst til x. ■

Øvelse 70 *Overvej at også det additivt inverse til et givet reelt tal x er entydigt bestemt.*

2.11 Eksistens og entydighed

Mange sætninger udsiger både eksistens og entydighed. De begynder ofte med ordene "der findes én og kun én..." eller "der findes netop én..."

Sætning 71 *Der findes netop en positiv rod i ligningen $x^2 + x = 2$.*

Bevis. Da $1^2 + 1 = 2$, er 1 en positiv rod i ligningen, og da $x^2 + x$ er voksende for $x > 0$ er 1 den eneste positive rod. ■

2.12 Opgaver

1. Afgør om følgende udsagn er sande eller falske (giv bevis eller modeksempel):
(a) $a^2 + b^2 = (a + b)^2$ for $a, b \in \mathbb{R}$.
(b) Der eksisterer naturlige tal x og y, så at $5x + 2y = 27$.

2. Lad x og y være positive reelle tal. Vis at

$$\frac{x}{y} + \frac{y}{x} \leq 2 \Rightarrow (x - y)^2 \leq 0. \tag{2.33}$$

Brug dette til at give et modstridsbevis for følgende sætning:
Hvis x og y er forskellige positive reelle tal, da er

$$\frac{x}{y} + \frac{y}{x} > 2. \tag{2.34}$$

3. Lad x og y være hele tal. Bevis følgende sætning:

$$x \cdot y \text{ er ulige, hvis og kun hvis } x \text{ er ulige og } y \text{ er ulige.} \tag{2.35}$$

I beviset må du gerne bruge Sætning 54.

4. Bevis at $x \cdot y$ er lige hvis og kun hvis x er lige eller y er lige

5.
(a) Bevis at $\sqrt{3}$ er irrational
(b) Bevis at $\sqrt{6}$ er irrational

(c) Gælder der følgende sætning? Summen af to irrationale reelle tal er irrational.

(d) Afgør om $\sqrt{2} + \sqrt{3}$ er irrational.

I beviserne må du gerne bruge Sætning 141

6. Bevis at for et vilkårligt helt tal n er $n^2 - 5n + 7$ ulige.

Kapitel 3

Reelle Tal især uligheder

I dette kapitel gennemgås nogle grundlæggende egenskaber ved de reelle tal især vedrørende uligheder. De reelle tal hører strengt taget ikke med til diskret matematik. Der er dog to grunde til at de behandles i dette kapitel: 1. De giver et godt eksempel på hvordan man kan benytte de ovennævnte bevismetoder til at udlede sætninger inden for et eksplicit formuleret aksiomssystem. 2. Uligheder og numerisk værdi er emner, som ikke behandles så grundigt i gymnasiet, men som kommer til at blive et vigtigt værktøj i den matematiske analyse (differential og integralregningen mm.).

3.1 Basale egenskaber ved de reelle tal

Vi skal nu se hvordan man fra aksiomerne for de reelle tal (Definition 1) kan udlede nogen af de basale regneregler. Vi vil kun bevise de indledende sætninger i teorien, men faktisk kan alle regneregler og sætninger om reelle tal bevises ud fra aksiomerne. Det gælder for eksempel reglerne for regning med brøker. Ovenfor har vi allerede taget hul på emnet. Vi har bevist at de neutrale elementer 0 og 1 er entydigt bestemt (Sætning 67) og vi har bevist at det inverse element til et givet tal er entydigt bestemt (Sætning 69). Endvidere har vi vist at 0 ikke har et multiplikativt inverst element (Sætning 51), at $0x = 0$ for alle reelle x (Sætning 43), og vi har bevist nul-reglen (Sætning 45).

Definition 72 *De omvendte regningsarter $-$ og $:$ defineres ved:*

$$x - y = x + (-y), \qquad x : y = \frac{x}{y} = x \cdot y^{-1} \quad \textit{(når } y \neq 0\textit{)}$$

Sætning 73 *For alle reelle tal x, y gælder:*

$$-0 = 0, \quad 1^{-1} = 1 \tag{3.1}$$

$$-(-x) = x, \qquad (y^{-1})^{-1} = y \quad \textit{(når } y \neq 0\textit{)}, \tag{3.2}$$

$$-(x+y) = (-x) + (-y), \tag{3.3}$$

$$(x \cdot y)^{-1} = x^{-1} \cdot y^{-1} \quad \textit{(når } x, y \neq 0\textit{)} \tag{3.4}$$

$$0 \cdot x = 0 \tag{3.5}$$

$$(-x) \cdot y = x \cdot (-y) = -x \cdot y \tag{3.6}$$

$$(-x) \cdot (-y) = x \cdot y \tag{3.7}$$

$$(-1)x = -x \tag{3.8}$$

$$x - y = 0 \Longleftrightarrow x = y \tag{3.9}$$

$$\frac{x}{y} = 1 \Longleftrightarrow x = y \quad \textit{(når } y \neq 0\textit{)} \tag{3.10}$$

$$\textit{Hvis } x \cdot y = 0, \textit{ så er enten } x = 0 \textit{ eller } y = 0 \tag{3.11}$$

Bevis. Vi har bevist (3.5) og (3.11). Vi beviser de tre første identiteter. Resten overlades til læseren:

(3.1): Vi skal vise at 0 er sin egen additivt inverse. Ifølge (3) gælder at $0 + 0 = 0$. Men det betyder ifølge (4) at 0 er en additiv invers til 0. Da vi har vist at den inverse til 0 (som vi jo benævnte -0) er entydigt bestemt kan vi slutte at $0 = -0$. På helt samme måde vises at $1^{-1} = 1$.

(3.2): Vi skal vise at x er den additivt inverse til $(-x)$. Men det følger direkte af den identitet, som siger at $(-x)$ er den additivt inverse til x: $x + (-x) = (-x) + x = 0$. Den anden identitet bevises på samme måde.

(3.3): Vi skal vise at $(-x) + (-y)$ er det additivt inverse til $(x + y)$, dvs. vi skal vise at hvis vi adderer $(-x) + (-y)$ til $(x + y)$ så får vi 0. Men det følger af følgende udregning (overvej hvilke aksiomer der bruges):

$$(x+y) + ((-x) + (-y)) = ((y+x) + (-x)) + (-y) =$$
$$(y + (x + (-x))) + (-y) = (y + 0) + (-y) = y + (-y) = 0$$

■

Bemærkning 74 *Læg mærke til bevisstrategien i disse beviser. For at bevise at et element er lig med et inverst til et givet element, er det nok at vise at det har den definerende egenskab, der skal til for at være et inverst til det givne. Thi det inverse til et givet element er entydigt bestemt, så to tal må være ens når de begge er inverse til det samme element. Man kunne måske tro at man kunne bevise (3.3) ved at gå i gang med at regne på $-(x + y)$, men det vil mislykkes.*

3.2 Uligheder

Definition 75 *Uligheden $x \leq y$ kan også skrives $y \geq x$.*

Den skarpe ulighed $x < y$ betyder pr. definition at $(x \leq y) \wedge (x \neq y)$

Bemærkning 76 *På grund af transitiviteten kan vi sammenskrive de to uligheder $x \leq y$ og $y \leq z$ til $x \leq y \leq z$. Derimod giver det ikke mening at samskrive uligheder, der peger hver sin vej (fx $x \leq y \geq z$).*

Sætning 77 ***Trikotomiloven:*** *For to vilkårlige reelle tal x og y gælder præcist én af udsagnene: $x < y$, $x > y$ og $x = y$.*

Bevis. Først vises at mindst et af udsagnene gælder. Vi benytter strategien i bemærkning 44. Antag derfor at to af udsagnene fx. $x < y$ og $x = y$ ikke gælder. Så skal vi vise at det tredie udsagn $x > y$ gælder. Hvis $x < y$ og $x = y$ ikke gælder så gælder $x \leq y$ ikke. Da ordningen er total (10) kan vi deraf slutte at $x \geq y$; men da vi har antaget at $x \neq y$ må $x > y$.

Dernæst skal vi vise at to af udsagnene $x < y$, $x > y$ og $x = y$ ikke kan være sande samtidigt. Af definitionen af $<$ og $>$ (definition 75) følger det at hvis $x = y$ kan hverken $x < y$ eller $y < x$ være sande. Kan $x < y$ og $x > y$ begge være sande? Nej, for hvis $(x < y) \wedge (x > y)$ så gælder at $(x \leq y) \wedge (x \geq y)$, og af antisymmetrien (13) følger da at $x = y$. Men det er umuligt når $x < y$. Dermed har vi vist at højst ét af de tre udsagn gælder. ■

Øvelse 78 *Bevis at $x < y \Leftrightarrow \neg(y \leq x)$.*

Definition 79 *De to delmængder $\mathbb{R}_+$ og $\mathbb{R}_-$ af de reelle tal er defineret ved:*

$$\mathbb{R}_+ = \{x \in \mathbb{R} \mid 0 < x\} \quad \textit{Tallene i denne mængde kaldes positive.}$$
$$\mathbb{R}_- = \{x \in \mathbb{R} \mid x < 0\} \quad \textit{Talle i denne mængde kaldes negative.}$$

Sætning 80 *Opdelingen af de reelle tal i de tre mængder $\{0\}$, $\mathbb{R}_+$ og $\mathbb{R}_-$ er en klassedeling; det vil sige at ethvert reelt tal ligger i præcist én af de tre mængder.*

Bevis. Beviset følger af trikotomiloven hvis man sætter $y = 0$ (overvej!). ■

Øvelse 81 *Bevis på samme måde, at for ethvert reelt tal a er følgende tre mængder en klassedeling af $\mathbb{R}$:*

$$\{a\}$$
$$\{x \in \mathbb{R} \mid x < a\}$$
$$\{x \in \mathbb{R} \mid a < x\}.$$

Bemærkning 82 *Aksiom (14) fortæller at man i en ulighed kan lægge samme tal til på begge sider. Heraf ses let, at man kan flytte et led[1] i en ulighed over på den anden side af ulighedstegnet, hvis man skifter fortegn på tallet. Ligeså viser aksiom (15) at man kan gange på begge sider af en ulighed med et ikke-negativt tal. Men hvad hvad sker der, når man ganger på begge sider af en ulighed med et negativt tal? Så vender uligheden! Før vi kan bevise dette skal vi se hvordan man regner med skarpe ulighedstegn:*

[1] Husk at et led er noget, som er lagt til, medens en faktor er noget, som er ganget på. Fx. er a et led i udtrykket $a + b$, medens der er en faktor i udtrykket $a \cdot b$

Sætning 83 *Hvis $x < y$ og $y \leq z$, så er $x < z$.*

Bevis. Antag at $x < y$ og $y \leq z$. At $x \leq z$ følger af transitiviteten (12). Men $x = z$ kan ikke lade sig gøre, for i så fald ville $x < y$ og $y \leq x$ hvilket er umuligt ifølge trikotomiloven. ■

Bemærkning 84 *På samme måde kan det vises (gør det!) at hvis $x \leq y$ og $y < z$, så er $x < z$. Vi kan derfor skrive for eksempel: $x < y \leq z$ og lignende udtryk med flere ulighedstegn efter hinanden, bare de vender samme vej. Hvis bare et af ulighedstegnene i en sådan kæde er et skarpt ulighedstegn, så er der skarp ulighedstegn mellem første og sidste tal i kæden.*

Sætning 85 *Hvis $a < b$ og $c \leq d$ så er $a + c < b + d$.*

Bevis. Først viser vi at $a + c < b + c$. At $a + c \leq b + c$ følger af (14). Vi skal altså vise at $a + c \neq b + c$. Men hvis $a + c = b + c$ kan vi lægge $(-c)$ til på begge sider, hvorved vi får $a = b$ i modstrid med at $a < b$.

Det generelle resultat følger nu af følgende kæde af uligheder:

$$a + c < b + c \leq b + d$$

■

Øvelse 86 *Vis at $a \leq b \wedge c \leq d \Rightarrow a + c \leq b + d$.*

Sætning 87 *For vilkårlige reelle tal a, b, c, d gælder:*

$$(0 < a < b) \wedge (0 < c \leq d) \Rightarrow \ ac < bd. \tag{3.12}$$

$$(0 < a \leq b) \wedge (0 < c \leq d) \Rightarrow ac \leq bd \tag{3.13}$$

Bevis. Bevises som de foregående analoge additive sætninger. ■

Sætning 88 *Hvis $x < y$ så er $-x > -y$.*

Specielt gælder $y > 0$ hvis og kun hvis $-y < 0$

Bevis. Antag at $x < y$. Ifølge trikotomiloven gælder enten $-x > -y$ eller $-x \leq -y$. Hvis $-x \leq -y$ så gælder ifølge sætning (85) at $0 = x + (-x) < y + (-y) = 0$ som er absurd. Derfor slutter vi at $-x > -y$.

Den anden del af sætningen overlades til læseren. ■

Sætning 89 *Hvis $x \leq y$ og $z < 0$, så er $xz \geq yz$. (bemærk at ulighedstegnet er vendt!)*

Bevis. Antag at $x \leq y$ og $z < 0$. Ifølge den foregående sætning er $-z > 0$ så af (15) kan vi slutte at $x(-z) \leq y(-z)$, så ifølge (3.6) $-xz \leq -yz$. Adderes $xz + yz$ til begge sider fås af (14) at $zy \leq zx$. ■

Sætning 90 $1 > 0$.

Bevis. Vi har forudsat at $1 \neq 0$. Hvis $1 < 0$ så følger af sætning (88) at $-1 > 0$. Men så gælder ifølge (15) at $1 = (-1) \cdot (-1) > 0$ hvilket strider mod antagelsen. Altså er $1 > 0$. ■

Sætning 91 ***Fortegnsreglerne:*** *Lad x og y være reelle tal. Da gælder:*

- *Hvis x og y begge er positive så er $x \cdot y$ positiv*
- *Hvis x og y begge er negative så er $x \cdot y$ positiv*
- *Hvis x er positiv og y er negativ så er $x \cdot y$ negativ*

Bevis. Overlades til læseren. ■

Sætning 92 *Hvis x er et reelt tal forskelligt fra 0, så har x og x^{-1} samme fortegn.*

Bevis. Brug fortegnsreglerne. ■

Bemærkning 93 *Overvej at det betyder at hvis $z \neq 0$ kan man dividere på begge sider af en ulighed, bare man husker at vende ulighedstegnet, når z er negativ.*

Sætning 94 *Vi kan samle ovenstående sætninger i følgende regneregler: For alle reelle tal x, y, og z gælder*

$$\begin{aligned} &x \leq y \Leftrightarrow x + z \leq y + z, \qquad x < y \Leftrightarrow x + z < y + z \\ &\textit{Hvis } z > 0 \textit{ gælder: } x \leq y \Leftrightarrow x \cdot z \leq y \cdot z, \qquad x < y \Leftrightarrow x \cdot z < y \cdot z \\ &\textit{Hvis } z < 0 \textit{ gælder: } x \leq y \Leftrightarrow x \cdot z \geq y \cdot z, \qquad x < y \Leftrightarrow x \cdot z > y \cdot z \end{aligned}$$

Bevis. Det overlades til læseren at overveje, at disse regneregler følger af de ovenstående sætninger. Bemærk at det står "$\Leftrightarrow$" i sætningen, så begge veje skal vises. ■

Sætning 95 *For alle reelle tal x, y forskellige fra 0, som begge er positive eller begge er negative, gælder*

$$x < y \Leftrightarrow x^{-1} > y^{-1}$$

Bevis. Overlades til læseren. ■

Øvelse 96 *Gælder ovenstående sætning når x, y har modsat fortegn?*

Eksempel 97 *Find de reelle tal x som opfylder uligheden*

$$\frac{2x+5}{x} \leq \frac{3x-1}{x}. \tag{3.14}$$

Først bemærker vi at vi må forudsætte at $x \neq 0$. Under denne forudsætning kan vi gange igennem med x. Men vi må dele op i to tilfælde alt efter om x er positiv eller negativ.

Antag først at x er positiv. Da kan vi gange igennem med x og beholde ulighedens retning.

$$2x + 5 \leq 3x - 1.$$

Nu kan vi så flytte led som vi plejer i en ligning og får så:

$$6 \leq x.$$

Da der gælder "$\Leftrightarrow$" mellem de ovenstående tre uligheder kan vi slutte at de positive værdier, som opfylder uligheden (3.14) netop er tallene der er større eller lig med 6.

Antag dernæst at x er negativ. Da skal vi vende ulighedstegnet, når vi ganger uligheden igennem med x, så vi får

$$\begin{aligned} \frac{2x+5}{x} &\leq \frac{3x-1}{x} \\ &\Leftrightarrow 2x + 5 \geq 3x - 1 \\ &\Leftrightarrow 6 \geq x. \end{aligned}$$

Uligheden gælder derfor for alle negative værdier af x.

Vi konkluderer altså at uligheden gælder for $x \in]-\infty, 0[\cup[6, \infty[$

Sætning 98 *Hvis x og y betegner to ikke-negative tal gælder:*

$$\begin{aligned} x = y &\Leftrightarrow x^2 = y^2 \\ x \leq y &\Leftrightarrow x^2 \leq y^2, \\ x < y &\Leftrightarrow x^2 < y^2. \end{aligned}$$

Bevis. Vi beviser den sidste biimplikation. De to første overlades til læseren.

Pilen mod højre følger af sætning (87) ved at sætte $x = a = c$ og $y = b = d$.

Pilen mod venstre vises ved kontraposition. Det kontraponerede udsagn siger $\neg(x < y) \Rightarrow \neg(x^2 < y^2)$ eller $x \geq y \Rightarrow x^2 \geq y^2$. Men det følger af (3.13) ved at sætte $x = b = d$ og $y = a = c$. ■

Sætning 99 *Hvis x og y betegner to ikke-negative tal og n et naturligt tal gælder:*

$$x = y \Leftrightarrow x^n = y^n, \tag{3.15}$$

$$x \leq y \Leftrightarrow x^n \leq y^n, \tag{3.16}$$

$$x < y \Leftrightarrow x^n < y^n. \tag{3.17}$$

Bevis. Bevises ved gentagen brug af ovenstående fremgangsmåde. Vi vil senere se hvordan sætningen kan bevises mere elegant ved såkaldt induktion. ■

3.3 Numerisk værdi

Definition 100 ***Den numeriske værdi*** *af et reelt tal x betegnes med $|x|$ og defineres ved*

$$|x| = x, \text{ hvis } x \geq 0$$
$$|x| = -x, \text{ hvis } x < 0$$

Bemærkning 101 *Den numeriske værdi af et reelt tal er altså det positive tal, man får ved at udelade et eventuelt negativt fortegn. Man kan tænke på den numeriske værdi af et reelt tal x som dets positive afstand til 0 på talaksen. Af definitionen følger at det for alle reelle tal x gælder at $|-x| = |x|$ og at $x \leq |x|$. Anvendes denne ulighed på $-x$ fås $-x \leq |-x| = |x|$. Heraf følger:*

Sætning 102 *For alle reelle tal x gælder at*

$$-|x| \leq x \leq |x| \tag{3.18}$$

Øvelse 103 *Overvej, hvornår der gælder lighedstegn til højre og til venstre i ovenstående ulighed.*

Sætning 104 *Hvis x og y betegner reelle tal gælder:*

$$x^2 = |x|^2, \tag{3.19}$$
$$|x| = |y| \Leftrightarrow x^2 = y^2, \tag{3.20}$$
$$|x| \leq |y| \Leftrightarrow x^2 \leq y^2 \tag{3.21}$$
$$|x| < |y| \Leftrightarrow x^2 < y^2. \tag{3.22}$$

Bevis. Identiteten (3.19) kan vises ved at behandle de tre tilfælde $x < 0$, $x > 0$ og $x = 0$ hver for sig. De tre biimplikationer følger heraf og af sætning (98). ■

Sætning 105 *For vilkårlige reelle tal m og y gælder*

$$|x \cdot y| = |x| \cdot |y| \tag{3.23}$$

Bevis. Man kan vise ligheden ved at op i tilfælde alt efter om x og y er positive, negative eller 0. Det er dog lettere at bemærke at vi ifølge (3.19) kan slutte at

$$(x \cdot y)^2 = x^2 \cdot y^2 = |x|^2 \cdot |y|^2 = (|x| \cdot |y|)^2.$$

Bruges nu (3.20) kan vi heraf slutte at

$$|x \cdot y| = ||x| \cdot |y|| = |x| \cdot |y|.$$

Sidste lighedstegn skyldes at $|x| \cdot |y|$ er ikke-negativ. ■

Korollar 106 *For et vilkårligt antal reelle tal $x_1, x_2, \ldots, x_n$ gælder at*

$$|x_1 \cdot x_2 \cdots x_n| = |x_1| \cdot |x_2| \cdots |x_n|.$$

Bevis. Gentagen brug af ovenstående sætning, eller mere formelt, induktion efter n. ■

Eksempel 107 *Find de reelle tal x som opfylder uligheden*

$$x^2 + x \geq 12. \tag{3.24}$$

Som når vi løser en andengradsligning er det smart at addere et tal på begge sider, så at venstresiden bliver et fuldstændigt kvadrat. Det ønskede tal er halvdelen af koefficienten til x kvadreret altså $\frac{1}{4}$:

$$\begin{aligned} x^2 + x &\geq 12 \\ &\Leftrightarrow x^2 + x + 1/4 \geq 12 + 1/4 \\ &\Leftrightarrow (x + \frac{1}{2})^2 \geq 12 + 1/4 \\ \left|x + \frac{1}{2}\right| &\geq \sqrt{12 + 1/4} = 3\frac{1}{2}. \end{aligned}$$

Hvis nu $x \geq -\frac{1}{2}$, så $x + \frac{1}{2} \geq 0$, fås:

$$\begin{aligned} \left|x + \frac{1}{2}\right| &\geq 3\frac{1}{2} \\ &\Leftrightarrow x + \frac{1}{2} \geq 3\frac{1}{2} \\ &\Leftrightarrow x \geq 3 \end{aligned}$$

Hvis derimod $x \leq -\frac{1}{2}$, så $x + \frac{1}{2} \leq 0$, fås:

$$\begin{aligned} \left|x + \frac{1}{2}\right| &\geq 3\frac{1}{2} \\ &\Leftrightarrow -(x + \frac{1}{2}) \geq 3\frac{1}{2} \\ &\Leftrightarrow -x - \frac{1}{2} \geq 3\frac{1}{2} \\ &\Leftrightarrow -x \geq 4 \\ &\Leftrightarrow x \leq -4. \end{aligned}$$

Løsningerne til uligheden (3.24) er altså de reelle tal, som ligger i mængden $]-\infty, -4] \cup [3, \infty[$

Det ville dog nok være lettere at løse den tilhørende ligning $x^2 + x = 12$ og finde rødderne 3 og -4. Da nu den tilhørende parabel er "glad", må de $x$er, som opfylder uligheden ligge uden for intervallet mellem de to løsninger.

Sætning 108 *For vilkårlige reelle tal gælder at*

$$||x| - |y|| \leq |x + y| \leq |x| + |y|\,, \tag{3.25}$$

$$||x| - |y|| \leq |x - y| \leq |x| + |y|\,. \tag{3.26}$$

Bevis. Da $|x|+|y|$ er ikke-negativ gælder at $|x|+|y| = ||x|+|y||$. Ifølge (3.21) kan vi derfor bevise (3.25) ved at vise at

$$(|x|-|y|)^2 \leq (x+y)^2 \leq (|x|+|y|)^2. \tag{3.27}$$

Da

$$\begin{aligned}(|x|-|y|)^2 &= |x|^2+|y|^2-2|x|\cdot|y| = x^2+y^2-|2xy|,\\ (x+y)^2 &= x^2+y^2+2xy,\\ (|x|+|y|)^2 &= |x|^2+|y|^2+2|x|\cdot|y| = x^2+y^2+|2xy|,\end{aligned}$$

er (3.27) ensbetydende med

$$-|2xy| \leq 2xy \leq |2xy|,$$

som følger af (3.18).
Den anden ulighed (3.26) følger af (3.25) ved at erstatte y med $-y$. ■

Øvelse 109 *Overvej, hvornår der gælder lighedstegn i (3.25) og (3.26).*

Korollar 110 *For et vilkårligt antal reelle tal $x_1, x_2, \ldots, x_n$ gælder*

$$|x_1 + x_{2+} \cdots + x_n| \leq |x_1| + |x_2| + \cdots + |x_n|.$$

Bevis. Gentagen brug af ovenstående sætning eller mere formelt ved induktion efter n. ■

Eksempel 111 *Bestem de reelle tal x, som opfylder uligheden*

$$|x-5| \leq 2.$$

Vi kan dele op i to tilfælde: $x-5 \geq 0$ (eller $x \geq 5$) og $x-5<0$ (eller $x<5$). I første tilfælde giver uligheden:

$$x-5 \leq 2 \quad \textit{eller} \quad x \leq 7,$$

og i andet tilfælde giver uligheden

$$-(x-5) \leq 2 \quad \textit{eller} \quad -x+5 \leq 2 \quad \textit{eller} \quad 3 \leq x.$$

Så de søgte værdier af x opfylder altså enten at $x \geq 5$ og $x \leq 7$, eller at $x<5$ og $3 \leq x$. Det vil sige at værdierne opfylder at $3 \leq x \leq 7$, dvs. at x ligger i intervallet $[3,7]$.

Bemærkning 112 *Den ovenstående beregning er formelt rigtig, men unødvendig kompliceret. Lidt geometrisk intuition giver resultatet direkte. Thi hvis man tænker på tallene a og b som liggende på talaksen, angiver $|a-b|$ afstanden mellem punkterne a og b. $|x-5|$ betyder altså afstanden mellem x og 5. I den ovenstående opgave skal denne afstand være mindre eller lig 2. Det betyder jo*

at x skal ligge i en afstand fra 5 som højst er 2, og det gælder jo netop tallene i intervallet $[3,7]$ (lav tegning på en tal-akse!).

Mere generelt, hvis x_0 er et givet reelt tal og ϵ er et positivt tal, betyder $|x-x_0|<\epsilon$ at x ligger i en afstand fra x_0, som er mindre end ϵ. Det gælder netop for tallene i intervallet $]x_0-\epsilon, x_0+\epsilon[$. Dette interval kaldes også en ϵ-omegn om x_0. Sådanne omegne spiller en stor rolle i den stringente fremstilling af differential- og integralregningen. Når I for eftertiden ser et udtryk som $|x-x_0|<\epsilon$, skal I ***aldrig*** *give jer til at regne, som vi gjorde i eksemplet ovenfor. I skal derimod, for jeres indre blik (eller på en tegning) se en omegn omkring x_0, som strækker sig ϵ til hver side af x_0.*

Øvelse 113 *Skitser følgende mængder på en talakse:*

1. $\left\{x\in\mathbb{R} \mid |x-10|<\frac{1}{2}\right\}$,
2. $\{x\in\mathbb{R} \mid |x-2|<3\}$,
3. $\{x\in\mathbb{R} \mid |x+5|\leq 2\}$,
4. $\{x\in\mathbb{R} \mid |x-5|\geq 3\}$.

3.4 Opgaver

1. Bevis de ikke beviste dele af Sætning 73.

2. Bevis de alternative aksiomer O1 og O2 i indledningsafsnittet ud fra aksiomssystemet brugt i dette kapittel.

3. (Omfattende) Vis ordningsaksiomerne for de reelle tal (altså (10)-(15) ud fra de alternative aksiomer O1 og O2 idet du definerer ordningsrelationen ved $x\leq y \overset{def}{\Leftrightarrow} (y-x)\in(\mathbb{R}_+\cup\{0\})$.

4. Bestem de reelle tal a og b så $\{x\in\mathbb{R} \mid (x-2)(x+4)<0\}=\{x\in\mathbb{R} \mid |x-a|<b\}$.

5. Bestem mængden $\left\{x\in\mathbb{R} \mid (x-5)^2>4\right\}$, og skitser den på den reelle akse.

6. For hvilke naturlige tal n gælder der for alle reelle x,y at

$$x^n=y^n\Leftrightarrow x=y,$$

og for hvilke gælder

$$x^n=y^n\Leftrightarrow |x|=|y|.$$

Argumenter for dit svar.

Kapitel 4

Hele tal

4.1 Divisorer og primtal

Bemærkning 114 *Tallene* $0, 1, 1+1, 1+1+1, \ldots$ *, som fås ved at begynde med* 0 *og successivt lægge* 1 *til, er alle forskellige. Thi da* $0 < 1$ *fås fra sætning 85 at* $0 < 1+1+1+\cdots+1$*. Hvis nu en sum* $1+1+1+\cdots+1$ *af* n 1*-taller er lig med en sum af* m 1*-taller (hvor* $m < n$*) så kan vi subtrahere* m 1*-taller på begge side og få* $0 = 1+1+1+\cdots+1$ *(*$n-m$ 1*-taller). Men det strider mod det lige beviste. Altså er følgen af tal vi får ved at begynde med* 0 *og successivt lægge* 1 *til en uendelig følge af forskellige tal, som vi på sædvanlig vis betegner med* $0, 1, 2, 3, 4, \ldots$.

Definition 115 $1, 2, 3, 4, \cdots$ *kaldes de* ***naturlige tal****. Mængden af naturlige tal betegnes med* $\mathbb{N}$.

Definition 116 *Tallene* $\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots$ *kaldes de* ***hele tal****. Det er altså de naturlige tal, deres additivt inverse og* 0*.Mængden af hele tal betegnes med* $\mathbb{Z}$.

Definition 117 *De tal, som kan skrives som brøker* a/b*, hvor* a *og* b *er hele tal og* $b \neq 0$*, kaldes de rationale tal . Mængden af rationale tal betegnes med* $\mathbb{Q}$.

Sætning 118 *De naturlige tal, de hele tal og de rationale tal opfylder visse af aksiomerne for de reelle tal men ikke dem alle:*

- *De naturlige tal opfylder de aksiomer, som ikke involverer inverse elementer eller nul (på nær den sidste), altså aksiomerne: (1)-(2), (5)-(7) og (9)-(15). Derudover opfylder de naturlige tal aksiomet:* $x < x+1$*, som ikke er en konsekvens af de øvrige.*

- *De hele tal opfylder alle aksiomern for de reelle tal, som ikke involverer den multiplikative inverse, dvs alle aksiomerne på nær (8).*

- *De rationale tal opfylder alle aksiomerne for de reelle tal på nær supremumsegenskaben.*

Definition 119 *Et helt tal d kaldes en **divisor** i et andet helt tal a, hvis der findes et helt tal q så $dq = a$. Vi skriver da $d \mid a$ og siger at d går op i a og at a er et **multiplum** af d.*

Øvelse 120 *Vis at hvis $d \mid a$ så vil $d \mid -a$, $-d \mid a$ og $-d \mid -a$*

Øvelse 121 *Vis at hvis $d \mid a$ og $d \mid b$ og $c \in \mathbb{Z}$ så gælder at $d \mid (a+b)$ og $d \mid ac$*

Øvelse 122 *Vis at hvis $a \mid b$ og $b \mid c$ da vil $a \mid c$*

Øvelse 123 *Vis at hvis $a \neq 0$ og $d \mid a$ så er $|d| \leq |a|$. Et helt tal forskelligt fra 0 har altså kun et endeligt antal divisorer*

Øvelse 124 *Vis at ethvert helt tal a har de **trivielle divisorer** $\pm a$, og ± 1.*

Definition 125 *Et helt tal $a \geq 2$ kaldes et **primtal** såfremt det ikke har andre divisorer end de trivielle divisorer $\pm a$, og ± 1.*

*Et helt tal $a \geq 2$ kaldes et **sammensat tal** hvis det ikke er et primtal, d.v.s. hvis det har en faktorisering $a = dq$, hvor $1 < d, q < a$.*

Bemærkning 126 *Tallet 1 kaldes altså ikke et primtal (og heller ikke et sammensat tal)*

Sætning 127 *For ethvert $n \in \mathbb{N}$ gælder: Hvis $2^n - 1$ er et primtal, da er n et primtal.*

Bevis. Vi fører beviset ved kontraposition Antag derfor, at $n \in \mathbb{N}$ ikke er et primtal. Vi vil vise, at $2^n - 1$ da heller ikke er et primtal. Såfremt $n = 1$, er dette klart, idet i så fald $2^n - 1 = 1$, som ikke er et primtal.

Vi kan altså gerne antage $n > 1$. Da n ikke er et primtal, findes en ikke-triviel faktorisering:

$$n = a \cdot b \tag{4.1}$$

hvor $a, b \in \mathbb{N}$ med $1 < a, b < n$.

Men nu verificerer man let, at vi i så fald har:

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1) \cdot (2^{a(b-1)} + \ldots + 2^a + 1) \ . \tag{4.2}$$

Idet $a > 1$, er $2^a - 1 > 1$. Idet $b - 1 \geq 1$ og $a > 1$, er $2^{a(b-1)} + \ldots + 2^a + 1 > 1$. Altså har vi i (4.2) en ikke-triviel faktorisering af $2^n - 1$. Følgelig er $2^n - 1$ ikke et primtal. ■

Bemærkning. Sætningen siger altså, at for, at $2^n - 1$ skal være et primtal, er det en nødvendig betingelse, at n er et primtal. Med andre ord: Ønsker vi at finde primtal af form $2^n - 1$, behøver vi kun at se på primtalseksponenter n.

Der findes faktisk primtal af form $2^p - 1$ (hvor altså p så selv må være et primtal): $p = 2$, $2^p - 1 = 3$ er et eksempel. Dog er ikke alle tal af form $2^p - 1$, hvor p er et primtal, selv et primtal: $p = 11$ giver et modeksempel, idet $2^{11} - 1 = 2047 = 23 \cdot 89$.

Primtal af form $2^p - 1$ kaldes *Mersenne-primtal* efter den franske matematiker Marin Mersenne (1588–1648).

Det i skrivende stund (29/5 2019) største, kendte primtal er et Mersenne-primtal, nemlig $2^{82.589.933} - 1$, et tal på 24,862,048 cifre. For mere information angående Mersenne-primtal, se:
http://www.mersenne.org/

Definition 128 *Hvis d er en divisor i de hele tal a og b siges d at være en* ***fælles divisor*** *for a og b. Den* ***største fælles divisor*** *for tallene a og b betegnes (a, b).*

Hvis $(a, b) = 1$ siges a og b at være ***indbyrdes primiske.*** *Vi siger også at a er primisk med b. I så fald er ± 1 deres eneste fælles divisor.*

Definition 129 *Hvis m er et multiplum af både a og b siges m at være et fælles multiplum af a og b. Det mindste fælles positive multiplum af a og b betegnes med $mfm(a, b)$ og kaldes det* ***mindste fælles multiplum*** *af a og b.*

Øvelse 130 *Bevis at to hele tal forskellig fra 0 har både en største fælles divisor og et mindste fælles multiplum. Find disse størrelser for tallene 10 og 15.*

Øvelse 131 *Bevis at et primtal p er indbyrdes primisk med et helt tal a hvis og kun hvis p ikke går op i a.*

Sætning 132 ***Division med rest.*** *Lad a være et helt tal og d et naturligt tal. Da findes to entydigt bestemte hele tal q (kvotienten) og r (resten), så*

$$a = dq + r \qquad og \quad 0 \leq r < d \tag{4.3}$$

Bevis. Betragt følgen: $\cdots < -3d < -2d < -d < 0 < d < 2d < 3d < \cdots$ Tallet a vil da ligge i netop et af intervallerne mellem tallene i følgen[1], så der findes præcist et $q \in \mathbb{Z}$ så

$$dq \leq a < (q + 1)d \tag{4.4}$$

eller

$$0 \leq a - dq < d. \tag{4.5}$$

Så hvis vi definerer resten r som $r = a - dq$ er $a = dq + r$. derfor følger (4.3) umidelbart af (4.5). Dermed har vi vist eksistensen af tallene q og r.

Entydigheden: Antag at der eksisterer to opskrivninger af a som i formel (4.3):

$$a = dq_1 + r_1 \qquad \text{og} \quad 0 \leq r_1 < d \tag{4.6}$$

$$a = dq_2 + r_2 \qquad \text{og} \quad 0 \leq r_2 < d. \tag{4.7}$$

[1] Det følger af velordningsegenskaben for de naturlige tal. Se Appendiks.

Heraf fås at

$$dq_1 + r_1 = dq_2 + r_2 \tag{4.8}$$

så

$$d(q_1 - q_2) = r_2 - r_1. \tag{4.9}$$

Men da r_1 og r_2 begge ligger i intervallet $[0, d)$ må deres differens være numerisk mindre end d. Altså fås

$$|d(q_1 - q_2)| < d \tag{4.10}$$

hvorfor

$$|(q_1 - q_2)| < 1. \tag{4.11}$$

Da $(q_1 - q_2)$ er et helt tal må det derfor være lig 0, så $q_1 = q_2$. Og så fås fra (4.9) at $r_2 = r_1$.

De to opskrivninger (4.6) og (4.7) må altså være ens, så der er altså kun én sådan opskrivning. ■

Bemærkning 133 *Sætningen ovenfor har fået sit navn, fordi den kan opfattes som en sætning der siger noget om hvad der sker når man dividerer a med d. Måske går divisionen a/d op, og giver et helt tal q. Så er $a/d = q$ eller $a = qd$ eller $a = qd + r$ hvor $r = 0$. Men hvis divisionen ikke går op, så dividerer vi så resten bliver mindst mulig: $a/d = q + r/d$ eller $a = dq + r$. Det er vores erfaring fra skolen at vi altid kan få resten til at blive mindre end dividenden. Det er netop det som uligheden i (4.3) siger. Når man skal bruge sætning 132 så skal man altså bare dividere a med d og finde kvotienten og resten. Grunden til at man formulerer sætningen uden at bruge division er at denne operation egentligt ikke er defineret i de hele tal.*

4.2 Euklids algoritme

Euklids algoritme[2] En algoritme til at bestemme den største fælles divisor for to naturlige tal $a \geq b$.

Sætning 134 *Først bruges division med rest på parret a, b som vi for simpelheds skyld omdøber til $a = r_0$ og $b = r_1$:*

$$r_0 = q_1 r_1 + r_2 \quad \textit{hvor} \;\; 0 \leq r_2 < r_1. \tag{4.12}$$

Hvis $r_2 = 0$ stopper vi. Ellers bruges division med rest på parret r_1, r_2 :

$$r_1 = q_2 r_2 + r_3 \quad \textit{hvor} \;\; 0 \leq r_3 < r_2. \tag{4.13}$$

Sådan fortsættes:

$$r_{i-1} = q_i r_i + r_{i+1} \quad \textit{hvor} \;\; 0 \leq r_{i+1} < r_i. \tag{4.14}$$

[2] Efter den græske matematiker Euklid, som beviste sætning 135 i sit værk Elementerne (ca. 300 f. Kr)

indtil resten bliver 0*:*

$$r_{n-1} = q_n r_n \tag{4.15}$$

Det må ske efter et endeligt antal skridt da der kun kan være endelig mange tal i rækken af rester:

$$r_0 \geq r_1 > r_2 > \cdots > r_n > 0 \tag{4.16}$$

Sætning 135 *Den sidste positive rest r_n i Euklids algoritme for to naturlige tal $a \geq b$ er deres største fælles divisor. Altså $(a, b) = r_n$.*

Bevis. 1. r_n er en divisor i a og b: Det bevises ved at trævle formlerne (4.12) - (4.15) op bagfra: Fra (4.15) ses at $r_n \mid r_{n-1}$. Men fra (4.14) ses at hvis r_n går op i både r_{i+1} og r_i (altså i to på hinanden følgende rester i algoritmen) så vil r_n også gå op i den foregående rest r_{i-1} (her bruges øvelse 121). Så da r_n går op i r_n og i r_{n-1} så går den op i r_{n-2} og derfor i r_{n-3} osv. Til slut kan vi konkludere at r_n går op i $r_1 = b$ og i $r_0 = a$.

2. r_n er den *største* fælles divisor: Dette vises ved at trævle formlerne (4.12) - (4.16) op forfra: Vi antager at d er en fælles divisor i $r_1 = b$ og $r_0 = a$. Fra (4.12) ses at d går op i r_2 (overvej), så fra (4.13) kan vi nu slutte at d går op i r_3 osv. Til slut kan vi konkludere at d går op i r_n. Enhver fælles divisor i a og b vil altså gå op i r_n hvorfor denne må være den største fælles divisor for a og b. ■

Eksempel 136 *Find den største fælles divisor i 375 og 885. Vi anvender Euklids algoritme:*

$$885 = 2 \cdot 375 + 135 \tag{4.17}$$
$$375 = 2 \cdot 135 + 105 \tag{4.18}$$
$$135 = 1 \cdot 105 + 30 \tag{4.19}$$
$$105 = 3 \cdot 30 + 15 \tag{4.20}$$
$$30 = 2 \cdot 15 \tag{4.21}$$

Altså er $(375, 885) = 15$*.*

Den næste ret bemærkelsesværdige sætning er kendt som *Bézouts Lemma.*

Sætning 137 *Hvis d er den største fælles divisor i de hele tal a og b (som ikke begge er nul), da findes hele tal x og y, så d kan skrives på formen*

$$d = xa + yb. \tag{4.22}$$

Bevis. Hvis fx. $a = 0$ vil $(a, b) = b$ og i så fald er sætningen oplagt. Ligeså hvis $b = 0$.

Hvis vi har vist sætningen for naturlige tal følger opskrivningen (4.22) for alle hele a og b. Man skriver bare $d = x\,|a| + y\,|b|$ hvorfra (4.22) fås ved evt at skifte fortegn på x eller y.

Vi skal altså bare vise sætningen for naturlige a og b. Her kan vi finde opskrivningen (4.22) ved at trævle Euklids algoritme op bagfra. Vi vil mere

generelt vise at når r_{i-1} og r_i er to på hinanden følgende rester i Euklids algoritme kan man finde hele tal x_{i-1} og y_i så

$$d = x_{i-1}r_{i-1} + y_i r_i. \tag{4.23}$$

For $i = 1$ giver denne opskrivning det ønskede (4.22) da $r_0 = a$ og $r_1 = b$.

Den næstsidste division i Euklid's algoritme ((4.14) for $i = n - 1$) giver

$$r_{n-2} = q_{n-1}r_{n-1} + r_n \tag{4.24}$$

og da $d = r_n$ kan det skrives

$$d = r_{n-2} + (-q_{n-1})r_{n-1} \tag{4.25}$$

som jo er af formen (4.23) for $i = n - 1$.

Den trediesidste division i Euklids algoritme giver

$$r_{n-3} = q_{n-2}r_{n-2} + r_{n-1} \tag{4.26}$$

eller

$$r_{n-1} = r_{n-3} - q_{n-2}r_{n-2} \tag{4.27}$$

som indsat i (4.25) giver

$$d = r_{n-2} + (-q_{n-1})(r_{n-3} - q_{n-2}r_{n-2}) = (-q_{n-1})r_{n-3} + (1 + q_{n-1}q_{n-2})r_{n-2} \tag{4.28}$$

som jo er af formen (4.23) for $i = n - 2$.

På helt samme måde ses det nu at hvis man allerede ved, at d kan skrives på formen $d = x_i r_i + y_{i+1}r_{i+1}$ for et eller andet i (altså at man allerede kender x_i og y_{i+1}) og man ønsker at finde x_{i-1} og y_i ud fra dem, så får man af (4.14) at

$$d = x_i r_i + y_{i+1}(r_{i-1} - q_i r_i) = y_{i+1}r_{i-1} + (x_i - y_{i+1}q_i)r_i. \tag{4.29}$$

Det udtrykker jo d på formen (4.23) ud fra det foregående par rester. (Man har jo netop $x_{i-1} = y_{i+1}$ og $y_i = x_i - y_{i+1}q_i$ og x_i og y_{i+1} er antaget kendte.) Ved at bruge denne udregning successivt kommer man til sidst til den ønskede opskrivning (4.22). ($x = x_0,\ a = r_0$ og $y = y_1,\ b = r_1$.) ■

Eksempel 138 *Ved at regne baglæns i Euklids algoritme for tallene 375 og 885 (eksempel 136) fås:*

$$\begin{aligned}
15 &= 105 - 3 \cdot 30 && (4.30)\\
&= 105 - 3 \cdot (135 - 1 \cdot 105) = (-3) \cdot 135 + 4 \cdot 105 && (4.31)\\
&= (-3) \cdot 135 + 4(375 - 2 \cdot 135) = (-11) \cdot 135 + 4 \cdot 375 && (4.32)\\
&= (-11) \cdot (885 - 2 \cdot 375) + 4 \cdot 375 = (-11) \cdot 885 + 26 \cdot 375 && (4.33)
\end{aligned}$$

Sætning 139 *Lad a og b være hele tal, hvoraf ikke begge er nul, og lad $d = (a, b)$ være deres største fælles divisor. Da vil et tal c være en fælles divisor i a og b hvis og kun hvis c er en divisor i d.*

Bevis. Hvis c er en divisor i d er c ifølge øvelse 122 en divisor i både a og b.

Omvendt, da d kan skrives på formen $d = xa + yb$ hvor $x, y \in \mathbb{Z}$ vil c være en divisor i d hvis det er en divisor i både a og b (iflg øvelse 121). ■

Korollar 140 *To hele tal a og b er indbyrdes primiske hvis og kun hvis der findes hele tal x og y så $1 = xa + yb$.*

Bevis. Hvis a og b er indbyrdes primiske er $(a, b) = 1$ så af sætning 137 følger at der findes hele tal x og y så $1 = xa + yb$.

Omvendt, hvis $1 = xa + yb$, hvor $x, y \in \mathbb{Z}$ vil en fælles divisor i a og b også være en divisor i 1. De fælles divisorer i a og b er altså ± 1 så den største fælles divisor er 1 hvorfor a og b er indbyrdes primiske. ■

4.3 Aritmetikkens fundamentalsætning

Sætning 141 ***Det fundamentale primtalslemma*** *Hvis a og b er hele tal og p er et primtal da gælder*

$$p \mid ab \Leftrightarrow p \mid a \quad \textit{eller} \quad p \mid b. \tag{4.34}$$

Bevis. $\Leftarrow$: Oplagt.

$\Rightarrow$: Vi benytter bevisstrategien fra anden del af Bemærkning 44. Antag at $p \mid ab$. Antag endvidere at $p \nmid a$. Da p er et primtal har p kun de trivielle divisorer ± 1 og $\pm p$, men da p ikke er divisor i a er 1 den største fælles divisor i p og a. Ifølge korollar 140 kan vi altså skrive $1 = xa + yp$, hvor $x, y \in \mathbb{Z}$. Ved multiplikation med b fås

$$b = xab + ypb \tag{4.35}$$

og da $p \mid ab$ går p op i højresiden, hvorfor $p \mid b$. ■

Bemærkning 142 *Forudsætningen om at p er et primtal er afgørende for at ovenstående sætning gælder. Find selv et eksempel på tre hele tal a, b, c så $c \mid ab$ men $c \nmid a$ og $c \nmid b$.*

Sætning 143 *Hvis $n > 1$ er et naturligt tal findes der et primtal p som går op i n.*

Bevis. Hvis n er et primtal er vi færdige. Hvis ikke kan n skrives som et produkt $n = n_1 m_1$ hvor $1 < n_1, m_1 < n$. Hvis et af tallene n_1 eller m_1 er primtal er vi færdige. Ellers kan n_1 faktoriseres som $n_1 = n_2 m_2$. Igen er vi færdige hvis et af tallene n_2 eller m_2 er primtal. Ellers fortsætter vi faktoriseringen. Derved får vi en aftagende følge af naturlige tal $n > n_1 > n_2 > \cdots > n_k$. Da der kun er endeligt mange naturlige tal mindre end n må denne følge altså stoppe på et tidspunkt, og da har vi altså nået en primdivisor i n. ■

Følgende hovedsætning og dens bevis går i al væsentligt tilbage til Euklids Elementer (ca. 300 f.Kr.)

Sætning 144 *Der findes uendeligt mange primtal.*

I beviset skal vi bruge begrebet '(ikke tom) endelig mængde', hvis betydning vi vil komme tilbage til (se afsnit 12.1). Her kan vi nøjes med at forstå dette begreb intuitivt som betydende, at mængdens elementer kan skrives op i en liste $a_1, \ldots, a_k$ nummereret ved de første k naturlige tal (for et eller andet $k \in \mathbb{N}$).

Bevis. Beviset føres som et modstridsbevis, så vi starter med at antage, at konklusionen er falsk, dvs. vi antager at mængden af primtal er endelig.

Mængden af primtal er dog ikke tom: eksempelvis er 2 klart et primtal. På grund af vores antagelse kan vi nu stille samtlige primtal op i en endelig liste $p_1, p_2, ..., p_k$. Med andre ord har vi nu - på grund af vores antagelse - følgende implikation:

$$p \text{ primtal} \Rightarrow p \in \{p_1, p_2, ..., p_k\} \tag{4.36}$$

Nu, givet de endeligt mange tal $p_1, p_2, ..., p_k$ kan vi betragte deres produkt $p_1 \cdot p_2 \cdot ... \cdot p_k$, som er et naturligt tal. Vi har dermed også følgende naturlige tal:

$$N = p_1 \cdot p_2 \cdot ... \cdot p_k + 1 \tag{4.37}$$

Da klart $N > 1$, ved vi fra Sætning 143, at der findes et primtal p, som går op i N. Dvs. vi kan skrive:

$$N = p \cdot m \tag{4.38}$$

med et naturligt tal m.

På den anden side: Idet p er et primtal, følger af (4.36), at p er et af tallene $p_1, p_2, ..., p_k$; dvs. $p = p_i$ for et $i \in \{1, 2, ..., k\}$. Men i så fald har vi:

$$p_1 \cdot p_2 \cdot ... \cdot p_k = p \cdot n \tag{4.39}$$

for et vist $n \in \mathbb{N}$, nemlig produktet af alle tallene $p_1 \cdot p_2 \cdot ... \cdot p_k$ på nær p_i.

Men sammenligner vi nu (4.37), (4.38) og (4.39), finder vi:

$$p \cdot n + 1 = p_1 \cdot p_2 \cdot ... \cdot p_k + 1 = N = p \cdot m \tag{4.40}$$

hvorfor $1 = p(m - n)$. Således går p op i 1, og p er derfor ikke et primtal. På grundlag af vores antagelse om at sætningen er falsk, har vi nu sluttet os til eksistensen af et naturligt tal p, således at

$$(p \text{ er primtal}) \wedge (p \text{ er ikke primtal}). \tag{4.41}$$

Da dette er en modstrid, er sætningen dermed bevist. ■

Sætning 145 ***Aritmetikkens fundamentalsætning.*** *Ethvert naturligt tal $n > 1$ har en entydig primopløsning.*

Det vil sige at

1. n har en primopløsnig

$$n = p_1 p_2 \cdots p_s, \tag{4.42}$$

hvor p_i'erne er primtal, og

2. hvis $n = p_1 p_2 \cdots p_s$ og $n = q_1 q_2 \cdots q_t$ er to primopløsninger af n så er $s = t$, og efter en passende omordning af q'erne kan man opnå at $p_i = q_i$ for alle $i = 1, 2, \ldots, s$.

Primtallene p_1,$p_2, \cdots, p_s$ kaldes $n's$ primdivisorer.

Bevis. Se sætning 162 og 168. ■

Sætning 146 *Hvis a og b ikke har nogen fælles primdivisor da er $(a, b) = 1$.*

Bevis. Hvis $d > 1$ er en fælles divisor i a og b må d ifølge aritmetikkens fundamentalsætning have en primdivisor, og denne må derfor være en primdivisor i både a og b. Men a og b har ingen fælles primdivisorer, så vi kan slutte at a og b ikke har nogen fælles divisorer større end 1. De er altså indbyrdes primiske. ■

Sætning 147 *Hvis a og b er naturlige tal gælder at*

$$ab = (a, b) \cdot mfm(a, b)$$

Bevis. Se opgave 3 i dette kapitel. ■

4.4 Rationale tal

Til slut skal vi se lidt på de rationale tal altså brøkerne a/b hvor a og b er hele tal (kaldet tæller og nævner) og $b \neq 0$. Det ses let at sum, differens og produkt af to rationale tal igen giver rationale tal og at et rationalt tal divideret med et rationalt tal, som ikke er 0, igen er et rationalt tal. Det er også velkendt at man kan forlænge en brøk, d.v.s gange både tæller og nævner med samme hele tal forskellig fra 0. Hvis det hele tal t går op i både tæller og nævner kan man forkorte brøken med t d.v.s. dividere tæller og nævner med t.

Definition 148 *En brøk a/b kaldes **uforkortelig** hvis $(a, b) = 1$.*

Sætning 149 *Ethvert rationalt tal kan skrives som en uforkortelig brøk m/n. Hvis det rationale tal er positivt kan man vælge m og n positive.*

Bevis. Lad a/b være et rationalt tal hvor $a > 0$ og $b > 0$. Da kan a og b primopløses. Ved at forkorte alle fælles primdivisorer bort kan man opnå at $a/b = m/n$ hvor m og n er naturlige tal uden fælles primdivisorer. Men så følger af sætning 146 at $(m, n) = 1$.

Hvis $a/b < 0$ kan a/b skrives på formen $(-c)/e$, hvor $c > 0$ og $e > 0$. Ved at bruge ovenstående argument på c/e fås det ønskede.

Tallet 0 kan skrives som $0/1$, som er uforkortelig. ■

4.5 Opgaver

1. Brug Euklids algoritme til at bestemme den største fælles divisor d i 616 og 1210. Bestem dernæst hele tal x og y så

$$d = x \cdot 616 + y \cdot 1210. \tag{4.43}$$

2. Find primopløsninger af tallene 1001 og 5390 og opskriv 1001/5390 som uforkortelig brøk.
3. Find største fælles divisor for 825 og 693.
4. Find mindste fælles multiplum for 825 og 693.
5. Bestem største fælles divisor d for 1155 og 550 og bestem hele tal x,y så d=1155x+550y

6. Formuler og bevis en sætning om hvordan man fra primopløsningerne for to naturlige tal kan bestemme deres største fælles divisor og deres mindste fælles multiplum. Bevis dernæst Sætning 147.

Kapitel 5

Analyse og syntese.

5.1 Matematisk kreativitet

Videnskabsteoretikere skelner mellem en "context of justification" og en "context of discovery". Den første handler om, hvordan man argumenterer for allerede indhøstet viden, den anden om, hvordan man opdager eller skaber ny viden. I matematik argumenterer man for sin viden ved hjælp af de meget formaliserede og stringente beviser, som DIS især handler om. Men ny viden indhøstes sjældent på denne måde. I princippet kunne man fodre en computer med alle en teoris aksiomer og alle de tilladte slutningsregler, og så sætte den til at bevise nye sætninger. Det vil den også kunne gøre, men langt størstedelen af de sætninger maskinen vil udlede, ville vi mennesker opfatte som aldeles uinteressante. Hvis man for eksempel bad en computer (eller en fantasiløs person) om at deducere sætninger om de naturlige tal, kunne den måske gå i gang med at bevise at $1 + (1 + 1) = (1 + 1) + 1$, $1 + (1 + (1 + 1)) = ((1 + 1) + 1) + 1$, og så videre. Computeren ville dermed have udstukket et "forskningsprojekt", som til dommedag ville blive ved med at spytte sande sætninger ud. Men ikke én af disse sætninger ville forekomme os at være interessante.

Dette eksempel viser, hvad der sker, hvis man på må og få deducerer sætninger fra aksiomerne. Problemet er at vi ikke kan formalisere, hvilke sætninger der er interessante og hvilke der er uinteressante. Det er her matematikere af kød og blod kommer ind. Matematikeren bruger sin intuition, sin fantasi, analogier mm. til at udtænke sætninger, som er interessante. Om de så er sande, må man checke ved formelle beviser. Men også udtænkningen af disse beviser kræver fantasi og intuition.

Mange matematikere, psykologer og filosoffer har diskuteret, hvordan matematikere får ideer til nye resultater og deres beviser. I princippet er alt tilladt i denne kreative fase af matematikken. Så længe den kreative proces ender med et stringent bevis for sætningen, er vi tilfredse. Matematisk kreativitet er lige så uforklarlig som kreativitet i andre områder af menneskelivet og er derfor svær at undervise i. (Se dog for eksempel Polya's bog "How to solve it"). Der er

dog visse heuristiske metoder, som man kan lære sig. Dette kapitel handler om en af dem, nemlig den matematiske analyse. Den kommer i to udgaver: en til brug ved problemløsning, og en anden, som man bruger, når man skal finde på beviser for sætninger. *Begge er kendetegnet ved at de tager udgangspunkt i det søgte, ubekendte eller ubeviste og arbejder sig tilbage til det kendte eller beviste.*

5.2 Eksistensproblemer

Problem 150 *Undersøg om polynomiet* $P(x) = x^4 - 2x^3 - 3x^2 + 5x + 2$ *har rationale rødder, og i så fald hvilke.*

Her er altså tale om et eksistensproblem, efterfulgt af et problem om at bestemme samtlige objekter, som opfylder det ønskede. I forrige afsnit beviste vi at 2 var en rational rod i polynomiet. Men vi afslørede ikke, hvordan tallet 2 var fremkommet. Vi trak det bare op af hatten. Her skal vi se, hvordan man kan komme frem til denne kandidat.

Man kunne måske tro, at problemet mest effektivt løses ved at bruge en formel for løsningen af ligningen. Det er imidlertid ikke tilfældet. Ganske vist findes der en formel for løsningen af en fjerdegradsligning. Men den er meget kompliceret, og det vil være meget svært ad den vej at bestemme om rødderne er rationale tal. Mere metodologisk kan man også sige at det vil være at skyde gråspurve med kanoner hvis man brugte en formel som frembringer samtlige fire komplekse rødder, når nu spørgsmålet kun handler om rationale løsninger.

Lad os i stedet begynde med eksistensproblemet: Findes der et rationalt tal, som er rod i $P(x)$? Hvis vi kan finde et rationalt tal p/q så $P(p/q) = 0$, så har vi besvaret spørgsmålet med ja. Beviset går da bare ud på at indsætte p/q i $P(x)$ og vise, at resultatet er nul. Men hvordan skal vi finde en kandidat p/q?

Analyse.

Det gøres mest effektivt ved at lave en *analyse* af problemet. En analyse går ud på, at vi *antager,* vi har bestemt et objekt, der har den ønskede egenskab (en løsning til problemet), og så ser vi, hvad vi kan udlede om dette objekt. I det forelagte problem antager vi, at p/q er en rod i polynomiet og undersøger, om vi deraf kan slutte os til noget om p og q.

Vi vil først gå lidt mere generelt til værks, idet vi antager at p/q er en rod i polynomiet $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ med heltallige koefficienter. Vi antager altså at

$$a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0 = 0. \tag{5.1}$$

Hvis vi ganger igennem med q^n, ser vi at

$$a_n p^n + a_{n-1}p^{n-1}q^1 + \cdots + a_1 p q^{n-1} + a_0 q^n = 0 \tag{5.2}$$

Ifølge sætning 149 kan vi endvidere antage, at p/q er forkortet mest muligt så de to hele tal p og q er indbyrdes primiske (dvs. at de ikke har nogen fælles hele

divisorer ud over 1 og -1). Hvis vi nu isolerer første led i ligningen fås:

$$a_n p^n = -a_{n-1}p^{n-1}q^1 - \cdots - a_1 pq^{n-1} - a_0 q^n. \tag{5.3}$$

Da q går op i alle led på højresiden, og derfor i hele højresiden, går det også op i venstresiden $a_n p^n$. Men da q er indbyrdes primisk med p og derfor med p^n, må q gå op i a_n. Her har vi brugt, at hvis et helt tal q går op i et produkt rs af to hele tal, og det er indbyrdes primisk med det ene tal r, så må det gå op i det andet tal s (Dette bevises ved samme teknik som blev brugt i beviset for det fundamentale primtalslemma Sætning 141).

Ved at isolere $a_0 q^n$ i ligning (5.2) kan vi på helt samme måde se, at p må gå op i a_0. Vi har dermed vist følgende sætning:

Sætning 151 *Hvis en uforkortelig brøk p/q ($p, q \in \mathbb{Z}$) er rod i polynomiet $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ med heltallige koefficienter, så går p op i a_0, og q går op i a_n*

Hvis vi nu betragter det konkrete polynomium $P(x) = x^4 - 2x^3 - 3x^2 + 5x + 2$ så siger sætningen, at hvis den uforkortelige brøk p/q er rod i polynomiet, så vil p gå op i 2, og q vil gå op i 1. Det betyder at p er en af tallene 1, -1, 2, -2, og q er et af tallene 1, -1. Derfor må p/q være et af tallene 1, -1, 2, -2.

Hvad er det vi nu har vist? Har vi vist at de fire tal 1, -1, 2, -2 er rødder i polynomiet, eller at et af tallene er rod i polynomiet? Nej, vi har ikke vist nogen af delene. Det vi har vist er, at *hvis* polynomiet har rationale rødder, skal de findes blandt disse fire tal. Vi har med andre ord fundet fire kandidater til eksistensproblemet. Hermed er analysen slut.

Syntese.

Når vi har kandidaterne kan vi gå i gang med at bevise, at de opfylder det ønskede, eller rettere undersøge *om* de opfylder det ønskede. Det kalder man ofte *syntesen*.

I det forelagte problem skal vi bare indsætte de fire tal 1, -1, 2, -2 i ligningen, det ene efter det andet, og undersøge om ligningen er opfyldt. Vi ser let at $P(1) = 3$, $P(-1) = -3$, $P(2) = 0$ og $P(-2) = 12$. Altså har vi bevist, at der eksisterer en rational rod i polynomiet $P(x)$.

Entydigheden.

Hvis vi bare var faldet over kandidaten 2 ved at prøve os frem eller ved et inspireret gæt, ville vi også ved indsættelse have kunnet bevise, at den var en rod. Men analysen har faktisk givet os meget mere information. Vi sluttede jo fra analysen, at *hvis* p/q var en rational rod i polynomiet, så måtte p/q være et af de fire tal 1, -1, 2, -2. Vi ved altså, at der ikke eksisterer andre rationale rødder end disse fire. Da vi derefter ved simpel indsættelse i polynomiet konstaterede, at de tre tal 1, -1, -2 ikke var rødder, medens 2 var en rod, kan vi nu slutte at 2 er den *eneste* rationale rod i ligningen. Ud over at give os en kandidat til eksistensspørgsmålet har analysen altså givet os et entydighedsbevis. Og vi har endog fået fundet den entydigt eksisterende rod. Dermed har vi fået løst hele Problem 150.

5.3 Analyse og syntese

Lad os rekapitulere, hvad analyse-syntese metoden går ud på. Vi ønsker at vise, at der eksisterer et objekt med en bestemt egenskab. Vi antager at vi kender objektet og undersøger, hvad vi kan sige om det. Hvis det er et algebraisk objekt, giver vi det et navn som et bogstav (her kaldte vi det p/q), og vi regner med det som om det var kendt. Hvis det er et geometrisk objekt, tegner vi det ind på figuren og deducerer, som om det var kendt (vi laver en prøvefigur). I heldige tilfælde kan vi slutte os til, at hvis objektet findes med de givne egenskaber, så er det entydigt bestemt. Hvis det sker har vi allerede vist entydigheden af objektet, i den forstand at hvis der overhovedet findes et objekt med de ønskede egenskaber, så er der kun et, nemlig det objekt (den kandidat), som kom ud af analysen. For at vise eksistensen skal vi bevise at (eller om) kandidaten har den ønskede egenskab. Hvis den har egenskaben, har vi vist eksistensen (og eftervisningen kaldes det syntetiske bevis eller syntesen); hvis den ikke har egenskaben, har vi vist, at der ikke eksisterer objekter med den givne egenskab.

I andre tilfælde (som i ovenstående eksempel) fører analysen ikke til en entydig karakterisation af det søgte objekt, men til en overskuelig mængde kandidater (i ovenstående eksempel fire kandidater). Man må da efterprøve, om kandidaterne har egenskaben. Hvis ingen har egenskaben kan vi slutte, at der ikke eksisterer løsninger til problemet. Hvis nogle af kandidaterne opfylder egenskaben, så udgør beviset herfor det syntetiske eksistensbevis. Desuden har vi vist, at der ikke findes andre løsninger på problemet. Hvis der kun er én af kandidaterne, som opfylder egenskaben, giver analysen entydigheden af løsningen. Hvis der er flere, fås ikke entydighed, men vi har fundet hele mængden af løsninger.

Øvelse 152 *I Kapitel 2 beviste vi sætningen: Der findes et naturligt tal x så $x^2 = x$. Lav en analyse, og undersøg, om det fører til en entydig kandidat. Gennemfør syntesen, og formuler den sætning, du kan konkludere ud fra undersøgelsen.*

5.4 Ligningsløsning. Et eksempel på analyse - syntese

Når man løser ligninger benytter man analyse - syntese metoden. Lad os se på et eksempel:

Problem 153 *Find et kvadrat, som lagt sammen med sin side giver 2.*

Med andre ord: Vi ønsker at finde ud af, om der eksisterer sådanne kvadrater, og hvis der findes nogen, skal vi angive dem. Vi fortolker opgaven sådan, at det vi skal finde, er længden af det ønskede kvadrats side.

Hvis vi kun var interesseret i eksistensspørgsmålet kunne et bevis se således ud:

Da $1^2 + 1 = 2$ har et kvadrat med siden 1 den ønskede egenskab.

Men hvis vi også vil forklare, hvor ettallet kom fra (eller vi ikke kan gætte det), og vi også ønsker at undersøge om der findes andre løsninger, kan vi ty til en *analyse* af problemet:

Vi *antager* derfor, at vi kender et kvadrat, som har den givne egenskab, og vi kalder dens sidelængde x. Nu opererer vi med x som om det var et kendt tal. Da kvadratet antages at opfylde egenskaben i problemet, gælder der, at

$$x^2 + x = 2 \tag{5.4}$$

Hvis vi lægger $\frac{1}{4}$ til på begge sider, får vi, at x må opfylde at

$$x^2 + x + \frac{1}{4} = (x + \frac{1}{2})^2 = 2\frac{1}{4}, \tag{5.5}$$

og dermed, at

$$x + \frac{1}{2} = \pm\sqrt{2\frac{1}{4}} = \pm 1\frac{1}{2}, \tag{5.6}$$

så

$$x = 1 \text{ eller } x = -2. \tag{5.7}$$

Vi har nu fundet ud af at hvis x er siden i et kvadrat, som lagt sammen med sin side er lig med 2, så må x være et af tallene 1 eller -2. Det færdiggør analysen.

Nu skal vi vise om de to tal virkeligt opfylder betingelsen:

Da 1 er længden af siden i et kvadrat, og $1^2 + 1 = 2$, er 1 en løsning på problemet. Tallet -2 derimod, kan ikke være længde af et kvadrats side så -2 er ikke en løsning på problemet. Altså er 1 den eneste løsning af problemet. Vi har dermed vist en eksistens og entydighedssætning.

Faktisk er det netop dette vi gør når vi løser ligninger. Vi kalder den ubekendte x og regner med den, som om den var kendt. Efter en række omskrivninger af den oprindelige ligning (som er den egenskab x skal opfylde), kommer vi (forhåbentligt) frem til nogle værdier af x. Hvis vi vil løse $x^2 + x = 2$ kan vi ligesom ovenfor argumentere som følger:

$$x^2 + x = 2 \tag{5.8}$$

$$\Rightarrow x^2 + x + \frac{1}{4} = 2\frac{1}{4} \tag{5.9}$$

$$\Rightarrow (x + \frac{1}{2})^2 = 2\frac{1}{4} \tag{5.10}$$

$$\Rightarrow x + \frac{1}{2} = \pm\sqrt{2\frac{1}{4}} = \pm 1\frac{1}{2} \tag{5.11}$$

$$\Rightarrow x = 1 \text{ eller } x = -2 \tag{5.12}$$

Det vi så har argumenteret for er, at hvis x opfylder ligningen så er $x = 1$ eller $x = -2$. For at bevise at 1 og -2 virkeligt er løsninger, skal vi "gøre prøve", dvs. vi skal indsætte de to værdier i ligningen og se, om de opfylder den. Det

gør de, hvorfor vi kan slutte at 1 og -2 er løsninger til ligningen, og de er de eneste.

I den ovenstående deduktion (5.7) brugte vi kun medførepile. Det var derfor vi efter endt deduktion ikke kunne slutte baglæns til, at 1 og -2 faktisk også er løsninger til ligningen. Man kan også ved ligningsløsning vælge at slutte ensbetydende ved hver omskrivning. Faktisk er alle de åbne udsagn i kæden (5.10) ensbetydende, så vi i virkeligheden kan slutte således:$\Leftrightarrow$

$$x^2 + x = 2 \tag{5.13}$$

$$\Leftrightarrow x^2 + x + \frac{1}{4} = 2\frac{1}{4} \tag{5.14}$$

$$\Leftrightarrow (x + \frac{1}{2})^2 = 2\frac{1}{4} \tag{5.15}$$

$$\Leftrightarrow x + \frac{1}{2} = \pm\sqrt{2\frac{1}{4}} = \pm 1\frac{1}{2} \tag{5.16}$$

$$\Leftrightarrow x = 1 \text{ eller } x = -2 \tag{5.17}$$

Når man gør det, kan man naturligvis straks konkludere at 1 og -2 er løsninger og de er de eneste. Der er altså ikke grund til at lave en særskilt syntese eller prøve. Vi har sammenbygget analysen og syntesen.

Nogle gange kan det godt betale sig at slutte gennem ensbetydende udsagn, men andre gange er det for besværligt at holde rede på begge implikationerne samtidigt, og det kan være en kilde til fejl i argumentet. Så meget ofte er det lettere og mere sikkert at holde de to implikationsretninger separate, og altså lave analysen og syntesen hver for sig.

5.5 Ikke stringent analyse

Hvis man bare er interesseret i et rent eksistensudsagn, er det som sagt ligegyldigt, hvordan man kommer frem til en kandidat, bare det kan bevises, at den virker. Man kan stadig have glæde af at lave en analyse, men så behøver man ikke gøre sig umage for at sikre sig, at ens slutninger i analysen er helt stringente. Lad os se på et eksempel. I parenteser angiver jeg de overvejelser vi springer over:

Problem 154 *Vis at der eksisterer en løsning til differentialligningen*

$$f''(x) = -f(x) \tag{5.18}$$

på $\mathbb{R}$ *som opfylder*

$$f(0) = 0 \quad og \quad f'(0) = 1. \tag{5.19}$$

Analyse: Antag at f løser problemet og skriv den som en potensrække

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 \cdots + a_n x^n + \cdots \tag{5.20}$$

(Det er slet ikke sikkert, at en eventuel løsning kan skrives som en potensrække; men det bekymrer vi os ikke om. Vi bekymrer os heller ikke for meget om rækkens konvergens). Vi differentierer rækken to gange og får:

$$f'(x) = a_1 + 2a_2x + 3a_3x^2 \cdots + na_nx^{n-1} + \cdots \tag{5.21}$$

$$f''(x) = 2a_2 + 2 \cdot 3a_3x \cdots + (n-1)na_nx^{n--2} + \cdots \tag{5.22}$$

(Her differentierer vi ledvist uden at bekymre os om vi nu må gøre det). Differentialligningen kan altså skrives:

$$2a_2 + 2 \cdot 3a_3x \cdots + (n-1)na_nx^{n--2} + \cdots \tag{5.23}$$

$$= -(a_0 + a_1x + a_2x^2 + a_3x^3 \cdots + a_{n-2}x^{n-2} + \cdots). \tag{5.24}$$

Sammenlignes led til ens potenser af x (må vi det?), får vi ligningssystemet:

$$2a_2 = -a_0 \tag{5.25}$$

$$2 \cdot 3a_3 = -a_1 \ ... \tag{5.26}$$

$$(n-1)na_n = a_{n-2} \ ... \tag{5.27}$$

Men da vi forudsatte, at $f(0) = 0$ og $f'(0) = 1$ (5.19), ser vi fra (5.20), (5.21), at $a_0 = 0$ og $a_1 = 1$. Så fra (5.26) ser vi, at $a_2 = 0$, $a_3 = -\frac{1}{3!}$, $a_4 = 0$, $a_5 = \frac{1}{5!}$ osv. (Vi behøver ikke gå igennem et egentligt induktionsbevis). Det fører til følgende rækkeudvikling:

$$f(x) = x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5 - \cdots \tag{5.28}$$

Vi genkender denne række som potensrækken for $\sin x$ og har derfor fundet en kandidat til en løsning af problemet.

Så kan det egentlige bevis (syntesen) begynde. Beviset går simpelthen ud på at checke, at funktionen $\sin x$ opfylder differentialligningen (5.18) på hele $\mathbb{R}$ og begyndelsesværdibetingelserne (5.19) i 0. Det ses let at være tilfældet. Dermed har vi løst eksistensproblemet og fundet en løsning på problemet.

Selv om vi ikke var omhyggelige med vores argumenter i analysen, gav den os altså en brugbar kandidat, som vi kunne bruge i eksistensbeviset. Men netop fordi vi ikke var omhyggelige med analysen, kan vi ikke bruge den til at slutte, at vi har fundet den eneste løsning. Analysen havde jo ikke formen: Hvis f er en løsning, så må den være af formen (5.28). Den havde i stedet formen: Hvis f er en løsning, og forskellige andre ting er opfyldt (især at f kan rækkeudvikles i en potensrække som er konvergent overalt på $\mathbb{R}$), så er f af formen (5.28). Hvis vi havde holdt rede på hvilke ting vi havde forudsat undervejs i analysen, kunne vi have sluttet at $\sin x$ er den eneste løsning til problemet, som opfylder disse forudsætninger. Men da vi ikke holdt rede på det må vi nøjes med at bruge analysen til at give os en kandidat til løsningen.

5.6 Advarsler

Man skal passe meget på med ikke at forveksle analysen med syntesen, og man skal være opmærksom på at analysen kun leverer kandidater og eventuelt viser

entydighed (eller n-tydighed). Der er berømte eksempler på, at selv gode matematikere har forvekslet en analyse med en syntese. Lad os illustrere det med et bevis for cirklens såkaldt "isoperimetriske" egenskab:

Cirklen er den lukkede kurve med given omkreds (iso=ens, perimeter=omkreds), som omslutter det største areal.

Jacob Steiner gav følgende bevis: Han antog at en kurve med den givne omkreds omsluttede det størst mulige areal og viste så, at kurven måtte være en cirkel. (Vi skal ikke gå ind på hans elegante og korrekte bevis for dette). Derfra sluttede han at cirklen havde den isoperimetriske egenskab. Som Dirichlet senere påpegede, kan man naturligvis ikke slutte sådan. Det eneste man kan slutte fra Steiners argument er en entydighed, nemlig at *hvis* der eksisterer en isoperimetrisk kurve, så må det være cirklen. Steiner havde faktisk kun lavet analysen og havde glemt syntesen. Det skyldes naturligvis, at han mente, at det var klart, at der eksisterer en isoperimetrisk kurve. Men det er faktisk noget der bør bevises.

Lad mig vise et eksempel på hvordan man kan komme til et helt absurd resultat, hvis man på Steinersk vis forveksler analysen med syntesen, idet man forudsætter eksistensen af det objekt man vil finde:

"Sætning". Tallet 1 er det største naturlige tal.

"Bevis". Antag at n er det største naturlige tal. Jeg vil nu vise ved kontraposition at $n = 1$. Antag nemlig at $n \neq 1$. Så er $n^2 > n$ hvorfor n ikke er det største naturlige tal. Derfor må n altså være lig med 1. Derfor er 1 det største naturlige tal. QED

Konklusionen er her så åbenlys tåbelig, at alle kan se, at der er noget galt med beviset. Det, der er galt, er at vi har forvekslet analysen med syntesen. Vi argumenterede helt rigtigt for at *hvis* n er det største naturlige tal må n være lig med 1. Det er en analyse. Det vi heraf kan slutte er at 1 er den eneste mulige kandidat, altså at *hvis* der et største naturligt tal, må det være tallet 1. Det går først galt når vi derfra slutter at så må 1 være det største naturlige tal. Det ville vi kunne gøre, hvis vi havde et bevis for, at der eksisterede et største naturligt tal. Men da dette naturligvis er usandt, kan vi ikke slutte fra analysens entydighedsudsagn til eksistensudsagnet. Steiner's bevis for cirklens isoperimetriske egenskab er af helt samme natur, blot er eksistensudsagnet i dette tilfælde intuitivt plausibelt (og faktisk også korrekt under passende antagelser). Steiner gav dog ikke eksistensbeviset.

Lad os se på endnu en forkert brug af en analyse:

Definition 155 *Følgen af* ***Fibonaccital***[1] a_n *defineres rekursivt ved at* $a_1 = a_2 = 1$ *og* $a_{n+2} = a_{n+1} + a_n$.

De første led i følgen er: 1,1,2,3,5,8,13,21....

Sætning 156 *Forholdet* a_{n+1}/a_n *mellem to på hinanden følgende Fibonaccital konvergerer mod* $\frac{1+\sqrt{5}}{2}$ *for* $n \longrightarrow \infty$

[1] Efter Leonardo Fibonacci af Pisa (ca. 1170-1240)

"Bevis": Da $a_{n+2} = a_{n+1} + a_n$, fås ved division med a_{n+1}at

$$\frac{a_{n+2}}{a_{n+1}} = 1 + \frac{a_n}{a_{n+1}}. \tag{5.29}$$

Hvis grænseværdien af forholdet a_{n+1}/a_n kaldes A, ses af ovenstående ligning (ved brug af regnereglerne for grænseværdier), at

$$A = 1 + \frac{1}{A} \tag{5.30}$$

eller

$$A^2 = A + 1. \tag{5.31}$$

Denne ligning har rødderne $A = \frac{1\pm\sqrt{5}}{2}$. Da det er klart at grænseværdien ikke kan være negativ, må den være lig med $\frac{1+\sqrt{5}}{2}$ (det gyldne snit). QED

Kommentar: Resultatet er faktisk korrekt, men argumentet er ikke korrekt. I argumentet har vi jo taget for givet, at følgen a_{n+1}/a_n konvergerer. Vi har således i virkeligheden ikke lavet et bevis men en analyse. Vi har nemlig set at *hvis* følgen a_{n+1}/a_n konvergerer, må grænseværdien være $\frac{1+\sqrt{5}}{2}$. Men vi har ikke vist konvergensen.

Igen kan vi illustrere hvor galt det kan gå, hvis man bruger et lignende argument på en anden følge:

"Sætning". Fibonaccifølgen a_n konvergerer mod 0 for $n \longrightarrow \infty$.

"Bevis". Hvis grænseværdien kaldes a, fås fra den definerende ligning $a_{n+2} = a_{n+1} + a_n$ at $a = a + a$, hvoraf vi slutter at $a = 0$.

"Sætningen" og dens "bevis" er naturligvis forkerte, og faktisk divergerer a_n mod ∞ for $n \longrightarrow \infty$.

5.7 Terminologi

I matematik betyder ordet analyse faktisk to meget forskellige ting. Den betydning vi her har set på går tilbage til antikke græske matematikere og filosoffer. Når man taler om matematisk analyse i dag mener man dog normalt den gren af matematikken, som er udsprunget af differential- og integralregningen og som indeholder emner som uendelige rækker, differentialligninger, topologiske vektorrum mm.

5.8 Problem- og sætningsanalyse

Alle analyser, vi har set på indtil nu, er analyser af problemer. Analyse-metoden er dog også nyttig når man skal bevise sætninger. Som forklaret i Afsnit 2.2 er et bevis for en sætning jo en kæde af udsagn, som ender med denne sætning, og hvori ethvert udsagn enten er et aksiom i teorien, eller en allerede bevist sætning eller fremgår ved en gyldig slutning af de tidligere udsagn i kæden. Beviser

for sætninger starter altså med aksiomerne, eller allerede beviste sætninger og foregår ved successive gyldige slutninger derfra. Hvis man skal bevise en bestemt sætning er problemet naturligvis, at det sjældent er klart, hvilke aksiomer og tidligere sætninger, man skal ty til, og hvilke logiske slutninger, man skal lave for at nå frem til sætningen. Blind brug af tidligere sætninger og slutningsregler fører sjældent (aldrig) til målet. Derimod kan man få ideen til beviset ved at starte med den sætning, man skal bevise, og så prøve at finde nogle udsagn, hvorfra sætningen kan udledes. Hvis disse er aksiomer eller allerede beviste sætninger er vi færdige. Hvis ikke, prøver vi at finde andre udsagn, hvorfra de kan udledes og så videre. Hvis man er heldig, vil man til sidst ende med nogle udsagn, som man ved er sande, fordi de enten er aksiomer eller allerede beviste sætninger.

For at tydeliggøre denne ide, kan vi se på en sætning s, som kan bevises ved følgende simple kæde af udsagn startende fra aksiomet a.

$$a \Rightarrow p_1 \Rightarrow p_2 \Rightarrow p_3 \Rightarrow p_4 \Rightarrow s \tag{5.32}$$

Hvis vi bliver bedt om at finde et bevis for s, kan vi gå frem på følgende måde: Jeg vil bevise s. Hvis jeg bare kunne bevise p_4, ville jeg være færdig, thi s følger fra p_4. Men for at bevise p_4, behøver jeg bare bevise p_3, thi p_3 medfører p_4. Og da $p_2 \Rightarrow p_3$, vil jeg være færdig, hvis jeg bare kunne vise p_2. Men p_2 følger fra p_1, som er sand, da den følger fra aksiomet a. På denne måde vil vi altså have trævlet beviset op bagfra. Jeg vil kalde dette en analyse, fordi vi begynder med det vi vil vise og ender med det vi ved er sandt. Men da vi hele tiden har argumenteret med pilene i den rigtige retning, giver analysen faktisk et korrekt bevis. Man vil ofte foretrække at præsentere det færdige bevis ved at starte med a og så arbejde sig til højre i kæden af udsagn. Men det skyldes kun æstetiske hensyn og ønsket om at gøre beviset mere overskueligt. Derved adskiller denne type analyser sig fra de ovenfor behandlede problemanalyser, hvor analysen og syntesen var helt adskildte.

Man kunne naturligvis også lave en bevisanalyse ved at gå gennem en kæde af konsekvenser af sætningen indtil man når et aksiom eller noget bevist:

$$a \Leftarrow p_1 \Leftarrow p_2 \Leftarrow p_3 \Leftarrow p_4 \Leftarrow s, \tag{5.33}$$

men så skal man ligesom i problemanalysen efterfølgende lave en separat syntese, som sikrer at man faktisk kan gå den modsatte vej fra a til s.

I de fleste tilfælde er strukturen af et bevis for en sætning mere kompleks end en simpel kæde som (5.32), og i mange tilfælde har man faktisk også en fornemmelse af hvilke sande sætninger eller aksiomer, man skal begynde med. Det gælder især i matematikundervisningen hvor man bliver præsenteret for en velformuleret sætning, som man skal bevise. I dette tilfælde har sætningen altid formen: Hvis a, b, c, d så e. I beviset skal man så antage at a, b, c, d er sande og skal så bevise at e er sand. I dette tilfælde er det klart at udsagnene a, b, c, d skal indgå i beviset (måske sammen med andre aksiomer og sætninger i den teori sætningen er en del af). I sådanne tilfælde vil man normalt prøve at finde beviset ved at starte fra begge ender og se, om man kan få argumentet

til at mødes på midten. Mere præcist, man vil prøve at finde konsekvenser af a, b, c, d, som går i retning af e, og man vil prøve at finde udsagn som medfører e og som ligger "nærmere" ved a, b, c, d. Forhåbentligt kan man så få processen til at mødes på midten. Vi skal senere se på nogle eksempler.

5.9 Opgaver

1. Find de rationale rødder i polynomiet $2x^2 + 5x - 3$.

Kapitel 6

Induktionsbeviser

6.1 Simpel induktion

Ved beviser for sætninger, der involverer et vilkårligt naturligt tal, kan man ofte benytte en særlig bevisteknik kaldet induktion. Lad os som eksempel betragte følgende sætning:

Sætning 157 *For ethvert $n \in \mathbb{N}$ gælder, at summen af de første n ulige tal er lig med n^2, altså:*

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2 \tag{6.1}$$

Man kan naturligvis prøve sætningen af for de første værdier af n:

$$1 = 1^2 \tag{6.2}$$

$$1 + 3 = 4 = 2^2 \tag{6.3}$$

$$1 + 3 + 5 = 9 = 3^2 \tag{6.4}$$

$$\text{osv.} \tag{6.5}$$

Men uanset hvor mange værdier af n vi tester sætningen for, vil det ikke kunne gøre det ud for et bevis. Højst en sandsynliggørelse.

Den generelle metode til at bevise en universel sætning, som skal gælde om alle $n \in \mathbb{N}$, er at antage at n er et vilkårligt naturligt tal, og så bruge generelle sætninger om naturlige tal til at vise sætningen for n. For eksempel vil et bevis for den generelle gyldighed af

$$(n + 1)^2 = n^2 + 2n + 1 \tag{6.6}$$

forløbe således:

Lad $n \in \mathbb{N}$. Da følger af regnereglerne for naturlige tal, at

$$(n + 1)^2 = (n + 1)(n + 1) \tag{6.7}$$

$$= n^2 + n + n + 1 = n^2 + 2n + 1. \tag{6.8}$$

Det er imidlertid svært at se, hvordan man på denne måde direkte skulle kunne udlede (6.1). Hvis man derimod først har fået udledt sætningen for et bestemt n, så er det let at se at sætningen også er sand for det næste naturlige tal $n+1$. Hvis vi ved at $1+3+5+\cdots+(2n-1)=n^2$, så kan vi nemlig argumentere som følger:

$$(n+1)^2 = n^2+2n+1 = 1+3+5+\cdots+(2n-1)+(2n+1)\,, \tag{6.9}$$

hvorfor sætningen er sand for det efterfølgende naturlige tal $n+1$. Men når først vi har indset, hvordan vi på denne måde kan komme fra n til $n+1$, kan vi jo argumentere for sætningen på følgende vis:

Først indses at (6.1) er sand for $n=1$. Det har vi checket i (6.2). Men så må (6.1) gælde for det efterfølgende naturlige tal, altså for $n=2$, hvorfor det gælder for $n=3$, hvorfor det gælder for $n=4$, osv. Ligesom i (6.5) slutter dette argument med osv. men nu har vi vished for, at vi faktisk kan fortsætte argumentet skridt for skridt lige så længe vi vil, hvorved vi vil kunne nå et hvilket som helst naturligt tal.

Generelt kan vi bevise en sætning for alle værdier af $n \in \mathbb{N}$ ved at bevise

1. at sætningen er sand for $n=1$

2. at *hvis* sætningen er sand for n lig en bestemt værdi m, *så* er den sand for $n=m+1$

Vi kan formulere dette princip som en sætning:

Sætning 158 *(Princippet om **simpel induktion**). Lad $p(x)$ være et prædikat, hvor den frie variabel x kan løbe over de naturlige tal $\mathbb{N}$.*

Såfremt $p(x)$ har følgende 2 egenskaber:

1. *$p(1)$ er sand,*

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

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

Når et bevis gennemføres efter dette princip, kalder man det et **induktionsbevis.** Punkt 1. kaldes **induktionsstarten**, og punkt 2. kaldes **induktionsskridtet**. I punkt 2. antager man altså $p(m)$, og konkluderer da $p(m+1)$. Derfor kaldes $p(m)$ for **induktionsantagelsen**.

Lad os gennemføre induktionsbeviset for Sætning 157:

Bevis. for Sætning 157: Lad $p(n)$ betegne følgende prædikat for $n \in \mathbb{N}$

$$p(n) : 1+3+5+\cdots+(2n-1)=n^2. \tag{6.10}$$

1. Induktionsstarten: Da $1=1^2$ er $p(1)$ sand.

2. Induktionsskridtet: Antag at $p(m)$ er sand, altså at

$$1 + 3 + 5 + \cdots + (2m - 1) = m^2. \tag{6.11}$$

Da viser følgende udregning at $p(m + 1)$ er sand:

$$(m + 1)^2 = m^2 + 2m + 1 = 1 + 3 + 5 + \cdots + (2m - 1) + (2m + 1)\,. \tag{6.12}$$

I denne udregning brugte vi induktionsantagelsen (6.11) i andet lighedstegn.

Af princippet om simpel induktion følger at $p(n)$ er sand for alle $n \in \mathbb{N}$, og dermed er sætningen bevist. ■

Lad os gennemføre et par andre eksempler på induktionsbeviser.

Sætning 159 *En $(n + 2)$-kant har vinkelsum lig $n \cdot 180°$.*

Bevis. Vi beviser sætningen ved induktion efter n:

1. Induktionsstarten: Det forudsættes bekendt, at vinkelsummen i en trekant er 180°. Et bevis findes i Euklids Elementer bog I.

2. Induktionsskridtet: Antag, at for en bestemt værdi af $m \in \mathbb{N}$ er vinkelsummen i enhver $(m+2)$-kant lig $m \cdot 180°$. Betragt en vilkårlig $((m + 1) + 2)$-kant, altså en $(m + 3)$-kant. Ved at tegne en passende valgt diagonal, kan vi dele denne $(m+3)$-kant i en trekant og en $(m+2)$-kant. Vinkelsummen i $(m+3)$-kanten er da summen af vinkelsummen i trekanten og vinkelsummen i $(m + 2)$-kanten, altså lig $180° + m \cdot 180° = (m + 1) \cdot 180°$. Hermed er påstanden vist for $n = (m + 1)$.

Ifølge princippet om simpel induktion er sætningen dermed bevist for alle $n \in \mathbb{N}$. ■

Sætning 160 *For ethvert $n \in \mathbb{N}$ går 6 op i $(n^3 - n)$.*

Bevis. Vi beviser sætningen ved induktion efter n.

1. *Induktionsstarten*: Sætningen er sand for $n = 1$, da $\left(1^3 - 1\right) = 0$ og $6 \mid 0$.

2. *Induktionsskridtet*: Antag at $6 \mid \left(m^3 - m\right)$ for en bestemt værdi af m. Vi skal vise at $6 \mid \left((m + 1)^3 - (m + 1)\right)$. Nu gælder at

$$(m + 1)^3 - (m + 1) = m^3 + 3m^2 + 3m + 1 - m - 1 \tag{6.13}$$
$$= (m^3 - m) + 3m\,(m + 1)\,. \tag{6.14}$$

Ifølge induktionsantagelsen går 6 op i det første led, og da et af tallene m og $m + 1$ er lige må $m\,(m + 1)$ indeholde en faktor 2, så 6 også går op i sidste led. Derfor må 6 gå op i summen. Vi har altså vist at $6 \mid \left((m + 1)^3 - (m + 1)\right)$.

Ifølge princippet om simpel induktion er sætningen dermed sand for alle $n \in \mathbb{N}$. ■

Ovenfor gav vi et løsagtigt osv. bevis for Sætning 99. Lad os nu give et ordentligt induktionsbevis.

Bevis. for Sætning 99. Vi antager altså at x, y er to ikke-negative reelle tal. Først vises pilene mod højre. Lad os vise (3.16) altså $x \leq y \Rightarrow x^n \leq y^n$. De andre går på samme vis. Vi fører beviset ved induktion efter n.

1. *Induktionsstarten*: Sætningen gælder klart for $n = 1$.

2. Induktionsskridtet: Antag at implikationen er sand for en bestemt værdi M altså at $x \leq y \Rightarrow x^m \leq y^m$. Vi skal da bevise at $x \leq y \Rightarrow x^{m+1} \leq y^{m+1}$. Antag derfor at $x \leq y$. Ifølge induktionsantagelsen er da $x^m \leq y^m$. Ved brug af (3.13) sluttes da at $x^{m+1} \leq y^{m+1}$.

Ifølge princippet om simpel induktion er sætningen dermed sand for alle $n \in \mathbb{N}$.

Lad os dernæst bevise pilene mod venstre. Igen lad os bevise (3.16) altså $x \leq y \Leftarrow x^n \leq y^n$. Det kan ved kontraposition omformes til udsagnet $x > y \Rightarrow x^n > y^n$. Men det følger af pilen til højre i (3.17). ■

Vi vil nu generalisere det fundamentale primtalslemma 141:

Sætning 161 ***Det fundamentale primtalslemma****: Hvis p er et primtal og $a_1, a_2, ..., a_n$ er hele tal, så gælder*

$$p \mid a_1 a_2 \cdots a_n \Rightarrow (p \mid a_1) \vee (p \mid a_2) \vee ... \vee (p \mid a_n)\,. \tag{6.15}$$

Bevis. Beviset føres ved induktion efter antal faktorer n.

1. *Induktionsstarten*: For $n = 1$ er sætningen triviel.

2. *Induktionsskridtet*: Antag at sætningen er sand for m faktorer, altså at hvis $a_1, a_2, ..., a_m$ er vilkårlige hele tal så gælder

$$p \mid a_1 a_2 \cdots a_m \Rightarrow (p \mid a_1) \vee (p \mid a_2) \vee ... \vee (p \mid a_m)\,. \tag{6.16}$$

   Vi skal da vise at sætningen er sand for $m + 1$ faktorer. Antag altså at $a_1, a_2, ..., a_{m+1}$ alle er hele tal. Vi skal da vise at

$$p \mid a_1 a_2 \cdots a_{m+1} \Rightarrow (p \mid a_1) \vee (p \mid a_2) \vee ... \vee (p \mid a_{m+1})\,. \tag{6.17}$$

   Antag derfor at $p \mid a_1 a_2 \cdots a_{m+1}$ eller hvad der er det samme

$$p \mid (a_1 a_2 \cdots a_m) a_{m+1}. \tag{6.18}$$

   Ifølge det fundamentale primtalslemma 141 ved vi så at $(p \mid (a_1 a_2 \cdots a_m)) \vee (p \mid a_{m+1})$. Ved nu at bruge induktionsantagelsen (6.16) konkluderes at $(p \mid a_1) \vee (p \mid a_2) \vee ... \vee (p \mid a_{m+1})$ hvorfor sætningen er sand for $m + 1$ faktorer.

Ifølge princippet om simpel induktion er sætningen dermed sand for alle $n \in \mathbb{N}$. ■

Nu vil vi vise entydighedsdelen af artimetikkens hovedsætning 145:

Sætning 162 *Hvis $p_1, p_2, \cdots, p_s$ og $q_1, q_2, \cdots, q_t$ alle er primtal og*

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t, \tag{6.19}$$

så er $s = t$, og efter en passende omordning af q'erne kan man opnå at $p_i = q_i$ for alle $i = 1, 2, \ldots, s$.

Bevis. Beviset føres ved induktion efter s.

1. *Induktionsstarten*:For $s = 1$ er venstresiden af 6.19 det ene primtal p_1. Hvert af faktorerne q_i på højresiden er derfor en faktor i p_1 og da p_i kun har trivielle faktorer og $q_i > 1$ slutter vi at $t = 1$ og at $p_1 = q_1$.

2. *Induktionsskridtet*: Antag at sætningen er sand når antallet af primtal på venstresiden er $s - 1$. Vi skal da vise sætningen når der er s primtal på venstresiden. Antag derfor at $p_1, p_2, \cdots, p_s$ og $q_1, q_2, \cdots, q_t$ alle er primtal og at (6.19) gælder.Primtallet p_s går da op i højresiden af (6.19). I følge den generelle version af det fundamentale primtalslemma 161 vil p_s derfor gå op i et af tallene $q_1, q_2, \cdots, q_t$, men da disse er primtal må det betyde at p_s er lig med et af disse primtal. Ved at omordne faktorerne på højresiden kan vi antage at $p_s = q_t$. Men så fås fra (6.19) at

   $$p_1 p_2 \cdots p_{s-1} = q_1 q_2 \cdots q_{t-1}. \tag{6.20}$$

   Men ifølge induktionsantagelsen betyder det at $s - 1 = t - 1$ og at efter omordning af q'erne kan man opnå at $p_i = q_i$ for alle $i = 1, 2, \ldots, s - 1$. Sammenholdt med at $p_s = q_t$ betyder det at $s = t$ og at $p_i = q_i$ for alle $i = 1, 2, \ldots, s$. Altså har vi vist at sætningen er sand når antallet af primtal på venstresiden er s.

Ifølge princippet om simpel induktion er sætningen dermed sand for alle $s \in \mathbb{N}$ ■

Bemærkning 163 *I ovenstående bevis var det af notationshensyn bedre at formulere induktionsskridtet på formen: For ethvert $s \in \mathbb{N}$, $s > 1$, kan man af $p(s-1)$ slutte $p(s)$.*

Induktionsskridtet kan også formuleres $p(m) \Rightarrow p(m+1)$. Her er det værd at huske, at dette udsagn *ikke* betyder: "*da* $p(m)$ er sand, er $p(m+1)$ også sand" men derimod "*hvis* $p(m)$ er sand, så er $p(m+1)$ også sand". Induktionsskridtet alene beviser altså ikke at $p(m+1)$ er sand. Først når Induktionsstarten (altså sandheden af $p(1)$) er bevist, kan man successivt bruge induktionsskridtet til at slutte: Da $p(1)$ er sand er $p(2)$ sand. Da $p(2)$ er sand er $p(3)$ sand, osv.

Hvis $q(n)$ betegner prædikatet

$$q(n) : 1 + 3 + 5 + \cdots + (2n - 1) = n^2 + 7 \tag{6.21}$$

(sammenlign med (6.10)), så kan vi bevise $q(m) \Rightarrow q(m+1)$, ganske som vi viste induktionsskridtet i beviset for Sætning 157. Men det viser intet om, hvorvidt $q(n)$ er sand for nogle eller alle $n \in \mathbb{N}$. Først hvis vi kunne vise, at $q(1)$ var sand, ville vi kunne slutte at q ville være sand for alle $n \in \mathbb{N}$. Men vi kan naturligvis ikke vise $q(1)$ (overvej), og faktisk er $q(n)$ falsk for alle $n \in \mathbb{N}$.

Moralen er at man skal huske at bevise induktionsstarten.

Man skal også være meget opmærksom på om induktionsskridtet virkelig gælder for *alle* $m \in \mathbb{N}$. Ellers kan man "bevise" "sætninger" som den følgende:

"**Sætning**": Alle kaniner har samme farve.

"**Bevis**": Det er klart, at der er et endeligt antal kaniner i verden. Sætningen er altså bevist, hvis vi for ethvert $n \in \mathbb{N}$ kan vise, at i en mængde af n kaniner, har alle kaninerne samme farve. Vi fører beviset herfor ved induktion efter n.

Induktionsstarten: I en mængde med kun 1 kanin, er det klart at alle kaniner har samme farve.

Induktionsskridtet: Antag nu at sætningen er sand for enhver mængde med m kaniner. Lad K være en mængde med $m+1$ kaniner. Tag en kanin k_1 væk fra K. Ifølge induktionsantagelsen har de resterende m kaniner samme farve (kald den F). Sæt nu k_1 tilbage, og borttag en anden kanin k_2, som jo har farven F. Da har de resterende kaniner (igen ifølge induktionsantagelsen) alle samme farve, og da alle kaninerne på nær måske k_1 har farven F, må alle kaninerne have farven F. Derfor har alle kaninerne i K samme farve.

Ifølge princippet om simpel induktion har kaninerne i enhver endelig mængde af kaniner samme farve.

Øvelse 164 *Erfaring og sund fornuft fortæller os at der må være noget galt med ovenstående bevis. Find fejlen.*

Bemærkning 165 *Det er klart (og kan let vises ud fra princippet om simpel induktion) at man kan begynde induktionen ved et andet tal end* 1. *Med andre ord, hvis vi beviser at* $p(k)$ *er sand og at induktionsskridtet er sandt for alle* $m \geq k$*, så kan vi slutte at* $p(n)$ *er sand for alle* $n \geq k$

6.2 Fuldstændig induktion

Nogle gange er det ikke nok at vide, at $p(m)$ er sand, når man skal vise at $p(m+1)$ er sand. Men det kan være, at man kan slutte $p(m+1)$, når man ved at $p(n)$ er sand for alle foregående naturlige tal, altså for $1, 2, 3, \cdots, m$. Og hvis man kan vise at $p(1)$ er sand, kan man skridtvis slutte som følger: Da $p(1)$ er sand er $p(2)$ sand; da $p(1)$ og $p(2)$ er sande, er $p(3)$ sand; da $p(1)$, $p(2)$ og $p(3)$ er sande er $p(4)$ sand; osv. Dermed kan vi bevise at $p(n)$ er sand for alle $n \in \mathbb{N}$. Vi formulerer denne bevisstrategi som en sætning:

Sætning 166 *(Princippet om **fuldstændig induktion**). Lad $p(x)$ være et prædikat, hvor den frie variabel x kan løbe over de naturlige tal $\mathbb{N}$.*

Såfremt $p(x)$ har følgende 2 egenskaber:

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

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

Bemærkning 167 *Også fuldstændig induktion kan begynde med et andet tal end 1. Det vil vi benytte i det næste bevis.*

Vi illustrerer brugen af fuldstændig induktion med eksistensdelen af aritmetikkens fundamentalsætning 145.

Sætning 168 *Ethvert naturligt tal $n > 1$ er et produkt af primtal.*

Bevis. Bemærk først, at når vi taler om "et produkt af primtal", så er det underforstået at dette produkt gerne må bestå af kun en faktor; med andre ord: Et primtal anses for i sig selv at være et "produkt af primtal".

Betragtes prædikatet $p(n)$ defineret ved:

$$(n \text{ er et produkt af primtal}), \tag{6.22}$$

hvor den frie variabel n tillades at løbe over de naturlige tal $\mathbb{N}$, så er vores opgave at vise, at $p(n)$ er sand for alle $n \geq 2$.

Vi viser dette ved fuldstændig induktion efter n startende ved 2.

Induktionsstarten: Da 2 er et primtal er $p(2)$ sand.

Induktionsskridtet: Vi lader nu $m \in \mathbb{N}$ være vilkårlig men ≥ 2, og antager at udsagnene $p(2), p(3), .., p(m)$ alle er sande. Vi skal da vise $p(m+1)$ altså at $m+1$ er et produkt af primtal. Vi splitter beviset herfor op i to tilfælde:

1. $m+1$ er et primtal: I så fald er $m+1$ ifølge ovenstående konvention et produkt af primtal, og vi er færdige.
2. $m+1$ er ikke et primtal: Da $m+1 > 1$, må $m+1$ i så fald være sammensat (se Definition 125). Der findes altså $a, b \in \mathbb{N}$ så:

   $$m + 1 = a \cdot b, \tag{6.23}$$

   og så $1 < a, b < m+1$. Da $a, b < m+1$, gælder $a, b \leq m$, så udsagnene $p(a)$ og $p(b)$ forekommer begge i listen $p(2)$, $p(3)$, ..., $p(m)$. På grund af induktionsantagelsen ved vi altså at både $p(a)$ og $p(b)$ er sande, dvs at såvel a og b er et produkt af primtal. Det samme gælder da om $m+1 = a \cdot b$.

   Altså er $p(m+1)$ sand.

Sætningen følger nu fra princippet om fuldstændig induktion. ■

6.3 Induktionsaksiomet

Vi har præsenteret induktionsprincipperne som oplagte følger af sund fornuft. Formelt er de følger af aksiomerne for de naturlige tal. Disse kan formuleres som følger:

Definition 169 ***Peano's aksiomssystem for de naturlige tal***[1]

De naturlige tal er en mængde $\mathbb{N}$ *udstyret med en efterfølgerfunktion* $S : \mathbb{N} \longrightarrow \mathbb{N}$*, hvorom det gælder:*

1. $1 \in \mathbb{N}$.
2. *For ethvert* $n \in \mathbb{N} : 1 \neq S(n)$.
3. *For ethvert* $m, n \in \mathbb{N} : m \neq n \Rightarrow S(m) \neq S(n)$.
4. ***Induktionsaksiomet****: Hvis det om en delmængde* $A \subseteq \mathbb{N}$ *gælder, at* $1 \in A$ *og* $m \in A \Rightarrow S(m) \in A$*, så gælder, at* $A = \mathbb{N}$.

Fra dette aksiomssystem kan man opbygge hele aritmetikken for naturlige tal. Det vil vi dog ikke gøre i denne bog. Vi vil nøjes med at bevise, at princippерne om simpel og fuldstændig induktion er konsekvenser af aksiomerne, specielt induktionsaksiomet.

Vi bemærker at operationen addition (+) indføres på en måde så at $S(n) = n + 1$ for alle $n \in \mathbb{N}$.

Intuitivt siger de første tre aksiomer, at man kan starte med 1 og successivt danne *nye* naturlige tal ved at tage efterfølgeren (altså lægge en til). Induktionsaksiomet siger, at alle naturlige tal kan nås på denne måde. Hvor de første aksiomer kan opfattes som generatorer af naturlige tal, er induktionsaksiomet et aksiom, der sikrer, at der ikke er flere naturlige tal, end de tal som genereres ved hjælp at de første tre aksiomer.

Intuitivt er det klart, at det netop er induktionsaksiomet, som får induktionsbeviser til at virke. Når vi ved at $p(1)$ og $p(n) \Rightarrow p(n+1)$, kan vi jo successivt slutte at p er sand for alle de successive efterfølgere af 1, og induktionsaksiomet siger at der ikke er andre naturlige tal end disse.

Lad os formalisere denne idé:

Bevis. (Sætning 158 om Simpel induktion): Lad $p(n)$ være et prædikat, hvor den frie variabel kan løbe over de naturlige tal. Antag endvidere at $p(1)$ er sand og at $p(m) \Rightarrow p(m+1)$. Vi skal da vise at $p(n)$ er sand for alle $n \in \mathbb{N}$.

Betragt sandhedsmængden for p altså

$$A = \{n \in \mathbb{N} \mid p(n) \text{ er sand}\}. \tag{6.24}$$

Da $p(1)$ er sand gælder, at $1 \in A$.

Da $p(m) \Rightarrow p(m+1)$, gælder det at $m \in A \Rightarrow S(m) \in A$.

[1] Opkaldt efter den Italienske matematiker Giuseppe Peano (1858-1932)

Mængden A opfylder altså forudsætningerne i induktionsaksiomet, hvorfor vi af aksiomet kan slutte at $A = \mathbb{N}$. Men det betyder at $p(n)$ er sand for alle $n \in \mathbb{N}$.

Dermed har vi vist princippet om simpel induktion. ■

For at se at induktionsaksiomet er nødvendigt for at kunne bruge princippet om simpel induktion, kan vi betragte følgende eksempel:

Eksempel 170 *Lad*

$$A = \left\{ x \in \mathbb{R} \mid x = 2 - \frac{1}{n} \text{ for et } n \in \mathbb{N} \right\} \tag{6.25}$$

og

$$B = \left\{ x \in \mathbb{R} \mid x = 3 - \frac{1}{n} \text{ for et } n \in \mathbb{N} \right\} \tag{6.26}$$

og definer $C = A \cup B$. Definer efterfølgerfunktionen $S : C \longrightarrow C$ ved

$$S(2 - \frac{1}{n}) = 2 - \frac{1}{n+1}, \tag{6.27}$$

$$S(3 - \frac{1}{n}) = 3 - \frac{1}{n+1} \tag{6.28}$$

for alle $n \in \mathbb{N}$. Da opfylder C med denne efterfølgerfunktion de tre første aksiomer i Peanos aksiomssystem men ikke induktionsaksiomet. Der gælder jo at $A \subseteq C$ og $1 \in A$ og $x \in A \Rightarrow S(x) \in A$, men $A \neq C$.

Hvis $p(x)$ er et prædikat, hvor den frie variabel kan løbe over C og vi ved at $p(2 - \frac{1}{1})$ er sand, og at $p(x) \Rightarrow p(S(x))$ så er det intuitivt klart at $p(x)$ er sand for alle $x \in A$, men det er også klart, at man ikke kan slutte at $p(x)$ er sand for $x \in B$. Vi kan jo ikke ved successivt at tage efterfølgeren, nå fra $2 - \frac{1}{1}$ til et element i B.

Eksemplet kan gives en anden iklædning:

Betragt mængden $\mathbb{N} = \{1, 2, 3, ..., n, ...\}$ og mængden $\mathbb{N}' = \{1', 2', 3', ..., n', ...\}$ og sæt dem efter hinanden: $\mathbb{N} \cup \mathbb{N}' = \{1, 2, 3, ..., n, ..., 1', 2', 3', ..., n', ...\}$. Lad efterfølgerfunktionen være defineret på $\mathbb{N} \cup \mathbb{N}'$ ligesom den er på hver del for sig. Da opfylder $\mathbb{N} \cup \mathbb{N}'$ Peanos tre første aksiomer men ikke induktionsaksiomet.

Vi vil dernæst bevise princippet om fuldstændig induktion ud fra princippet om simpel induktion:

Bevis. (Sætning 166 om Fuldstændig induktion): Lad $p(n)$ være et prædikat, hvor den frie variabel kan løbe over de naturlige tal. Antag endvidere at $p(1)$ er sand og at $p(1) \wedge p(2) \wedge \ldots \wedge p(m) \Rightarrow p(m+1)$. Vi skal da vise at $p(n)$ er sand for alle $n \in \mathbb{N}$.

Betragt hertil følgende prædikat i den frie variabel n :

$$q(n) : (\forall k \in \mathbb{N} : k \leq n \Rightarrow p(k)). \tag{6.29}$$

Den frie variabel n kan her antage værdier i $\mathbb{N}$.[2]

[2] Vi kan også skrive $q(n)$ som $p(1) \wedge p(2) \wedge \ldots \wedge p(n)$.

Vi påstår nu, at vi kan vise $q(n)$ for alle $n \in \mathbb{N}$ via simpel induktion. Er dette gjort, følger $p(n)$ for alle $n \in \mathbb{N}$: For hvis vi har $q(n)$ for et $n \in \mathbb{N}$, er implikationen $k \leq n \Rightarrow p(k)$ sand for ethvert $k \in \mathbb{N}$. Idet $n \leq n$ kan vi derfor slutte $p(n)$.

Induktionsstarten: $q(1)$ er udsagnet: $\forall k \in \mathbb{N} : k \leq 1 \Rightarrow p(k)$. Dette udsagn er sandt, thi det eneste naturlige tal med $k \leq 1$ er tallet 1, og vi har antaget at $p(1)$ er sand.

Induktionsskridtet: Antag nu at $q(m)$ er sand for et $m \in \mathbb{N}$. Da udsagnet $k \leq m$ er sandt for $k = 1, 2, \ldots, m$, følger derfor $p(k)$ for $k = 1, 2, \ldots, m$. På grund af vores antagelse om $p(x)$, kan vi heraf slutte $p(m+1)$. Men da er implikationen

$$k \leq m + 1 \Rightarrow p(k) \tag{6.30}$$

sand, d.v.s. vi har sluttet $q(m+1)$.

Fra princippet om simpel induktion kan vi nu slutte at $q(n)$ er sand for alle $n \in \mathbb{N}$. ■

Man kan omvendt vise, at princippet om simpel induktion følger af princippet om fuldstændig induktion. Beviset overlades til læseren. De to principper er altså ækvivalente.

Bemærkning 171 *Vær opmærksom på, at det ikke er alle sætninger om naturlige tal, som mest hensigtsmæssigt bevises ved et induktionsbevis. Mange sætninger bevises som sædvanlige universelle sætninger, jvf. beviset i starten af dette afsnit for at* $(n+1)^2 = n^2 + 2n + 1$. *Det kan kun betale sig at bruge et induktionsbevis, hvis beviset for* $p(m+1)$ *simplificeres ved at antage, at* $p(m)$ *(eller* $p(1) \wedge p(2) \wedge \ldots \wedge p(m)$*) er sand. Hvis du opdager, at du slet ikke har brugt induktionsantagelsen i beviset for* $p(m+1)$*, så har du jo et universelt bevis for* $p(m+1)$.

Bemærkning 172 *I filosofisk og dagligdags tale betyder induktion noget andet end i matematik. Induktion i filosofisk forstand betyder en slutning fra det specielle til det generelle, som når man ud fra enkeltobservationer slutter sig til en generel lovmæssighed. For eksempel har jeg observeret, at solen står op hver dag i mit liv, og jeg slutter derfra den generelle lovmæssighed, at solen står op hver dag. Ligeså har man observeret at de kendte planeter bevæger sig om solen i ellipser, og slutter derfra, at alle planeter (også de eventuelt uopdagede) vil bevæge sig om solen i ellipser. Disse slutninger er induktive. I modsætning hertil står deduktioner, som er slutninger fra det generelle til det specielle. For eksempel, når man fra gravitationsloven udleder, at planeter bevæger sig i ellipser, er der tale om en deduktion.*

Naturvidenskaber benytter induktion, hvorimod matematik kun bruger deduktive slutninger. Selv matematisk induktion er en type deduktion, i ordets filosofiske betydning.

6.4 Rekursion

Hvis $a \in \mathbb{R}$, defineres a^n for ethvert $n \in \mathbb{N}$ ved følgende to regler:

1. $a^1 = a$,
2. $\forall n \in \mathbb{N} : a^{n+1} = a \cdot a^n$.

Ideen i definitionen er at vi starter med at definere a^1 og derfra successivt (rekursivt) bestemmer a^2, a^3, osv. ud fra den foregående værdi, ved hjælp af den anden regel. Man kalder en sådan definition for en rekursiv definition.

Ved første øjekast kan det synes ret oplagt, at man på denne måde kan definere a^n for alle $n \in \mathbb{N}$. Men ligesom i tilfældet med induktionsprincippet bør man bevise, at vi har formuleret en holdbar definition. Det bygger faktisk på følgende sætning af Dedekind (1888):

Sætning 173 ***Rekursionssætningen****: Lad der være givet en mængde A, et element $a \in A$, og en afbildning $f : A \longrightarrow A$.*

Da findes der netop en afbildning $\phi : \mathbb{N} \longrightarrow A$ med følgende egenskaber:

1. $\phi(1) = a$,
2. $\forall n \in \mathbb{N} : \phi(n+1) = f(\phi(n))$.

Det intuitive indhold i sætningen er at vi successivt definerer

$$\phi(1) := a \tag{6.31}$$
$$\phi(2) := f(\phi(1)) = f(a) \tag{6.32}$$
$$\phi(3) := f(\phi(2)) = f(f(a)) \tag{6.33}$$
$$\text{osv.} \tag{6.34}$$

Vi skal ikke gennemgå det subtile formelle bevis for denne sætning, blot nævne at det bygger på induktionsaksiomet.

Lad os se, hvordan rekursionssætningen kan begrunde den ovennævnte definition af a^n:

Lad $A = \mathbb{R}$ og $a \in \mathbb{R}$ vilkårlig, og $f(x) := a \cdot x$. Rekursionssætningen siger da at der findes netop en afbildning $\phi : \mathbb{N} \longrightarrow \mathbb{R}$, så

1. $\phi(1) = a$,
2. $\forall n \in \mathbb{N} : \phi(n+1) = a \cdot \phi(n)$.

Man definerer da $a^n = \phi(n)$.

Ofte vil man i en rekursiv definition af en funktion benytte andre end den umiddelbare forgænger ved definitionen af $\phi(n+1)$. Man kan formulere og bevise en generalisation af rekursionssætningen, der siger at dette er tilladt og entydigt bestemt. Vi vil dog ikke formulere denne generalisering, da den er af noget teknisk natur.

Definition 155 af Fibonaccitallene er et eksempel på en sådan mere generel rekursiv definition.

Rekursive definitioner forekommer gang på gang i matematikken, specielt i kombinatorik og talteori.

6.5 Opgaver

1. Brug et induktionsbevis til at bevise, at for ethvert $n \in \mathbb{N}$ gælder:

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}. \tag{6.35}$$

2. Brug fuldstændig induktion til at bevise, at ethvert naturligt tal er en sum af forskellige potenser af to. (Overvej, hvorfor argumentet fejler, hvis du prøver at vise at ethvert naturligt tal kan skrives som en sum af forskellige potenser af tre).

3. Giv et induktionsbevis for at 4 går op i $5^n - 1$ for alle $n \in \mathbb{N}$.

4. Gæt en formel for

$$a_n = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)}, \tag{6.36}$$

og bevis din formodning.

5. Bevis at følgende formler er korrekte for alle $n \in \mathbb{N}$:

$$2 + 5 + 8 + \cdots + (3n - 1) = \frac{n(3n+1)}{2} \tag{6.37}$$

$$1 + 5 + 9 + \cdots + (4n - 3) = n(2n - 1) \tag{6.38}$$

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2. \tag{6.39}$$

6. Lad $f(x) = \ln x$. Udregn de første afledede af f, og opstil en formodning om en formel for $\frac{d^n f}{dx^n}$. Bevis din formodning ved induktion.

7. Bevis, at enhver ikke tom delmængde af de naturlige tal har et mindste element (velordningsprincippet). Vink: Antag at $A \subseteq \mathbb{N}$ og at A ikke har et mindste element. Brug da induktionsaksiomet på $\complement A$ til at vise, at A er tom.

8. Lad $x \neq 1$ være et reelt tal. Definer rekursivt betydningen af

$$1 + x + x^2 + \cdots + x^n, \tag{6.40}$$

og bevis ved induktion at

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}. \tag{6.41}$$

9. Lad $k \in \mathbb{N}$ og lad $A \subseteq \mathbb{N}$, og antag at det gælder at
(a) $k \in A$
(b) $m \in A \Rightarrow (m+1) \in A$.
Vis at $\{n \in \mathbb{N} \mid k \leq n\} \subseteq A$.

10. Formuler en sætning, svarende til princippet om simpel induktion, men hvor induktionen ikke starter ved 1, men ved et vilkårligt $k \in \mathbb{N}$. Brug resultatet i opgave 9 til at bevise din sætning.

11. Betragt polynomier

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \tag{6.42}$$

med rationale koefficienter $a_0, \ldots a_n$. Hvis $a_n \neq 0$, så kaldes n for f's grad og betegnes med $\deg f$. Således er $\deg f$ kun defineret, hvis $f \neq 0$.

Et polynomium f af grad ≥ 1 kaldes reducibelt, hvis der findes en spaltning $f = g \cdot h$, hvor g, h er polynomier med grader strengt mindre end $\deg f$. Er f ikke reducibel, kaldes f irreducibel.

Vis ved fuldstændig induktion, at ethvert polynomium er et produkt af irreducible polynomier

Kapitel 7

Mængdelære

7.1 Hvad er en mængde?

En mængde er det mest basale begreb i matematikken. Man definerer alle andre matematiske begreber inden for mængdelæren. Men hvordan definerer man da mængder? Man definerer dem ud fra en række aksiomer. Det foretrukne aksiomssystem kaldes Zermelo-Fraenkels aksiomssystem eller ZFC hvor C står for det omdiskuterede udvalgsaksiom (axiom of Choice). I dette kursus vil vi nøjes med en mere naiv tilgang til mængder, idet vi betragter dem som samlinger af ting, hvor "ting" skal tages i vid betydning. Tingene, som udgør mængden kaldes dens *elementer.*

Man angiver ofte mængder med store bogstaver og elementerne med små bogstaver. Man kan angive en mængde ved at opskrive en liste af dens elementer i en tuborg-parentes. For eksempel betyder $M = \{1, 2, 7\}$ mængden bestående af de tre tal 1, 2 og 7.. Elementernes rækkefølge er ligegyldig. Altså $\{1, 2, 7\} = \{2, 7, 1\}$. Mængder kan have andre mængder som elementer. For eksempel har mængden $\{4, \{2, 3\}\}$ to elementer nemlig 4 og $\{2, 3\}$, medens tallene 2 og 3 *ikke* er element i mængden $\{4, \{2, 3\}\}$. At x er element i M skrives $x \in M$ og siges ofte: "x ligger i M". Altså har vi $4 \in \{4, \{2, 3\}\}$, og $\{2, 3\} \in \{4, \{2, 3\}\}$, hvorimod $2 \notin \{4, \{2, 3\}\}$. Her betyder $\notin$ naturligvis "ikke element i" altså: $x \notin M \Leftrightarrow \neg(x \in M)$.

En mængde er entydigt karakteriseret ved sine elementer. Det betyder at to mængder er ens, hvis de har samme elementer: Eller skrevet formelt:

Definition 174 *Lad A og B være mængder. Da er $A = B$ hvis*

$$x \in A \Leftrightarrow x \in B. \tag{7.1}$$

Mængder kan godt have ét element f.eks. $\{1\}$. Det er dog vigtigt at sondre mellem tallet 1 og mængden $\{1\}$, som har det ene element 1. Ja, man tillader endog at en mængde slet ingen elementer har. Eksistensen af en sådan mængde er et aksiom. Vi vil nu bevise entydigheden:

Sætning 175 *Der er præcist én mængde uden nogen elementer.*

Bevis. Lad A og B være to mængder uden elementer. Vi skal da vise at $A = B$. Ifølge Definition 174 skal vi altså vise at

$$x \in A \Leftrightarrow x \in B. \tag{7.2}$$

Men dette udsagn er sandt, da både $x \in A$ og $x \in B$ er falsk for alle x (jvf. Definition 176). ■

Bemærk at dette bevis følger den strategi for entydighedsbeviser, som blev beskrevet i forbindelse med formel (2.30).

Definition 176 *Den entydige mængde uden elementer kaldes den* ***tomme mængde*** *og betegnes med* $\emptyset$.

Bemærkning 177 *Der er forskel på* $\emptyset$ *og* $\{\emptyset\}$. *Mængden* $\emptyset$ *er den tomme mængde, og har ingen elementer. Mængden* $\{\emptyset\}$ *er derimod mængden af den tomme mængde. Den har ét element, nemlig* $\emptyset$.

Øvelse 178 *Hvilke elementer har mængderne:* $\{\emptyset, \{\emptyset\}\}$ *og* $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$*?*

Når man opgiver en mængde ved at angive alle dens elementer i en tuborgparentes, siger man at mængden er givet på elementform. Denne form kan strengt taget kun bruges til at angive endelige mængder, og i praksis kun mængder med få elementer; men man bruger den også nogle gange til at betegne mængder med uendeligt mange elementer. For eksempel kan man skrive mængden af lige tal på formen $\{2, 4, 6, ...\}$, medens $\{2, 4, 6, ...100\}$ betegner de lige tal mindre eller lig 100. Det er klart at denne måde at betegne mængder kun kan bruges, når der ikke kan opstå tvivl om hvad "..." står for.

Notation 179 *Følgende notation bruges om forskellige talmængder:*

$\mathbb{N}$ *betegner mængden af de naturlige tal altså mængden* $\{1, 2, 3, ...\}$.

$\mathbb{Z}$ *betegner mængden af de hele tal altså mængden* $\{...-3, -2, -1, 0, 1, 2, 3, ...\}$.

$\mathbb{Q}$ *betegner mængden af rationale tal altså mængden af brøker* $\frac{a}{b}$ *hvor* $a, b \in \mathbb{Z}$ *og* $b \neq 0$.

$\mathbb{R}$ *betegner mængden af reelle tal.*

$\mathbb{C}$ *betegner mængden af komplekse tal*

$\mathbb{Z}_+$, $\mathbb{Q}_+$, $\mathbb{R}_+$ *betegner henholdsvist de positive hele tal, de positive rationale tal og de positive reelle tal.*

$\mathbb{Z}_-$, $\mathbb{Q}_-$, $\mathbb{R}_-$ *betegner henholdsvist de negative hele tal, de negative rationale tal og de negative reelle tal*

Sandhedsmængder. Hvis $p(x)$ er et prædikat om elementerne i en mængde M, kan man betragte mængden bestående af de af M's elementer, som gør prædikatet sandt. Denne mængde kaldes p's sandhedsmængde og betegnes symbolsk ved

$$\{x \in M \mid p(x)\} \text{ eller } \{x \in M : p(x)\} \tag{7.3}$$

Man siger "mængden af de x i M for hvilke $p(x)$".

Bemærkning 180 *Notationen 7.3 kaldes en mængdebygger. I engelsksproget litteratur skrives normalt et kolon i stedet for den lodrette streg i mængdebyggeren:* $\{x \in M : p(x)\}$.

Eksempel 181 $\mathbb{Z}_+ = \{x \in \mathbb{Z} \mid x > 0\}$

Eksempel 182 $\mathbb{Q} = \{x \in \mathbb{R} \mid \exists a, b \in \mathbb{Z} : (b \neq 0) \wedge \left(x = \frac{a}{b}\right)\} = \{\frac{a}{b} \mid (a, b \in \mathbb{Z}) \wedge (b \neq 0)\}$

Hvis det er helt klart hvilken grundmængde den frie variabel x tænkes at løbe over, tillader man sig at skrive $\{x \mid p(x)\}$. Men man skal være forsigtig med denne skrivemåde. Mængdelærens aksiomer tillader ikke, at man danner mængden af al ting, som opfylder et bestemt prædikat. Vi skal senere se hvorfor.

Notation 183 ***Intervaller.*** *Man bruger følgende skrivemåde for intervaller af reelle tal (her er* $a, b \in \mathbb{R}$*):*

$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ kaldes det lukkede interval fra a til b.
$]a, b[= \{x \in \mathbb{R} \mid a < x < b\}$ kaldes det åbne interval fra a til b.
$[a, b[= \{x \in \mathbb{R} \mid a \leq x < b\}$ og $]a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$ kaldes halvåbne intervaller.
$[a, \infty[= \{x \in \mathbb{R} \mid a \leq x\}$ og $]-\infty, a] = \{x \in \mathbb{R} \mid x \leq a\}$ kaldes lukkede.
$]a, \infty[= \{x \in \mathbb{R} \mid a < x\}$ og $]-\infty, a[= \{x \in \mathbb{R} \mid x < a\}$ kaldes åbne.
I engelsksproget literatur er det mest almindeligt at betegne åbne intervaller med runde parenteser. F.eks. betegner (a, b) det åbne interval, som vi ovenfor har betegnet ved $]a, b[$.

7.2 Delmængder

Definition 184 *En mængde* A *kaldes en* ***delmængde*** *af en mængde* B *(eller at* A *er indeholdt i* B*), hvis alle elementerne i* A *også ligger i* B*. I så fald siger man også at* A *er indeholdt i* B*, eller at* B *indeholder* A*. Man skriver da* $A \subseteq B$ *eller* $B \supseteq A$.

Med andre ord $A \subseteq B$*, hvis*

$$x \in A \Rightarrow x \in B. \tag{7.4}$$

Bevisstrategi. Når man skal vise at $A \subseteq B$, skal man altså vise at et vilkårligt element i A ligger i B. Beviset begynder derfor med ordene: "Lad $x \in A$" og fortsætter med at vise, at vi ud fra $x \in A$ kan slutte at $x \in B$. Antag nu at mængderne er givet som sandhedsmængder for to prædikater: $A = \{x \in M \mid p(x)\}$ og $B = \{x \in M \mid q(x)\}$. Beviset for $A \subseteq B$ vil da forløbe således: "Lad $x \in A$. Så vil $p(x)$ være opfyldt" så argumenteres for at $p(x) \Rightarrow q(x)$ hvorefter der sluttes: "Altså er $q(x)$ sand hvorfor $x \in B$".

Eksempel 185 *Vis, at* $\{x \in \mathbb{R} \mid x^2 < 2\} \subseteq \{x \in \mathbb{R} \mid x < 5\}$.

Bevis. Antag at $x \in \{x \in \mathbb{R} \mid x^2 < 2\}$, altså at $x^2 < 2$. Da gælder, at $x^2 < 4$, hvorfor $-2 < x < 2$. Heraf sluttes, at $x < 5$, altså at $x \in \{x \in \mathbb{R} \mid x < 5\}$. ■

Vi kan præcisere ovenstående bevisstrategi til en sætning:

Sætning 186 *Udsagnet $p(x) \Rightarrow q(x)$ er ensbetydende med udsagnet $\{x \in M \mid p(x)\} \subseteq \{x \in M \mid q(x)\}$*

Bevis. .

$$\{x \in M \mid p(x)\} \subseteq \{x \in M \mid q(x)\} \tag{7.5}$$
$$\Updownarrow \tag{7.6}$$
$$x \in \{x \in M \mid p(x)\} \Rightarrow x \in \{x \in M \mid q(x)\} \tag{7.7}$$
$$\Updownarrow \tag{7.8}$$
$$p(x) \Rightarrow q(x) \tag{7.9}$$

■

Sætning 187 *Den tomme mængde er en delmængde af enhver mængde. Altså hvis A er en mængde gælder*

$$\emptyset \subseteq A \tag{7.10}$$

Bevis. Vi skal vise at

$$x \in \emptyset \Rightarrow x \in A. \tag{7.11}$$

Men udsagnet $x \in \emptyset$ er falsk for alle x, hvorfor udsagnet $x \in \emptyset \Rightarrow x \in A$ er sandt (se bemærkning definition 11 og bemærkning 27). ■

Bemærk at når $A \subseteq B$ kan A og B godt være ens. Hvis vi vil udelukke det, skriver vi $A \subset B$:

Definition 188 *A kaldes en **ægte delmængde** af B hvis $A \subseteq B$ og $A \neq B$. Vi skriver da $A \subset B$. (I andre bøger bruges $\subset$ som symbol for det vi her skriver som $\subseteq$).*

Sætning 189 *Lad A og B være mængder. Da er $A = B$ hvis og kun hvis $(A \subseteq B) \wedge (B \subseteq A)$.*

Bevis. Ifølge Definition 174 og 184 og Eksenpel 15 gælder følgende biimplikationer:

$$A = B \tag{7.12}$$
$$\Updownarrow \tag{7.13}$$
$$x \in A \Leftrightarrow x \in B \tag{7.14}$$
$$\Updownarrow \tag{7.15}$$
$$(x \in A \Rightarrow x \in B) \wedge (x \in A \Leftarrow x \in B) \tag{7.16}$$
$$\Updownarrow \tag{7.17}$$
$$(A \subseteq B) \wedge (B \subseteq A) \tag{7.18}$$

■

Bevisstrategi. Når man skal vise at to mængder A og B er lig med hinanden beviser man ofte først $A \subseteq B$ og dernæst $B \subseteq A$.

Sætning 190 *Mængden af punkter i planen, som ligger lige langt fra to givne punkter A og B, er midtnormalen til linjestykket AB.*[1]

Bevis. Vi viser først at mængden af punkter i planen, som ligger lige langt fra A og B, er indeholdt i midtnormalen. Lad derfor C være et punkt, som ligger lige langt fra A og B. Tegn trekant ABC. Halver linjestykket AB i D og tegn CD. Nu er siderne i ΔCAD og ΔCBD parvist lige store, hvorfor de to trekanter er kongruente (Euklid I.8). Men så er $\angle CDA = \angle CDB$, hvorfor de ifølge definitionen på en ret vinkel (Euklid Def. 10) må være rette. Men det betyder at linjen CD er midtnormalen til AB. Altså ligger C på denne midtnormal.

Dernæst viser vi omvendt, at ethvert punkt på AB's midtnormal ligger lige langt fra A og B. Antag altså at C ligger på AB's midtnormal, som skærer AB i midtpunktet, som vi kalder D. Tegn trekant ABC. Ifølge Euklid I.4 er ΔCDA kongruent med ΔCDB, thi $\angle CDA = \angle CDB$, og de to hosliggende sider er også parvist lige store. Men så er $CA = CB$, så C ligger lige langt fra A og B. ■

Bemærkning 191 *I geometri kaldes mængden af punkter, som opfylder en bestemt egenskab, for "det geometriske sted for de punkter, der opfylder egenskaben". Vi har altså bevist at det geometriske sted for de punkter i planen, som ligger lige langt fra to punkter, er midtnormalen til linjestykket mellem punkterne.*

Sætning 192 *Lad A, B og C være mængder. Hvis $A \subseteq B$ og $B \subseteq C$, så gælder $A \subseteq C$.*

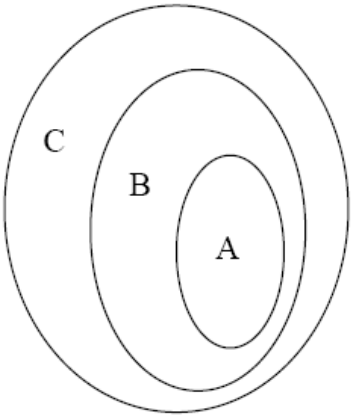
Bevis. Antag at $A \subseteq B$ og $B \subseteq C$. Vi skal vise, at $A \subseteq C$, altså at $x \in A \Rightarrow x \in C$. Lad derfor $x \in A$. Vi skal da vise at $x \in C$.

Da $A \subseteq B$, kan vi af $x \in A$ slutte, at $x \in B$, og da $B \subseteq C$, slutter vi videre at $x \in C$. ■

Notation 193 *Hvis $A \subseteq B$ og $B \subseteq C$ tillader man sig derfor at skrive $A \subseteq B \subseteq C$. På lignende måde kan man skrive $A \subset B \subseteq C$, $A \subseteq B \subset C$ og $A \subset B \subset C$. Betydningen heraf er klar. Derimod skriver man ikke strenge hvor inklusionstegnene vender hver sin vej (f.eks. $A \supseteq B \subseteq C$).*

Venn-diagrammer. Man kan illustrere mængder i et såkaldt Venn-diagram. Figur 7.1 illustrerer situationen $A \subseteq B \subseteq C$. Punkterne inden for bollerne forestiller elementerne i mængden. Sætning 192 kan nærmest aflæses ud af figuren. En sådan figurinspektion kan dog formelt ikke gøre det ud for et bevis, men den kan give gode ideer til hvilke formodninger, man skal opstille. Venndiagrammer giver også en god intuition om situationen, så det anbefales, at du så vidt muligt laver diagrammer, der illustrerer de følgende sætninger om mængder.

[1] Midtnormalen til et linjestykke er en ret linje, som står vinkelret på midten af linjestykket.



Figur 7.1: Venn-diagram, som illustrerer: $A \subseteq B \subseteq C$

7.3 Fællesmængde og foreningsmængde

Definition 194 *Lad A og B være to mængder. Mængden af de elementer, som ligger i både A og B kaldes for* ***fællesmængden*** *for A og B. Den betegnes $A \cap B$. Med andre ord*

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\} \tag{7.19}$$

eller

$$x \in A \cap B \Leftrightarrow (x \in A) \wedge (x \in B) \tag{7.20}$$

Bevisstrategi: Når man skal vise at et element ligger i fællesmængden for to mængder skal man altså vise at det ligger i begge de to mængder.

Eksempel 195 $\{a, b, c, d, e, f\} \cap \{d, e, f, g, h, i\} = \{d, e, f\}$.

Eksempel 196 $\mathbb{Z} \cap \mathbb{R}_+ = \mathbb{Z}_+$.

Eksempel 197 *Lad AB være et linjestykke med midtpunkt D, og lad DC betegne dens midtnormal. Da er $AB \cap DC = D$*

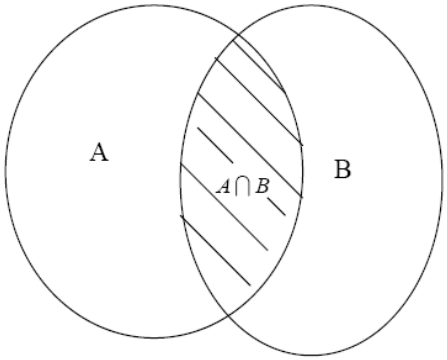
På Venn-diagrammet i Figur 7.2 er fællesmængden for A og B skraveret

Sætning 198 *Lad A, B og C være mængder. Da gælder*

$$A \cap B = B \cap A \tag{7.21}$$

og

$$(A \cap B) \cap C = A \cap (B \cap C). \tag{7.22}$$



Figur 7.2: Fællesmængden $A \cap B$

Bevis. Følger af de tilsvarende logiske regler for " $\wedge$ " ■

På grund af (7.22) giver det ikke anledning til misforståelser at skrive $A \cap B \cap C$ og tilsvarende for flere mængder.

Sætning 199 *Lad A og B være mængder. Da gælder:*

$$A \cap A = A, \qquad A \cap B \subseteq A, \text{ og } A \cap \emptyset = \emptyset \tag{7.23}$$

Definition 200 *Lad A og B være mængder. Hvis $A \cap B = \emptyset$, siges A og B at være* ***disjunkte.***

Definition 201 *Lad A og B være to mængder. Mængden af elementer, som ligger i enten A eller B kaldes* ***foreningsmængden*** *af (eller for) A og B. Den betegnes med $A \cup B$. Med andre ord*

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\} \tag{7.24}$$

eller

$$x \in A \cup B \Leftrightarrow (x \in A) \vee (x \in B) \tag{7.25}$$

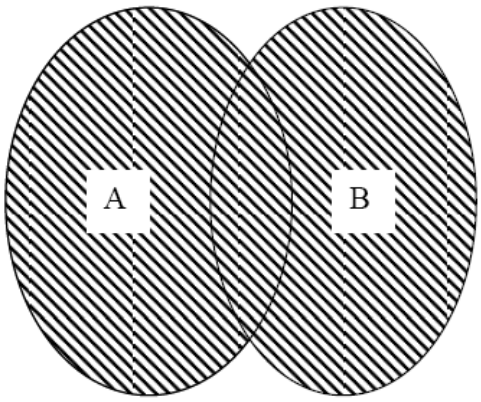
Bevisstrategi: Når man skal vise at et element ligger i foreningsmængden af to mængder skal man altså vise at det ligger i mindst en af de to mængder.

Eksempel 202 $\{a, b, c, d, e, f\} \cup \{d, e, f, g, h, i\} = \{a, b, c, d, e, f, g, h, i\}$.

Eksempel 203 $(\mathbb{Z}_+ \cup \mathbb{Z}_-) \cup \{0\} = \mathbb{Z}$

På Venn-diagrammet i Figur 7.3 repræsenterer hele det skraverede område foreningsmængden af A og B.

Bemærkning 204 *I definitionen af fællesmængden og foreningsmængden har vi misbrugt mængdebyggernotationen, idet vi ikke har angivet en grundmængde,*



Figur 7.3: Foreningsmængden $A \cup B$

som x skal tilhøre. I tilfældet med fællesmængden, er det uproblematisk, idet man kan bruge en af de to mængder, som grundmængde, fx: $A \cap B = \{x \in A \mid (x \in A) \wedge (x \in B)\}$. I tilfældet med foreningsmængden skal vi som grundmængde bruge en mængde C som indeholder både A og B. At en sådan mængde findes sikres af et af mængdelærens aksiomer.

Sætning 205 *Lad A, B og C være mængder. Da gælder*

$$A \cup B = B \cup A \tag{7.26}$$

og

$$(A \cup B) \cup C = A \cup (B \cup C). \tag{7.27}$$

Bevis. Følger af de tilsvarende logiske regler for " $\vee$ " . ■

På grund af (7.27) giver det ikke anledning til misforståelser at skrive $A \cup B \cup C$ og tilsvarende for flere mængder.

Sætning 206 *Lad A og B være mængder. Da gælder:*

$$A \cup A = A, \quad A \cup B \supseteq A, \text{ og } A \cup \emptyset = A \tag{7.28}$$

Man kan endog danne foreningsmængde og fællesmængde af en hel (eventuelt uendelig) familie af mængder.

7.3.1 Familier af mængder.

Eksempel 207 *Betragt intervallerne $I_1 = [0, 1]$, $I_2 = \left[0, \frac{1}{2}\right]$, $I_3 = \left[0, \frac{1}{3}\right]$, ..., $I_n = \left[0, \frac{1}{n}\right]$,.... De udgør en familie af delmængder af $\mathbb{R}$. De er indiceret ved de naturlige tal, i den forstand, at der til hvert naturligt tal svarer netop et af intervallerne (til n svarer I_n).*

Eksempel 208 *Betragt enhedscirklerne i planen med centrum i et punkt på x-aksen. Lad C_t betegne den enhedscirkel, hvis centrum har koordinaterne $(t, 0)$. Da udgør alle C_t 'erne en familie af cirkler indiceret ved det reelle index t.*

Definition 209 *Mere generelt, hvis Λ er en mængde (af indices), og der til ethvert index $\alpha \in \Lambda$ svarer en mængde A_α, da siger vi at A_α'erne udgør en familie af mængder, der er indiceret ved Λ. Familien betegnes ved $\{A_\alpha\}_{\alpha\in\Lambda}$.*

Definition 210 *Lad $\{A_\alpha\}_{\alpha\in\Lambda}$ være en familie af mængder, hvor Λ er en ikke-tom indexmængde. Fællesmængden for alle familiens mængder ("fællesmængden for A_α'erne for α i Λ") betegnes med $\bigcap_{\alpha\in\Lambda} A_\alpha$ og defineres formelt ved:*

$$\bigcap_{\alpha\in\Lambda} A_\alpha = \{x \mid \forall\alpha \in \Lambda : x \in A_\alpha\}. \tag{7.29}$$

Med andre ord $x \in \bigcap_{\alpha\in\Lambda} A_\alpha$, hvis $x \in A_\alpha$ for alle $\alpha \in \Lambda$. I tilfælde af at indexmængden er $\{1, 2, 3, ..., m\}$ eller $\mathbb{N}$, skriver man også $\bigcap_{n=1}^{m}$ og $\bigcap_{n=1}^{\infty}$.

Bemærkning 211 *Ved negation af definitionen ses at $x \notin \bigcap_{\alpha\in\Lambda} A_\alpha$, hvis og kun hvis $\exists\alpha \in \Lambda : x \notin A_\alpha$*

Eksempel 212 *Betragt familien af intervaller $\{I_n\}_{n\in\mathbb{N}}$ defineret i eksempel 207. Vi vil vise at $\bigcap_{n\in\mathbb{N}} I_n = \{0\}$.*

Bevis. $\supseteq$: Det er let at vise at $\bigcap_{n\in\mathbb{N}} I_n \supseteq \{0\}$. Vi skal vise at ethvert element i $\{0\}$ ligger i $\bigcap_{n\in\mathbb{N}} I_n$ altså i I_n for alle $n \in \mathbb{N}$. Men det eneste element i $\{0\}$ er 0, og $0 \in I_n = \left[0, \frac{1}{n}\right]$ for alle $n \in \mathbb{N}$.

$\subseteq$: For at vise at $\bigcap_{n\in\mathbb{N}} I_n \subseteq \{0\}$ skal vi vise at

$$x \in \bigcap_{n\in\mathbb{N}} I_n \Rightarrow x \in \{0\}, \tag{7.30}$$

eller med andre ord at

$$x \in \bigcap_{n\in\mathbb{N}} I_n \Rightarrow x = 0. \tag{7.31}$$

Det vil vi vise ved kontraposition, så vi vil altså vise at

$$x \neq 0 \Rightarrow x \notin \bigcap_{n\in\mathbb{N}} I_n \tag{7.32}$$

Antag altså at $x \neq 0$. Det betyder at $x < 0$ eller $x > 0$. Vi behandler de to tilfælde hver for sig og skal altså (iflg. bemærkning 211) vise, at under hver af de to antagelser eksisterer der et $n \in \mathbb{N}$, så $x \notin \bigcap_{n\in\mathbb{N}} I_n$.

Antag altså først at $x < 0$. Da gælder for alle $n \in \mathbb{N}$, at $x \notin I_n$, og så meget mere eksisterer der da et $n \in \mathbb{N}$, så $x \notin I_n$.

Antag dernæst at $x > 0$. Bestem da $n \in \mathbb{N}$, så $n > \frac{1}{x}$. At dette er muligt, vil vi senere bevise stringent. Men så er $x > \frac{1}{n}$, hvoraf følger at $x \notin I_n = \left[0, \frac{1}{n}\right]$. Altså har vi vist, at der findes et $n \in \mathbb{N}$ så $x \notin I_n$. ■

Bemærkning 213 *I dette bevis har vi brugt en stor del af det maskineri, vi har bygget op tidligere. Prøv at lokaliser alle de tidligere definitioner og bevisstrategier, vi har haft i gang.*

Definition 214 *Lad $\{A_\alpha\}_{\alpha\in\Lambda}$ være en familie af mængder. Foreningsmængden af alle familiens mængder ("foreningsmængden af A_α'erne for α i Λ) betegnes med $\bigcup_{\alpha\in\Lambda} A_\alpha$ og defineres formelt ved:*

$$\bigcup_{\alpha\in\Lambda} A_\alpha = \{x \mid \exists\alpha \in \Lambda : x \in A_\alpha\} \tag{7.33}$$

Med andre ord $x \in \bigcup_{\alpha\in\Lambda} A_\alpha$, hvis der findes et $\alpha \in \Lambda$, så $x \in A_\alpha$. I tilfælde af at indexmængden er $\{1, 2, 3, ..., m\}$ eller $\mathbb{N}$ skriver man også $\bigcup_{n=1}^{m}$ og $\bigcup_{n=1}^{\infty}$.

Bemærkning 215 *Ved negation af definitionen ses at $x \notin \bigcup_{\alpha\in\Lambda} A_\alpha$, hvis og kun hvis $\forall\alpha \in \Lambda; x \notin A_\alpha$.*

Eksempel 216 *Betragt familien af intervaller defineret ved $J_n = \left[0, 1 - \frac{1}{n}\right]$ for $n \in \mathbb{N}$. Vi vil vise at $\bigcup_{n=1}^{\infty} J_n = [0, 1[$.*

Bevis. $\subseteq$: Antag først at $x \in \bigcup_{n=1}^{\infty} J_n$. Vi skal vise, at $x \in [0, 1[$. Når $x \in \bigcup_{n=1}^{\infty} J_n$ betyder det pr. definition, at der findes et $n \in \mathbb{N}$, så $x \in J_n$. Men da $J_n = \left[0, 1 - \frac{1}{n}\right] \subseteq [0, 1[$, ses heraf, at $x \in [0, 1[$.

$\supseteq$: Antag dernæst at $x \in [0, 1[$. Vi skal vise at $x \in \bigcup_{n=1}^{\infty} J_n$, altså at $\exists n \in \mathbb{N} :$ $x \in J_n$. Når $x \in [0, 1[$, gælder specielt at $x < 1$ eller at $0 < 1 - x$, så vi kan bestemme et $n \in \mathbb{N}$, så $\frac{1}{1-x} < n$. Men da er $\frac{1}{n} < 1 - x$ eller $x < 1 - \frac{1}{n}$. Da vi endvidere havde antaget, at $0 \leq x$, følger det, at $x \in J_n = \left[0, 1 - \frac{1}{n}\right]$. ■

Bemærk at foreningsmængden af en uendelig familie af lukkede intervaller ikke behøver at være lukket.

Bemærkning 217 *I sidste del af beviset bestemte jeg pludseligt et n så $\frac{1}{1-x} < n$. Ved første blik kunne det se ud som en kanin, der blev trukket op af hatten. Men naturligvis er denne ide fremkommet ved en analyse, hvor vi begynder med det vi vil vise: Vi vil bestemme n så $x \in J_n$. Da vi jo har antaget at $x \in [0, 1[$ skal vi bare sørge for, at $x < 1 - \frac{1}{n}$. Men det betyder, at $\frac{1}{n} < 1 - x$, eller at $\frac{1}{1-x} < n$ (her bruges at $1 - x > 0$). Og det kan netop lade sig gøre, fordi $x \neq 1$. Syntesen, som blev præsenteret i beviset, er bare analysen kørt baglæns.*

Bemærkning 218 *Vi kunne også i beviserne for eksemplerne 212 og 216 have brugt at* $\frac{1}{n} \to 0$ *for* $n \to \infty$*. Men da det ikke ville have simplificeret beviset, er det bedre at undgå brugen af dette resultat.*

Sætning 219 *Lad* $\{A_\alpha\}_{\alpha\in\Lambda}$ *være en familie af mængder, og lad* A *være en mængde.*

a. Hvis $A \subseteq A_\alpha$ *for alle* $\alpha \in \Lambda$*, da gælder at* $A \subseteq \bigcap_{\alpha\in\Lambda} A_\alpha$*.*

b. Hvis $A_\alpha \subseteq A$ *for alle* $\alpha \in \Lambda$*, da gælder at* $\bigcup_{\alpha\in\Lambda} A_\alpha \subseteq A$*.*

Bevis. Overlades til læseren. ■

7.4 Mængdedifferens og komplementærmængde

Definition 220 *Lad* A *og* B *være mængder. Mængden af de elementer i* A*, som ikke er element i* B*, kaldes mængdedifferensen mellem* A *og* B*. Den betegnes med* $A \setminus B$*. Med andre ord:*

$$A \setminus B = \{x \mid (x \in A) \wedge (x \notin B)\} \tag{7.34}$$

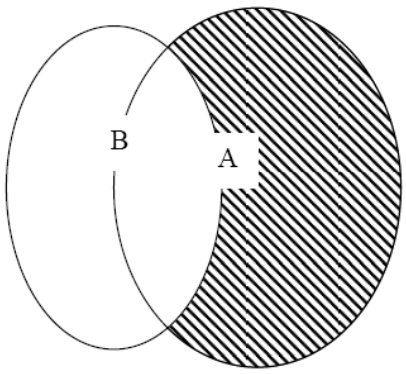
eller

$$x \in A \setminus B \Leftrightarrow (x \in A) \wedge (x \notin B) \tag{7.35}$$

Eksempel 221 $\{a, b, c, d, e, f\} \setminus \{d, e, f, g, h, i\} = \{a, b, c\}$.

Eksempel 222 $\mathbb{Z} \setminus \mathbb{Z}_- = \mathbb{Z}_+ \cup \{0\}$.

På Venn-diagrammet i Figur 7.4 er $A \setminus B$ skraveret.



Figur 7.4: Mængdedifferensen $A \setminus B$

Sætning 223 *Lad A og B være mængder. Da gælder:*

$$A \setminus B \subseteq A, \quad A \setminus A = \emptyset \quad og \quad A \setminus \emptyset = A \tag{7.36}$$

Øvelse 224 *Bevis at $A \setminus B$, $B \setminus A$ og $A \cap B$ er disjunkte mængder hvis foreningsmængde er lig med $A \cup B$.*

Det er ofte naturligt at betragte mængder, som alle er delmængder af en fast mængde, som vi da kalder **grundmængden**. For eksempel, når man arbejder med reel analyse er talmængderne alle delmængder af grundmængden $\mathbb{R}$, og i plangeometrien er punktmængderne alle delmængder af planen, der altså spiller rollen af grundmængde.

Lad os nu se på en sådan situation, hvor alle betragtede mængder er delmængder af en grundmængde, som vi kalder U (Vi bruger bogstavet U, fordi grundmængden kaldes "the universe" på engelsk).

Definition 225 *Lad A være en delmængde af en grundmængde U. Da kaldes $U \setminus A$ for **komplementærmængden** til A, og den betegnes med $\complement A$.*

$$\complement A = U \setminus A = \{x \in U \mid x \notin A\} \tag{7.37}$$

Eksempel 226 *Inden for $\mathbb{R}$ gælder:*

$$\complement\, [a, \infty[=]-\infty, a[\tag{7.38}$$
$$\complement\,]a, b[=]-\infty, a] \cup [b, \infty[\tag{7.39}$$
$$\complement \mathbb{R}_+ = \mathbb{R}_- \cup \{0\}\,. \tag{7.40}$$

Sætning 227 *Inden for grundmængden U gælder:*

$$\complement U = \emptyset \quad og \quad \complement \emptyset = U. \tag{7.41}$$

og for en vilkårlig mængde A

$$\complement\complement A = A \tag{7.42}$$

Bemærkning 228 *Når man tager komplementærmængden til en mængde, er det vigtigt at vide, hvad grundmængden er. Man kunne måske tro at man kunne tage en helt universel grundmængde, altså mængden af al ting, så $\complement A$ kunne betyde alt der ikke er element i A. Det viser sig dog at det fører til problemer (se afsnit 7.8)*

7.5 Mængdealgebra

Vi har i det foregående indført en række operationer på mængder, som minder om regneoperationerne på de reelle tal. Foreningsmængde $\cup$ svarer på en ret oplagt måde til addition $+$, fællesmængde $\cap$ svarer, på en mindre oplagt måde, til multiplikation $\cdot$, og mængdedifferens $\setminus$ svarer til differens $-$. På samme

måde som regneoperationerne på $\mathbb{R}$ opfylder visse regneregler, så er der lignende regneregler for mængdeoperationerne. Dem skal vi udlede i dette afsnit.

Vi starter med to regneregler, som svarer til den distributive lov, som jo siger at

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{7.43}$$

Sætning 229 ***De distributive love.*** *Lad A, B og C være mængder. Da gælder*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{7.44}$$

og

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{7.45}$$

Bevis. Lad os vise den sidste identitet (7.45). Den første vises analogt.

For vilkårligt x gælder følgende biimplikationer:

$$\begin{aligned}
& x \in A \cup (B \cap C) && (7.46)\\
& \Leftrightarrow (x \in A) \vee (x \in B \cap C) && (7.47)\\
& \Leftrightarrow (x \in A) \vee ((x \in B) \wedge (x \in C)) && (7.48)\\
& \Leftrightarrow ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C)) && (7.49)\\
& \Leftrightarrow (x \in A \cup B) \wedge (x \in A \cup C) && (7.50)\\
& \Leftrightarrow x \in (A \cup B) \cap (A \cup C). && (7.51)
\end{aligned}$$

(Ved overgang fra (7.48) til (7.49) brugte vi den logiske regel (1.15). Heraf følger (7.45). ■

Bemærk at det her gav et mere overskueligt bevis at opskrive en række biimplikationer, end det ville have været at vise de to inklusioner $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ og $A \cup (B \cap C) \supseteq (A \cup B) \cap (A \cup C)$ hver for sig.

Bemærkning 230 *Der er ikke helt analogi mellem de algebraiske operationer og mængdeoperationerne. For mængdeoperationerne gælder begge de distributive love (7.44) og(7.45). For de algebraiske regneoperationer gælder kun (7.43), hvorimod udsagnet $a + (b \cdot c) = (a + b)(a + c)$ ikke generelt er sandt.*

Øvelse 231 *Tegn Venn-diagrammer der illustrerer de distributive love.*

De distributive love kan generaliseres til familier af mængder:

Sætning 232 ***De distributive love.*** *Lad A være en mængde og $\{B_\alpha\}_{\alpha \in \Lambda}$ en familie af mængder. Da gælder:*

$$A \cap \left(\bigcup_{\alpha \in \Lambda} B_\alpha \right) = \bigcup_{\alpha \in \Lambda} (A \cap B_\alpha) \tag{7.52}$$

og

$$A \cup \left(\bigcap_{\alpha \in \Lambda} B_\alpha \right) = \bigcap_{\alpha \in \Lambda} (A \cup B_\alpha) \tag{7.53}$$

Bevis. Denne gang viser vi den første identitet (7.52). Den sidste vises analogt.

For vilkårligt x gælder der følgende biimplikationer:

$$x \in A \cap (\bigcup_{\alpha\in\Lambda} B_\alpha) \tag{7.54}$$
$$\Leftrightarrow (x \in A) \wedge (x \in \bigcup_{\alpha\in\Lambda} B_\alpha) \tag{7.55}$$
$$\Leftrightarrow (x \in A) \wedge (\exists\alpha \in \Lambda : x \in B_\alpha) \tag{7.56}$$
$$\Leftrightarrow \exists\alpha \in \Lambda : (x \in A) \wedge (x \in B_\alpha) \tag{7.57}$$
$$\Leftrightarrow \exists\alpha \in \Lambda : x \in A \cap B_\alpha \tag{7.58}$$
$$\Leftrightarrow x \in \bigcup_{\alpha\in\Lambda} (A \cap B_\alpha) \tag{7.59}$$

(Ved overgang fra (7.56) til (7.57) brugtes en variant af formel (1.36).) Heraf følger (7.52). ■

Sætning 233 ***De Morgans love***[2]*. Lad X være en mængde og lad $\{B_\alpha\}_{\alpha\in\Lambda}$ være en familie af delmængder af X. Da gælder:*

$$X \setminus (\bigcup_{\alpha\in\Lambda} B_\alpha) = \bigcap_{\alpha\in\Lambda} (X \setminus B_\alpha) \tag{7.60}$$

og

$$X \setminus \bigcap_{\alpha\in\Lambda} B_\alpha = \bigcup_{\alpha\in\Lambda} (X \setminus B_\alpha) \tag{7.61}$$

Bevis. Vi beviser kun (7.61). Beviset for (7.60) er analogt.

For vilkårligt x har vi følgende biimplikationer:

$$x \in X \setminus \bigcap_{\alpha\in\Lambda} B_\alpha \tag{7.62}$$
$$\Leftrightarrow (x \in X) \wedge (\neg(x \in \bigcap_{\alpha\in\Lambda} B_\alpha)) \tag{7.63}$$
$$\Leftrightarrow (x \in X) \wedge (\neg(\forall\alpha \in \Lambda : x \in B_\alpha)) \tag{7.64}$$
$$\Leftrightarrow (x \in X) \wedge (\exists\alpha \in \Lambda : \neg(x \in B_\alpha)) \tag{7.65}$$
$$\Leftrightarrow \exists\alpha \in \Lambda : (x \in X) \wedge (\neg(x \in B_\alpha)) \tag{7.66}$$
$$\Leftrightarrow \exists\alpha \in \Lambda : (x \in X \setminus B_\alpha) \tag{7.67}$$
$$\Leftrightarrow x \in \bigcup_{\alpha\in\Lambda} (X \setminus B_\alpha) \tag{7.68}$$

Heraf følger (7.61) ■

Hvis vi specielt lader X være grundmængden U, så kan De Morgans love skrives på formen:

Sætning 234 *Lad $\{B_\alpha\}_{\alpha\in\Lambda}$ være en familie af delmængder af grundmængden U. Da gælder:*

$$\complement(\bigcup_{\alpha\in\Lambda} B_\alpha) = \bigcap_{\alpha\in\Lambda} (\complement B_\alpha) \tag{7.69}$$

[2] Efter Augustus de Morgan 1806-1871

og

$$\complement(\bigcap_{\alpha\in\Lambda} B_\alpha) = \bigcup_{\alpha\in\Lambda} (\complement B_\alpha) \tag{7.70}$$

Specielt hvis familien består af to delmængder, kan De Morgans love formuleres som følger:

Sætning 235 *Lad X, A og B være mængder. Da gælder:*

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B) \tag{7.71}$$

og

$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B) \tag{7.72}$$

Øvelse 236 *Tegn et Venn-diagram, der illustrerer disse specialtilfælde af De Morgans love.*

Bemærkning 237 *Ovenfor blev der brugt to forskellige måder at præsentere to resultater, hvoraf den ene er en generalisering af den anden. Ved præsentation af de distributive love formulerede jeg først det specielle tilfælde i sætning 229 og generaliserede det derefter i sætning 232. Ved præsentation af De Morgans love beviste jeg straks det generelle resultat (Sætning 233), hvorefter de specielle resultater i sætning 235 faldt ud som specialtilfælde. Den første metode kan have pædagogiske fordele, medens den anden er den korteste og matematisk mest elegante.*

Sætning 238 *Lad A, og B være mængder. Da gælder:*

$$B \setminus (B \setminus A) = A \cap B \tag{7.73}$$

og

$$(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B) \tag{7.74}$$

Øvelse 239 *Illustrer disse identiteter i et Venn-diagram og bevis dem formelt.*

7.6 Produktmængde

Definition 240 *Et **ordnet par** (a, b) er et par i en bestemt rækkefølge. Det betyder at to ordnede par er lig hinanden, hvis og kun hvis de indeholder de samme objekter i samme rækkefølge:*

$$(a_1, b_1) = (a_2, b_2) \Leftrightarrow (a_1 = a_2) \wedge (b_1 = b_2). \tag{7.75}$$

Bemærkning 241 *Det er vigtigt skelne mellem mængden $\{a, b\}$ og det ordnede par (a, b). Hvis $a \neq b$ er $(a, b) \neq (b, a)$ medens $\{a, b\} = \{b, a\}$. Desuden er der mening i at tale om talparret (a, a), hvorimod $\{a, a\}$ blot er en besværlig måde at skrive $\{a\}$.*[3]

[3] Det er dog muligt at definere et ordnet par (a, b) udelukkende i mængdeteoretiske termer. Man definerer det da som $\{\{a\}, \{a, b\}\}$

Definition 242 *Lad A og B være to givne mængder. Vi betragter da ordnede par (a, b), hvor a på førstepladsen er et element fra A og b på andenpladsen er et element fra B. Mængden af sådanne par kaldes* ***produktmængden*** *(eller det cartesiske produkt) af A og B og betegnes med $A \times B$.*

$$A \times B = \{(a, b) \mid (a \in A) \wedge (b \in B)\} \tag{7.76}$$

Eksempel 243 *Lad $A = \{1, 2\}$ og $B = \{a, b, c\}$. Da består $A \times B$ af følgende ordnede par:*

$$\begin{array}{ccc} c & (1,c) & (2,c) \\ b & (1,b) & (2,b) \\ a & (1,a) & (2,a) \\ & 1 & 2 \end{array} \tag{7.77}$$

Altså $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$

Notation 244 *Man kan naturligvis lade $A = B$ i definitionen af produktmængden. I så fald skriver man ofte A^2 i stedet for $A \times A$.*

Eksempel 245 *Bestem A^2 og B^2 når A og B har samme betydning som i eksempel 243*

Eksempel 246 $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ *består af reelle talpar (a, b) hvor $a, b \in \mathbb{R}$. Hvis man i planen indlægger to på hinanden vinkelrette tallinjer, kan man på velkendt og entydig vis tilordne et bestemt talpar fra $\mathbb{R}^2$ til ethvert punkt i planen.*

Øvelse 247 *Opskriv følgende delmængde af $\mathbb{R}^2$: $[1, 4] \times]-1, 3[$ på formen $\{(x, y) \mid ....\}$ og illustrer mængden i talplanen.*

Definition 248 *Produktmængden $A \times B \times C$ af tre givne mængder A, B og C defineres tilsvarende ved*

$$A \times B \times C = \{(a, b, c) \mid (a \in A) \wedge (b \in B) \wedge (c \in C)\}. \tag{7.78}$$

og så videre for flere mængder.

Sætning 249 *Lad A, B og C være mængder. Da gælder*

$$A \times (B \cap C) = (A \times B) \cap (A \times C), \tag{7.79}$$
$$A \times (B \cup C) = (A \times B) \cup (A \times C), \tag{7.80}$$
$$(A \cap B) \times C = (A \times C) \cap (B \times C), \tag{7.81}$$
$$(A \cup B) \times C = (A \times C) \cup (B \times C), \tag{7.82}$$
$$A \times (B \setminus C) = (A \times B) \setminus (A \times C), \tag{7.83}$$
$$(A \setminus B) \times C = (A \times C) \setminus (B \times C), \tag{7.84}$$
$$A \subseteq B \Rightarrow A \times C \subseteq B \times C, \tag{7.85}$$
$$A \subseteq B \Rightarrow C \times A \subseteq C \times B \tag{7.86}$$

Bevis. Vi viser kun (7.80). Resten overlades til læseren.

For et vilkårligt talpar (x, y) har vi følgende biimplikationer:

$$\begin{aligned}
&(x,y) \in A \times (B \cup C) && (7.87)\\
&\quad \Leftrightarrow (x \in A) \wedge (y \in B \cup C) && (7.88)\\
&\quad \Leftrightarrow (x \in A) \wedge ((y \in B) \vee (y \in C)) && (7.89)\\
&\quad \Leftrightarrow ((x \in A) \wedge (y \in B)) \vee ((x \in A) \wedge (y \in C)) && (7.90)\\
&\quad \Leftrightarrow ((x,y) \in A \times B) \vee ((x,y) \in A \times C) && (7.91)\\
&\quad \Leftrightarrow (x,y) \in (A \times B) \cup (A \times C) && (7.92)
\end{aligned}$$

Heraf følger (7.80). ■

7.7 Potensmængden

Som vi allerede har bemærket, kan mængder selv være elementer i andre mængder. En familie af mængder $\{B_\alpha\}_{\alpha \in \Lambda}$ er et eksempel på en mængde af mængder. Man betragter ofte en mængde af delmængder af en given mængde. Mængden der består af alle delmængderne af en given mængde kaldes dens potensmængde.

Definition 250 *Lad A være en mængde. Mængden af alle A's delmængder kaldes A 's potensmængde og betegnes med $P(A)$.*

Eksempel 251 *Betragt mængden $\{1, 2, 3\}$. Den har følgende delmængder: $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, $\{1, 2, 3\}$. Altså er*

$$P(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\} \qquad (7.93)$$

Eksempel 252 $P(\emptyset) = \{\emptyset\}$

Sætning 253 *Hvis A og B er mængder og $A \subseteq B$ da er $P(A) \subseteq P(B)$.*

Bevis. Antag at $A \subseteq B$, og antag at $X \in P(A)$. Vi skal da vise, at $X \in P(B)$. Udsagnet $X \in P(A)$ betyder pr. definition, at $X \subseteq A$. Da endvidere $A \subseteq B$, ved vi fra Sætning 192, at $X \subseteq B$, hvorfor $X \in P(B)$. ■

Sætning 254 *Lad A og B være mængder. Da gælder:*

$$P(A \cap B) = P(A) \cap P(B) \qquad (7.94)$$

og

$$P(A \cup B) \supseteq P(A) \cup P(B) \qquad (7.95)$$

Bevis. Overlades til læseren. ■

Øvelse 255 *Vis ved et modeksempel at inklusionen $P(A \cup B) \subseteq P(A) \cup P(B)$ ikke er sand generelt. Overvej hvad A og B skal opfylde for at $P(A \cup B) \subseteq P(A) \cup P(B)$.*

Bemærkning 256 *De to udsagn $A \subseteq B$ og $A \in P(B)$ er ækvivalente. Udsagnet $A \subseteq B$ er dog begrebsmæsigt simplere og bør derfor normalt foretrækkes frem for $A \in P(B)$. Man bør generelt formulere sig på den simplest mulige måde. Af samme grund vil det ofte være lettere forståeligt, hvis man skriver "en familie af delmængder af A" i stedet for "en delmængde af $P(A)$".*

7.8 Russels paradoks

Et paradoks er i daglig tale en selvmodsigende situation. Man siger, at der er et paradoks (eller en indre modstrid) i en matematisk teori, hvis man kan udlede en sætning p og også kan udlede dens negation $\neg p$. En sådan situation kan man ikke acceptere i matematikken. For ikke alene betyder det, at vi ikke ved, hvilken af de to alternativer p og $\neg p$ vi skal regne for sand (og logikkens regler kræver at præcist et af de to udsagn er sandt); det betyder faktisk også, at vi kan bevise ethvert udsagn q (og dets negation) i teorien. Husk nemlig at man kan bevise et udsagn q ved at vise at $\neg q \Rightarrow (p \wedge \neg p)$ (bevis ved modstrid). Men hvis både p og $\neg p$ er sætninger i teorien er $(p \wedge \neg p)$ sand, hvorfor udsagnet $\neg q \Rightarrow (p \wedge \neg p)$ er sandt. Altså er det vilkårlige udsagn q bevist ved modstrid. Altså hvis en teori indeholder ét paradoks, så er enhver sætning paradoksal i den forstand at både den og dens negation er sand, eller sagt anderledes: ethvert udsagn i teorien er både sandt og falsk. En sådan teori er både paradoksal og uinteressant.

Vi har flere gange i det foregående advaret mod at opfatte "alting" som en mængde. For eksempel insisterede vi på, at man skulle have en grundmængde for at kunne danne komplementærmængder, og vi understregede nødvendigheden af, at den frie variabel i et prædikat var begrænset til en given mængde, så vi ikke kan tale om alt i hele verden, som opfylder prædikatet. Man kan heller ikke tale om mængden af alle mængder, men kun om mængden af mængder, som er delmængder af samme givne mængde (potensmængden). Vi skal her se, hvordan der kan opstå paradokser, hvis man ikke tager disse forholdsregler. Så lad os lige for en stund glemme forholdsreglerne og formulere Russels paradoks[4].

Der er i verden nogle mængder, som indeholder sig selv som element, for eksempel mængden af mængder, og mængden af de mængder, som kan beskrives på dansk med under 20 ord. Denne sidstnævnte mængde indeholder jo sig selv, for jeg har lige beskrevet den med under 20 ord. Der er naturligvis også mængder, som ikke indeholder sig selv som element. Alle de mængder vi har set på i denne bog har således ikke haft sig selv som element. Nu kan vi så se på mængden M af alle de mængder, som ikke har sig selv som element, altså

$$M = \{X \mid X \notin X\} \tag{7.96}$$

Vi spørger så, om M har sig selv som element eller ej? For at tydeliggøre argumentet kalder vi prædikatet $X \notin X$ for $p(X)$. Altså er $M = \{X \mid p(X)\}$

[4] Efter matematikeren, filosoffen og fredsforkæmperen Bertrand Russell 1872 - 1970

Antag først at $M \in M$, altså at $M \in \{X \mid X \notin X\} = \{X \mid p(X)\}$. Ifølge definitionen på sandhedsmængden $\{X \mid p(X)\}$ betyder det, at $p(M)$ er sand altså at $M \notin M$.

Antag dernæst at $M \notin M$. Da $M = \{X \mid X \notin X\} = \{X \mid p(X)\}$, betyder det, at $p(M)$ er falsk, altså at $\neg p(M)$ er sand. Men det betyder, at $\neg(M \notin M)$, altså at $M \in M$.

Vi har altså vist at $M \in M \Rightarrow (\ \neg(M \in M))$ og $(\ \neg(M \in M)) \Rightarrow M \in M$. Men da et udsagn enten er sandt eller falsk, må enten $M \in M$ eller $(\ \neg(M \in M))$ være sandt. I begge tilfælde har vi udledt

$$M \in M \wedge (\neg(M \in M)) \tag{7.97}$$

altså et paradoks.

Der er altså indbygget et paradoks i mængdelæren, med mindre man forbyder nogle af de mængder, som indgår i Russels paradoks.

Russel's paradoks understreger vigtigheden af at formulere et sæt aksiomer for mængdelæren, altså regler for hvordan man må danne mængder og operere med dem. Det mest almindeligt accepterede aksiomssystem for mængdelæren er det såkaldte Zermelo-Fraenkel aksiomssystem eller ZFC. Vi skal ikke opstille dette aksiomssystem her, men blot understrege at vores tidligere forbud mod at tale om mængden af alt, er en følge af dette aksiomssystem. Inden for en mængdelære beskrevet ved ZFC kan Russels paradoks og lignende paradokser ikke opstå. Der kan dog ikke gives et bevis for, at der slet ikke kan opstå paradokser[5] (Gödels sætning).

7.9 Opgaver

1. Skriv følgende mængder på elementform:
(a) $\{x \in \mathbb{R} \mid 4x^2 - 4x - 3 = 0\}$
(b) $\{x \in \mathbb{Z} \mid 4x^2 - 4x - 3 = 0\}$
(c) $\{x \in \mathbb{N} \mid x \text{ går op i } 12\}$

2. Bevis, at
(a) $\{1, 2\} \subseteq \{x \in \mathbb{R} \mid x^2 + 2x \geq 3\}$
(b) $\{1, 2\} \subseteq \{x \in \mathbb{R} \mid x^4 - x^3 - x^2 - 5x + 6 = 0\}$
(c) $\{x \in \mathbb{R} \mid x^2 + 3x + 4 \leq 7\} \subseteq \{x \in \mathbb{R} \mid x^2 + 3x + 4 \leq 8\}$

3. Tegn Venn-diagrammer der illustrerer følgende situationer:
(a)$A \subseteq B \subseteq C$
(b) $A \subseteq C$, $B \subseteq C$, og $A \cap B = \emptyset$
(c) $A \cap B \subseteq C$, men hverken A eller B er delmængder af C
(d) $A \cap B \neq \emptyset$, $A \cap C \neq \emptyset$ og $B \cap C \neq \emptyset$, og mængderne $A \cap B$, $A \cap C$ og $B \cap C$ er parvist disjunkte

4. Lad A og B være delmængder af en given grundmængde U.

[5] Det kan i hvert fald ikke bevises inden for mængdelæren selv eller inden for en simplere matematisk teori.

(a) Vis, at $B \subseteq A$ hvis og kun hvis

$$A \cup \complement B = U \tag{7.98}$$

(b) Vis, at A og B er disjunkte, hvis og kun hvis

$$\complement A \cup \complement B = U \tag{7.99}$$

Overbevis dig først om rigtigheden af udsagnene ved at tegne Venn-diagrammer og giv derefter formelle beviser.

5. Bevis, at

$$\bigcap_{n=1}^{\infty}]-\frac{1}{n}, 1+\frac{1}{n}[= [0,1] \tag{7.100}$$

og

$$\bigcup_{n=1}^{\infty}]-\frac{1}{n}, 1+\frac{1}{n}[=]-1,2[\tag{7.101}$$

6. Bestem

$$\bigcap_{n=1}^{\infty} [-1, 1-\frac{1}{n}] \tag{7.102}$$

og

$$\bigcup_{n=1}^{\infty} [-1, 1-\frac{1}{n}] \tag{7.103}$$

og bevis dine påstande.

7. Bestem $\bigcap_{n=1}^{\infty}]n, n+1[$ og $\bigcup_{n=1}^{\infty}]n, n+1[$.

8. Gælder der følgende distributive love?

$$A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C), \tag{7.104}$$

$$A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C), \tag{7.105}$$

og

$$\complement(A \setminus B) = (\complement A) \setminus (\complement B)? \tag{7.106}$$

Angiv et modeksempel eller et bevis i hvert tilfælde.

9. Lad mængderne A og B være defineret ved:

$$A = \{10, 20, 30, 40\}, \tag{7.107}$$

$$B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \tag{7.108}$$

Tegn et skema med dobbelt indgang, hvis rubrikker svarer til $A \times B$.

Marker mængderne

$$K = \{(x, y) \in A \times B \mid x + y \text{ er delelig med } 5\} \tag{7.109}$$

og

$$K' = \{(x, y) \in A \times B \mid x + y \text{ er delelig med 7 og } x + y \text{ er et kvadrattal}\} \tag{7.110}$$

10. Lad A og B være mængder. Gælder det generelt at

$$P(A \setminus B) = P(A) \setminus P(B)? \tag{7.111}$$

Giv bevis eller modeksempel.

Kapitel 8

Kompositionsregler

8.1 Definition, eksempler og simple egenskaber

Regneoperationerne addition $+$ og multiplikation $\cdot$ er eksempler på kompositionsregler. Generelt definerer vi:

Definition 257 *En kompositionsregel $*$ på en mængde M er en forskrift, som til to elementer x og y knytter et nyt element $x * y$ i M*[1]

Notation 258 *Kompositionsregler benævnes ofte med tegn som $\star$, $\oplus$, $\otimes$, $+$ eller $\cdot$.*

En mængde M udstyret med en kompositionsregel $\star$ betegnes med $(M, \star)$.

Eksempel 259 *Her følger en række eksempler på kompositionsregler:*

1. *Addition og multiplikation på $\mathbb{R}$.*
2. *Subtraktion på $\mathbb{R}$.*
3. *Når M er en mængde, er $\cap$ og $\cup$ kompositionsregler på mængden $P(M)$ af delmængder af M.*
4. *Forskriften $x \oplus y = \frac{1}{2}(x+y)$ (gennemsnitsdannelse) er en kompositionsregel på $\mathbb{R}$.*
5. *Addition og multiplikation på $\mathbb{Z}$.*

Øvelse 260 *Overvej om de elementære regneoperationer $+, -, \cdot, :$ er kompositionsregler på følgende talmængder: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{Q}_+, \mathbb{R}, \mathbb{R}_+, \mathbb{R} \setminus \{0\}$. Det der afgør sagen, er om kompositionsreglen (lad os kalde den $\star$) er defineret for alle par (x, y) i mængden, og om $x \star y$ igen ligger i mængden.*

[1] Når vi har indført et præcist funktionsbegreb vil vi kunne definere en kompositionsregel som en funktion fra $M \times M$ ind i M.

Definition 261 *Lad $\star$ være en kompositionsregel på mængden M.*

1. *$\star$ siges at være **associativ,** hvis det for alle $x, y, z \in M$ gælder at*

$$x \star (y \star z) = (x \star y) \star z \tag{8.1}$$

2. *$\star$ siges at være **kommutativ,** hvis det for alle $x, y \in M$ gælder at*

$$x \star y = y \star x \tag{8.2}$$

Eksempel 262 *I Eksempel 259 er kompositionsreglerne i 1, 3 og 5. både associative og kommutative.*

Gennemsnitsdannelse nævnt i punkt 4 er kommutativ men ikke associativ (overvej dette).

Subtraktion på $\mathbb{R}$ er hverken kommutativ eller associativ. (overvej).

Bemærkning 263 *Når en kompositionsregel $\star$ er associativ, kan man tillade sig at skrive $x \star y \star z$ i stedet for $x \star (y \star z)$ eller $(x \star y) \star z$.*

Når der er tale om associative kompositionsregler, kan man i det hele taget tillade sig at sætte og hæve parenteser uden at ændre i udtryk af formen $x_1 \star x_2 \star \cdots \star x_n$ (overvej dette).

Når en kompositionsregel $\star$ er kommutativ og associativ, kan man bytte om på leddenes orden i udtryk af formen $x_1 \star x_2 \star \cdots \star x_n$ (overvej).

Definition 264 *Lad $\star$ være en kompositionsregel på mængden M. Et element $e \in M$ kaldes et **neutralt element** for $\star$ (eller i $(M, \star)$), hvis det for ethvert $x \in M$ gælder, at*

$$x \star e = e \star x = x \tag{8.3}$$

Eksempel 265 *Eksempler på neutrale elementer:*

1. *Tallet 0 er neutralt element i $(\mathbb{R}, +)$*
2. *Tallet 1 er neutralt element i $(\mathbb{R}, \cdot)$*
3. *Den tomme mængde $\emptyset$ er neutralt element for $\cup$ på $P(M)$*
4. *M er neutralt element for $\cap$ på $P(M)$.*

Øvelse 266 *Bevis at gennemsnitsdannelse beskrevet i Eksempel 259.4 ikke har noget neutralt element.*

Sætning 267 *Hvis en kompositionsregel $\star$ på en mængde M har et neutralt element, da er det entydigt bestemt.*

Bevis. Lad $\star$ være en kompositionsregel på mængden M og antag at e_1 og e_2 er neutrale elementer i $(M, \star)$. Da e_1 er et neutralt element gælder at $e_1 \star e_2 = e_2$. Da e_2 er et neutralt element gælder ligeledes at $e_1 \star e_2 = e_1$. Altså er $e_1 = e_2$. ■

Definition 268 *Lad $(M, \star)$ være en mængde med en kompositionsregel, og lad e være et neutralt element i $(M, \star)$. Ved et* ***inverst element*** *til et element $x \in M$ forstås et element $y \in M$, for hvilket*

$$x \star y = y \star x = e \tag{8.4}$$

Eksempel 269 *1. I $(\mathbb{R}, +)$ er $-x$ det inverse element til x.*

2. I $(\mathbb{R}_+, \cdot)$ er $1/x$ det inverse element til x.

Øvelse 270 *Overvej om ethvert element har et inverst element i følgende mængder med kompositionsregel:* $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$.

Sætning 271 *Lad $\star$ være en associativ kompositionsregel på mængden M, og lad e være et neutralt element for $\star$. Hvis et element $x \in M$ har et inverst element, da er det entydigt bestemt.*

Bevis. Antag, at y og z er inverse elementer til x altså, at $x \star y = y \star x = e$ og $x \star z = z \star x = e$. Da gælder:

$$y = y \star e = y \star (x \star z) = (y \star x) \star z = e \star z = z \tag{8.5}$$

■

Sætning 272 *Lad $\star$ være en associativ kompositionsregel på mængden M, og lad e være et neutralt element for $\star$. Da er e sit eget inverse element.*

Bevis. Vi skal checke at $e \star e = e$, men det følger af definitionen af det neutrale element. ■

8.2 Grupper

Mængder med en associativ kompositionsregel, hvori der findes et neutralt element, og hvori ethvert element har et inverst element, er så hyppigt forekommende i matematikken, at man giver dem et særligt navn:

Definition 273 *En* ***gruppe*** *$(G, \star)$ er en mængde G udstyret med en kompositionsregel $\star$, der har følgende egenskaber:*

1. *Kompositionsreglen $\star$ er associativ; d.v.s. for alle $x, y, z \in G$ gælder*

$$(x \star y) \star z = x \star (y \star z). \tag{8.6}$$

2. *Der findes et neutralt element $e \in G$; d.v.s. at for alle $x \in G$ gælder*

$$x \star e = e \star x = x. \tag{8.7}$$

3. *Ethvert element i G har et inverst element; d.v.s at for alle $x \in G$ findes et element, som vi vil kalde x^{-1}, for hvilket*

$$x \star x^{-1} = x^{-1} \star x = e \tag{8.8}$$

Antallet af elementer i gruppen kaldes gruppens orden. Hvis gruppen er uendelig er dens orden ∞.

Det fremgår af sætning 267 og 271, at det neutrale element i en gruppe er entydigt bestemt, og ligeledes at det inverse til et givet element også er entydigt. Derfor kan vi tillade os at tale om *det neutrale element, og give det navnet e* og vi kan tale om *det* inverse element til et element $x \in G$ og give det navnet x^{-1}.

Definition 274 *En gruppe $(G, \star)$ kaldes kommutativ eller abelsk[2], hvis kompositionsreglen $\star$ er kommutativ.*

Eksempel 275 *Følgende er eksempler på abelske grupper:* $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{C}, +)$, $(\mathbb{C} \setminus \{0\}, \cdot)$.

Vi kommer senere til at møde eksempler på grupper, som ikke er abelske.

Sætning 276 *Lad $(G, \star)$ være en gruppe med neutralt element e. Da gælder*

$$e^{-1} = e \tag{8.9}$$

Bevis. Følger af 272. ■

Sætning 277 *Lad $(G, \star)$ være en gruppe og $x \in G$. Da gælder:*

$$\left(x^{-1}\right)^{-1} = x \tag{8.10}$$

Bevis. Vi skal vise at x er det inverse element til x^{-1}, altså at

$$x^{-1} \star x = x \star x^{-1} = e. \tag{8.11}$$

Men det gælder, fordi x^{-1} er det inverse element til x. ■

Sætning 278 *Lad $(G, \star)$ være en gruppe og $x, y \in G$. Da er*

$$(x \star y)^{-1} = y^{-1} \star x^{-1}. \tag{8.12}$$

Bevis. Ved gentagen brug af associativiteten fås

$$(x \star y) \star \left(y^{-1} \star x^{-1}\right) \tag{8.13}$$
$$= x \star \left(y \star \left(y^{-1} \star x^{-1}\right)\right) \tag{8.14}$$
$$= x \star \left(\left(y \star y^{-1}\right) \star x^{-1}\right) \tag{8.15}$$
$$= x \star \left(e \star x^{-1}\right) = x \star x^{-1} = e. \tag{8.16}$$

På samme vis ses at $\left(y^{-1} \star x^{-1}\right) \star (x \star y) = e$. ■

De følgende såkaldte **forkortningsregler** i grupper kan ofte benyttes:

[2] Efter den norske matematiker Niels Henrik Abel (1802-1829)

Sætning 279 *Lad $(G, \star)$ være en gruppe og $x, y, z \in G$. Da gælder*

$$x \star y = x \star z \Rightarrow y = z. \tag{8.17}$$

$$y \star x = z \star x \Rightarrow y = z. \tag{8.18}$$

Bevis. Antag at $x \star y = x \star z$. Så gælder også

$$x^{-1} \star (x \star y) = x^{-1} \star (x \star z).$$

Ved at bruge associativiten ses at

$$x^{-1} \star (x \star y) = (x^{-1} \star x) \star y = e \star y = y$$

og analogt

$$x^{-1} \star (x \star z) = (x^{-1} \star x) \star z = e \star z = z.$$

Disse tre ligninger viser at $y = z$. Den anden forkortningsregel vises på samme måde. ■

I senere algebrakurser vil I komme til at undersøge grupper meget mere indgående, og I vil lære om mange smukke egenskaber ved dem.

Grupper er et eksempel på en **matematisk struktur**. En **matematisk struktur** er en mængde som er udstyret med en kompositionsregel, en relation eller lignende. I en vis forstand er en mængde også en struktur, men en meget fattig struktur. Det eneste, der strukturerer den er "$\in$". Det karakteristiske ved en matematisk struktur er, at man ikke fastlægger hvad elementerne i mængden er for en slags objekter, og man ikke fastlægger hvilken kompositionsregel eller relation eller andet man har med at gøre. Man kræver bare, at visse eksplicit angivne aksiomer er opfyldt. Aksiomerne for en gruppe er de tre krav opremset i definition 273. Senere i dette kursus vil vi indføre andre matematiske strukturer som partielt ordnede mængder og mængder med en ækvivalensrelation. I lineær algebra indføres vektorrum, som en vigtig slags matematisk struktur. Senere på studiet vil du stifte bekendtskab med andre strukturer som målrum og metriske rum.

Der er flere fordele ved at indføre og arbejde med matematiske strukturer.

1. Når man har vist en sætning om en matematisk struktur, gælder den for alle de konkrete eksempler på denne struktur. Man slår med andre ord mange fluer med et smæk.

2. Man får klargjort den logiske struktur i sin teori ved klart at fastlægge spillereglerne.

3. Det bliver lettere at gennemskue hvilke forudsætninger en sætning bygger på.

4. Ved at fjerne overflødige ting kan man ofte lettere finde beviser for sætninger.

Lad mig her især fremhæve punkt 1. Når man i lineær algebra viser en sætning om vektorrum, har man faktisk vist et væld af sætninger om forskellige vektorrum. Sætningen gælder jo uanset om elementerne i vektorrummet er reelle tal, vektorer i rummet eller funktioner, og uanset betydningen af vektoraddition og multiplikation med skalar. I algebrakurset vil du komme til at vise en lang række sætninger om grupper, og disse vil altså gælde for alle grupper, det være sig $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, eller en anden konkret gruppe. En gruppeteoretisk sætning indeholder altså i sig en lang række sætninger om tal, geometri mm.

Bemærkning 280 *Hvis læseren synes at nogle af de ovenstående beviser om grupper er velkendte er det nok fordi vi gennemgik de samme beviser i Kapitel 3 under omtalen af de reelle tal.*

8.3 Ringe

En gruppe er en algebraisk struktur, hvori der er givet én kompositionsregel, som opfylder visse aksiomer. Ofte møder man dog mængder, hvorpå der er givet to kompositionsregler, som spiller sammen på særlig vis. Talmængderne $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ og $\mathbb{C}$ har både en addition og en multiplikation, og i alle disse mængder spiller additionen og multiplikationen sammen via den distributive lov. For at kunne studere alle disse talmængder og andre lignende mængder med to sammenknyttede kompositionsregler under ét, definerer vi en ny struktur, nemlig en ring:

Definition 281 *En mængde R udstyret med to kompositionsregler $+$ og $\cdot$ kaldes en **ring** og betegnes med $(R, +, \cdot)$, hvis følgende aksiomer er opfyldt:*

R1: $+$ er kommutativ, dvs. for alle $x, y \in R$ gælder:

$$x + y = y + x. \tag{8.19}$$

R2: $+$ og $\cdot$ er associative, dvs. for alle $x, y, z \in R$ gælder:

$$x + (y + z) = (x + y) + z \quad og \quad x\,(yz) = (xy)\,z. \tag{8.20}$$

R3: Der eksisterer et additivt og et multiplikativt neutralellement kaldet hhv. 0 og 1, dvs for alle $x \in R$ gælder at:

$$x + 0 = x \quad og \quad 1 \cdot x = x \cdot 1 = x. \tag{8.21}$$

R4: Der eksisterer additive inverser, eller mere præcist: For ethvert $x \in R$ findes et element, vi vil kalde $-x$, hvorom det gælder at

$$x + (-x) = 0. \tag{8.22}$$

*R5: De **distributive love**: For alle $x, y, z \in R$ gælder:*

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \quad og \quad (y + z) \cdot x = (y \cdot x) + (z \cdot x) \tag{8.23}$$

Definition 282 *En ring R kaldes en kommutativ ring, hvis multiplikationen også er kommutativ, altså hvis det for alle $x, y \in R$ gælder at*

$$x \cdot y = y \cdot x. \tag{8.24}$$

Eksempel 283 *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ og $\mathbb{C}$ er alle kommutative ringe, når de udstyres med de sædvanlige kompositionsregler.*

Notation 284 *Som vi plejer når vi regner i $\mathbb{R}$, vil vi ofte tillade os at udelade multiplikationstegnet $\cdot$. Ligeså vil vi bruge den sædvanlige konvention om, at multiplikation udføres før addition, så vi kan udelade parenteser om produkter. Derved kan den distributive lov skrives:*

$$x\,(y + z) = xy + xz. \tag{8.25}$$

Sætning 285 *Hvis $(R, +, \cdot)$ er en ring er $(R, +)$ en abelsk gruppe.*

Bemærkning 286 *Den distributive lov fortæller, hvordan gruppestrukturen i $(R, +)$ spiller sammen med multiplikationen.*

Bemærkning 287 *Når der i det følgende tales om en ring $(R, +, \cdot)$, er det underforstået, at de neutrale elementer og de inverse elementer betegnes som i definitionen ovenfor.*

Sætning 288 *Det følger af sætning 267 og 271, at de neutrale elementer i en ring er entydigt bestemt, og at den additivt inverse til et element er entydigt bestemt. Det er derfor, vi kan tillade os at navngive disse elementer i definitionen af en ring.*

Bemærkning 289 *Da $(R, +)$ er en abelsk gruppe gælder de sætninger vi beviste i forrige kapitel. Lad os specielt fremhæve Sætning 276, 277 og 278. Oversat til notationen i dette kapitel siger disse sætninger det følgende:*

Sætning 290 *Lad $(R, +, \cdot)$ være en ring og lad x, y være vilkårlige elementer i R. Da gælder:*

$$-0 = 0, \tag{8.26}$$

$$-(-x) = x, \tag{8.27}$$

$$-\left(x + y\right) = (-x) + (-y)\,. \tag{8.28}$$

De følgende sætninger viser hvordan den additive og den multiplikative struktur på $(R, +, \cdot)$ spiller sammen. Derfor er det klart at den distributive lov skal bruges i beviserne.

Sætning 291 *Det additive neutrale element 0 i en ring $(R, +, \cdot)$ har følgende multiplikative egenskab:*

For ethvert $x \in R$ gælder:

$$x \cdot 0 = 0 \cdot x = 0 \tag{8.29}$$

Bevis. Sæt $y = x \cdot 0$. Da gælder:

$$y = x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0 = y + y. \tag{8.30}$$

Ved at lægge $-y$ til på begge sider fås:

$$y + (-y) = y + y + (-y) \tag{8.31}$$

hvoraf det følger at

$$0 = y \tag{8.32}$$

Det overlades til læseren at vise at $0 \cdot x = 0$. ■

Bemærkning 292 *I ovenstående bevis og i de følgende beviser er det vigtigt, at man kun bruger de regneregler, som er specificeret i aksiomerne for en ring, og de sætninger, man har udledt derfra. Notationen kunne forføre en til bare at regne, som man plejer i $\mathbb{R}$, men i ringe er der nogle af regnereglerne i $\mathbb{R}$, som ikke holder. Check derfor nøje at vi i ovenstående udregninger kun brugte ringaksiomerne.*

Hvis $x \in R$ er $-x$ defineret ud fra den additive gruppestruktur. Elementet 1 er derimod defineret ud fra den multiplikative struktur. De spiller dog sammen på følgende måde:

Sætning 293 *Lad $(R, +, \cdot)$ være en ring. For ethvert $x \in R$ gælder:*

$$-x = (-1) \cdot x = x \cdot (-1). \tag{8.33}$$

Bevis. Vi skal bevise at $(-1) \cdot x$ er det additivt inverse element til x. Det ses af følgende udregning:

$$x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1 + (-1)) \cdot x = 0 \cdot x = 0 \tag{8.34}$$

Da det inverse element er entydigt, gælder dermed, at $-x = (-1) \cdot x$.

Det overlades til læseren at bevise at $-x = x \cdot (-1)$. ■

Sætning 294 *Lad $(R, +, \cdot)$ være en ring. Da gælder:*

$$(-1)(-1) = 1. \tag{8.35}$$

Bevis. Ifølge sætning 293 er $(-1)(-1) = -(-1)$, og ifølge sætning 290 er $-(-1) = 1$. ■

Sætning 295 *Lad $(R, +, \cdot)$ være en ring. For ethvert $x, y \in R$ gælder:*

$$(-x)\, y = x\, (-y) = -(xy) \tag{8.36}$$

$$(-x)(-y) = xy. \tag{8.37}$$

Bevis. Beviset af første identitet følger af (8.33):

$$(-x)(y) = ((-1)x)y = (-1)(xy) = -(xy) \tag{8.38}$$
$$x(-y) = (x((-1)y) = (x(-1))y \tag{8.39}$$
$$= ((-1)x)y) = (-1)(xy) = -(xy). \tag{8.40}$$

Beviset for den sidste identitet overlades til læseren. ■

I det ovenstående bevis er hvert enkelt skridt i beviset skrevet ud, således at der i hvert lighedstegn kun er brugt et af aksiomerne. I det følgende vil beviserne ikke altid blive skrevet ud i samme detaljegrad. Da både addition og multiplikation er associative, kan vi jo tillade os at hæve og sætte parenteser Det vil vi gøre frit i det følgende. Vi skal bare passe på ikke at bytte om på faktorerne i et produkt.

Bemærkning 296 *Hvis man udstyrer en mængde med ét element a med de to ens kompositionsregler:* $a + a = a$ *, og* $a \cdot a = a$*, så er* $(\{a\}, +, \cdot)$ *en ring med to ens neutralelementer* $0 = 1 = a$*. Denne ring kaldes* ***nul-ringen****.*

Sætning 297 *Hvis en ring R har mere end ét element, er* $0 \neq 1$*.*

Bevis. Vi beviser sætningen ved kontraposition. Antag altså at $0 = 1$. Ifølge sætning 291 gælder for ethvert element $x \in R$, at

$$x = 1 \cdot x = 0 \cdot x = 0. \tag{8.41}$$

Altså er der kun ét element i R. ■

Bemærkning 298 *I det følgende vil vi kun betragte ringe med mere end ét element, hvori altså* $0 \neq 1$*.*

Definition 299 *Et element x i en ring R kaldes* ***invertibelt****, hvis det er invertibelt med hensyn til multiplikationen, dvs. hvis der findes et inverst element kaldet* x^{-1} *så*

$$x \cdot x^{-1} = x^{-1} \cdot x = 1. \tag{8.42}$$

Sætning 300 *Hvis x er invertibelt i ringen R, da er dens inverse entydigt bestemt.*

Bevis. Følger af sætning 271. ■

Sætning 301 *I en ring R med mere end et element er* 0 *ikke invertibelt.*

Bevis. For alle $x \in R$ gælder

$$0 \cdot x = 0 \neq 1. \tag{8.43}$$

■

Bemærkning 302 *I en ring kan man ikke altid slutte, at hvis et produkt er lig nul, da er en af faktorerne lig nul (**nul-reglen**). Det kommer vi til at se et eksempel på i næste kapitel.*

Definition 303 *En kommutativ ring (som ikke er nulringen) kaldes et **integritetsområde**, hvis nul-reglen gælder, altså hvis*

$$x \cdot y = 0 \Rightarrow (x = 0) \vee (y = 0)\,. \tag{8.44}$$

Eksempel 304 $(\mathbb{Z}, +, \cdot)$ *er et integritetsområde.*

Sætning 305 *Lad R være et integritetsområde og $x \in R$, $x \neq 0$. Da gælder*

$$x \cdot y = x \cdot z \Rightarrow y = z. \tag{8.45}$$

Bevis. Hvis $x \cdot y = x \cdot z$ gælder

$$0 = x \cdot 0 = x \cdot (y + (-y)) = x \cdot y + x(-y) \tag{8.46}$$
$$= x \cdot z + x \cdot (-y) = x(z + (-y)). \tag{8.47}$$

Da $x \neq 0$ slutter vi fra nulreglen, at

$$z + (-y) = 0 \tag{8.48}$$

så

$$z = z + (-y) + y = 0 + y = y. \tag{8.49}$$

■

Sætning 306 *Hvis alle elementer i en kommutativ ring R på nær 0 er invertible, er ringen et integritetsområde.*

Bevis. Antag at $x \cdot y = 0$ og at $x \neq 0$. Da har x ifølge forudsætningen en multiplikativ invers x^{-1}, og vi får:

$$y = 1 \cdot y = \left(x^{-1} \cdot x\right) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0. \tag{8.50}$$

■

Bemærkning 307 *Som i afsnittet om grupper har den opmærksomme læser nok opdaget at mange sætninger og beviser i dette afsnit er helt magen til sætninger og beviser som vi gennemgik i afsnittet om de elementære egenskaber ved de reelle tal. Det er jo fordi de reelle tal er en ring. Men da vi i dette afsnit har været omhyggelige med kun at bruge aksiomerne for en ring, ved vi at de udledte sætninger gælder for enhver ring altså også for fx. de hele tal og de rationale tal.*

8.4 Legemer

Definition 308 *En kommutativ ring (forskellig fra nul-ringen), hvori alle elementer forskellige fra* 0 *er invertible, kaldes et* ***legeme.***

Med andre ord:

En mængde L *med to kompositionsregler* $+$ *(kaldet addition) og* $\cdot$ *(kaldet multiplikation) kaldes et* ***legeme*** *og betegnes* $(L,+,\cdot)$*, hvis følgende aksiomer er opfyldt:*

L1: $+$ *og* $\cdot$ *er kommutative, dvs. for alle* $x,y \in L$ *gælder:*

$$x+y=y+x \quad og \quad x\cdot y=y\cdot x. \tag{8.51}$$

L2: $+$ *og* $\cdot$ *er associative, dvs. for alle* $x,y,z \in L$ *gælder:*

$$(x+y)+z=x+(y+z) \quad og \quad (x\cdot y)\cdot z=x\cdot(y\cdot z). \tag{8.52}$$

L3: Der eksisterer et additivt og et multiplikativt neutralt element kaldet hhv. 0 *og* 1*, d.v.s der eksisterer to elementer* $0\neq 1$ *i* L *så for alle* $x \in L$ *gælder:*

$$x+0=x \quad og \quad x\cdot 1=x. \tag{8.53}$$

L4: Der eksisterer additive og multiplikative inverser, eller mere præcist: For ethvert $x \in L$ *findes et element vi vil kalde* $-x$ *i* L*, hvorom det gælder, at*

$$x+(-x)=0, \tag{8.54}$$

og for ethvert $x \in L\setminus\{0\}$ *findes et element vi vil kalde* x^{-1} *i* L*, hvorom det gælder, at*

$$x\cdot x^{-1}=1 \tag{8.55}$$

L5: Den ***distributive lov****: For alle* $x,y,z \in L$ *gælder, at*

$$x\cdot(y+z)=(x\cdot y)+(x\cdot z). \tag{8.56}$$

Sætning 309 *Hvis* $(L,+,\cdot)$ *er et legeme, er* $(L,+)$ *og*$(L\setminus\{0\},\cdot)$ *abelske grupper.*

Bevis. Det overlades til læseren at checke at alle aksiomerne for abelske grupper er opfyldt. ■

Bemærkning 310 *Alle de sætninger vi har udledt om (abelske) grupper, ringe og integritetsområder beholder deres gyldighed for legemer. Her skal fremhæves de vigtigste.*

Sætning 311 *Lad* $(L,+,\cdot)$ *være et legeme med neutralelementer* 0 *og* 1*. Lad* $x,y \in L$*.*

Da er de neutrale elementer entydigt bestemt, og de inverse elementer til x *er entydigt bestemt (for multiplikation forudsat at* $x\neq 0$*).*

Desuden gælder:

$$-(-x)=x \quad og \quad \left(x^{-1}\right)^{-1}=x \tag{8.57}$$

$$-0 = 0 \quad og \quad 1^{-1} = 1, \tag{8.58}$$

$$-(-x) = x \quad og \quad \left(x^{-1}\right)^{-1} = x, \tag{8.59}$$

$$-(x+y) = (-x) + (-y) \quad og \quad (xy)^{-1} = x^{-1} \cdot y^{-1}. \tag{8.60}$$

$$x \cdot 0 = 0 \tag{8.61}$$

$$x \cdot y = 0 \Rightarrow (x = 0) \vee (y = 0) \tag{8.62}$$

$$-x = (-1)\, x \tag{8.63}$$

$$(-x)\, y = -xy \tag{8.64}$$

$$(-x)\,(-y) = xy \tag{8.65}$$

Definition 312 *Lad $(L, +, \cdot)$ være et legeme. Vi definerer de to nye kompositionsregler $-$ (subtraktion) og $:$ (division) på L som følger:*

For ethvert $x, y \in L$ defineres

$$x - y := x + (-y)\,. \tag{8.66}$$

For ethvert $x, y \in L$ med $y \neq 0$ defineres

$$x : y := x \cdot y^{-1} \tag{8.67}$$

Vi skriver også $x : y$ som $\frac{x}{y}$ eller x/y.

Bemærkning 313 *Faktisk er division ikke en kompositionsregel på hele L men kun på $L \setminus \{0\}$. Bemærk, at man også analogt kan definere kompositionsreglen subtraktion hvis L kun er en ring. Det skyldes, at de betingelser, der adskiller en ring fra et legeme, kun involverer multiplikation.*

Sætning 314 *Lad $(L, +, \cdot)$ være et legeme. For ethvert $x, y \in L$ gælder*

$$x - y = -(y - x) \tag{8.68}$$

og

$$xy^{-1} = \left(yx^{-1}\right)^{-1} \tag{8.69}$$

Bevis. For at vise (8.68), skal vi vise, at $x - y$ den additivt inverse til $y - x$. Det følger af følgende udregning:

$$(y - x) + (x - y) = (y + (-x)) + (x + (-y)) = \tag{8.70}$$

$$y + ((-x) + x) + (-y) = y + 0 + (-y) = y + (-y) = 0. \tag{8.71}$$

Alternativt kan man bare anvende Sætning 278 på gruppen $(L, +)$.

(8.69) vises på samme måde. ■

Øvelse 315 *Lad $(L, +, \cdot)$ være et legeme. Bevis, at for $x, y \in L$ gælder*

$$x - y = 0 \Leftrightarrow x = y \tag{8.72}$$

og hvis $y \neq 0$

$$x/y = 1 \Leftrightarrow x = y \tag{8.73}$$

De rationale tal og de reelle tal er eksempler på legemer. De har dog begge en endnu rigere struktur, idet de også er udstyret med en ordning, som spiller sammen med regnereglerne på passende måde. De kaldes **ordnede legemer**. Aksiomssystemet for et ordnet legeme er faktisk identisk med det aksiomssystem for de reelle tal, vi har opskrevet i definition (1) hvis man udelader supremumsegenskaben. I afsnittet om de reelle tal brugte vi slet ikke supremumsegenskaben. Alle de sætninger, vi viste, var derfor baseret alene på aksiomerne for et ordnet legeme, og de gælder derfor i ethvert ordnet legeme fx. også i $\mathbb{Q}$. Hvis man tilføjer supremumsegenskaben til aksiomssystemet, har man aksiomssystemet for det man kalder et fuldstændigt ordnet legeme. De rationale tal er ikke fuldstændigt, og man kan vise at der i en vis forstand kun er ét fuldstændigt ordnet legeme. Hvor der altså er mange eksempler på grupper, ringe og legemer, er et fuldstændigt ordnet legeme altså helt entydigt bestemt ved sine aksiomer. Det er denne entydigt bestemte struktur vi kalder de reelle tal.[3]

8.5 Opgaver

1. Overvej om kompositionsreglerne nævnt i Øvelse 260 er kommutative og associative og hvad er neutralellementet.

2. Lad $(G, *)$ være en gruppe. Antag at der gælder $x * x = e$ for alle $x \in G$. Vis at G er abelsk, altså at $x * y = y * x$ for alle $x, y \in G$.

3. Lad $(G, *)$ være en gruppe. For $x \in G$ betegner x^2 elementet $x * x$. Vis at følgende udsagn er ækvivalente:

(a) G er abelsk

(b) For alle $x, y \in G$ er $(x * y)^2 = x^2 * y^2$.

4. Lad $(G, *)$ være en gruppe. Vis at følgende udsagn er ækvivalente:

(a) G er abelsk

(b) For alle $x, y \in G$ er $(x * y)^{-1} = x^{-1} * y^{-1}$.

5. Lad $+, \cdot$ være den sædvanlige addition og multiplikation i mængden af reelle tal $\mathbb{R}$. Betragt delmængden $L = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ af $\mathbb{R}$.

(a) Vis, at for $x, y \in L$ er $x + y \in L$ og $xy \in L$.

(b) Vis, at $(L, +, \cdot)$ er en kommutativ ring.

(c) Vis, at $(L, +, \cdot)$ er et legeme, altså at der for ethvert element $x = a + b\sqrt{2} \in L, x \neq 0$, findes et $y \in L$, så $xy = 1$. (Man kan starte at starte med at beregne produktet $(a + b\sqrt{2})(a - b\sqrt{2})$. Hvorfor er produktet ikke lig 0? Er det et rationalt tal?)

[3] Man kan naturligvis altid omdøbe elementerne i et fuldstændigt ordnet legeme og derved få en anden mængde. Men strukturen forbliver den samme. Man siger at de to ordnere mængder er isomorfe. Isomorfibegrebet vil blive forklaret på jeres senere algebrakurser.

Kapitel 9

Restklasser og modulær aritmetik

I dette kapitel skal vi indføre nogle meget vigtige ringe og legemer. I vil få brug for dem i jeres senere kurser og i dette kursus vil de blive brugt som vigtige eksempler på ækvivalensklasser, som vil blive introduceret generelt i et senere kapitel.

Definition 316 *Lad $n \in \mathbb{N}$ og lad $a, b \in \mathbb{Z}$. Vi siger da, at a er **kongruent** med b modulo n, og vi skriver $a \equiv b \pmod{n}$ hvis $n \mid (a-b)$.*

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b) \tag{9.1}$$

Eksempel 317 *Lad os se på kongruens modulo 3. Vi vælger altså n ovefor til at være 3. Der gælder at $7 \equiv 1 \pmod{3}$, da $7-1=6$, som er divisibel med 3.*

Sætning 318 *Der gælder følgende to omskrivninger af ovenstående definition:*

1. *$a \equiv b \pmod{n}$ hvis og kun hvis der findes et $k \in \mathbb{Z}$ så $a = b + kn$.*
2. *$a \equiv b \pmod{n}$, hvis og kun hvis a og b har samme rest ved division med n.*

Bevis. Første omskrivning ses af følgende biimplikationer:

$$\begin{aligned} a \equiv b \pmod{n} &\Leftrightarrow n \mid (a-b) \\ &\Leftrightarrow \exists k \in \mathbb{Z} : nk = (a-b) \Leftrightarrow \exists k \in \mathbb{Z} : a = b + kn. \end{aligned}$$

For at vise den anden omskrivning antager vi at a og b har resterne henholdsvis r_1 og r_2 ved division med n. Det vil sige at der findes hele tal k_1 og k_2 så at

$$a = k_1 n + r_1 \quad \text{og} \quad b = k_2 n + r_2.$$

Omskrivningen følger da af følgende række biimplikationer:

$$\begin{aligned} & a \equiv b \pmod{n} \\ & \Leftrightarrow k_1 n + r_1 \equiv k_2 n + r_2 \pmod{n} \\ & \Leftrightarrow n \mid ((k_1 n + r_1) - (k_2 n + r_2)) \\ & \Leftrightarrow n \mid ((k_1 - k_2)n + (r_1 - r_2)) \\ & \Leftrightarrow n \mid (r_1 - r_2) \\ & \Leftrightarrow r_1 - r_2 = 0 \\ & \Leftrightarrow r_1 = r_2 \end{aligned}$$

Den næstsidste biimplikation følger af at $(r_1 - r_2)$ er et tal mellem 0 og $n-1$, og det eneste sådanne tal, som n går op i er 0. ■

Sætning 319 *Lad $n \in \mathbb{N}$. Da har relationen $a \equiv b \pmod{n}$ følgende fundamentale egenskaber for alle hele tal a, b, c:*

1. *$a \equiv a \pmod{n}$ (man siger ar relationen er **refleksiv**)*
2. *Hvis $a \equiv b \pmod{n}$, så gælder også at $b \equiv a \pmod{n}$ (man siger at relationen er **symmetrisk**)*
3. *Hvis $a \equiv b \pmod{n}$ og $b \equiv c \pmod{n}$ da gælder at $a \equiv c \pmod{n}$ (man siger at relationen er **transitiv**)*

Bevis. Refleksivitet og symmetri overlades til læseren.

Transitivitet: Antag at $a \equiv b \pmod{n}$, og at $b \equiv c \pmod{n}$. Det vil sige at $n \mid (a-b)$ og $n \mid (b-c)$. Men da

$$a - c = (a - b) + (b - c)\,, \tag{9.2}$$

medfører det at $n \mid (a-c)$, altså at $a \equiv c \pmod{n}$. ■

Eksempel 320 *Lad os igen se på kongruen modulo 3. Hvilke tal er da kongruente med 1 modulo 3? Ifølge ovenstående er det alle tal som har rest 1 ved division med 3, dvs $1, 4, 7, 10, \ldots$ samt $-2, -5, -8, \ldots$ De ligger altså på talaksen med afstand 3 mellem hinanden, begyndende i 1. Mængden af disse tal, altså mængden $\{\ldots -8, -5, -2, 1, 4, 7, 10, \ldots\} = \{1 + 3k \mid k \in \mathbb{Z}\}$ kaldes restklassen 1 modulo 3 og betegnes med $[1]_3$. Mere generelt defineres:*

Definition 321 *Givet et naturligt tal n og et helt tal a. Mængden af hele tal, som har samme rest som a ved division med n kaldes a's **restklasse** modulo n. Den betegnes $[a]_n$:*

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\} = \{a + nk \mid k \in \mathbb{Z}\} \tag{9.3}$$

$$= \{\ldots, a - 3n, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \ldots\} \tag{9.4}$$

Når det er klart hvilken værdi n har, skriver man ofte $[a]$ i stedet for $[a]_n$.

Sætning 322 *Lad $n \in \mathbb{N}$ og $a, a' \in \mathbb{Z}$. Da gælder:*

$$a \equiv a' \ (mod\ n) \Leftrightarrow a' \in [a]_n \Leftrightarrow [a']_n = [a]_n$$

Bevis. Den første biimplikation er definitionen af $[a]_n$.

Den anden biimplikation vises i to skridt.

Først vises "$\Leftarrow$": Antag derfor at $[a']_n = [a]_n$. Fra definitionen af $[a']_n$ er det klart at $a' \in [a']_n$ så da $[a']_n = [a]_n$ kan vi slutte at $a' \in [a]_n$

Dernæst vises "$\Rightarrow$": Antag nu at $a' \in [a]_n$. Vi skal vise at $[a']_n = [a]_n$.

Først viser vi at $[a']_n \subseteq [a]_n$. Antag derfor at $x \in [a']_n$. Per definition af $[a']_n$ betyder det at $x \equiv a'$ (mod n). Da $a' \in [a]_n$ vil endvidere $a' \equiv a$ (mod n), så fra transitiviteten kan vi slutte at $x \equiv a'$ (mod n), hvorfor $x \in [a]_n$.

Dernæst viser vi at $[a]_n \subseteq [a']_n$. Antag derfor at $x \in [a]_n$. Per definition af $[a]_n$ betyder det at $x \equiv a$ (mod n). Da $a' \in [a]_n$ vil endvidere $a' \equiv a$ (mod n) og derfor pr. symmetri $a \equiv a'$ (mod n). Transitiviteten giver derfor at $x \equiv a'$ (mod n), hvorfor $x \in [a']_n$. ■

Definition 323 *Et element i en restklasse kaldes* ***en repræsentant for restklassen.***

Bemærkning 324 *Grunden til denne sprogbrug er at ethvert element a i en restklasse repræsenterer restklassen i den forstand at restklassen kan skrives $[a]_n$. Det følger af Sætning 322.*

Definition 325 *Mængden af restklasser (mod n) benævnes $\mathbb{Z}/n$ (udtales Z modulo n) (Man bruger også betegnelsen $\mathbb{Z}_n$ og $\mathbb{Z}/\mathbb{Z}n$ for denne mængde).*

Eksempel 326 *$\mathbb{Z}/3$ består af tre restklasser nemlig*

$$[0]_3 = \{..., -6, -3, 0, 3, 6, ...\} \tag{9.5}$$
$$[1]_3 = \{..., -5, -2, 1, 4, 7, ...\} \tag{9.6}$$
$$[2]_3 = \{..., -7, -4, -1, 2.4, ...\}. \tag{9.7}$$

Hver restklasse repræsenteres af ethvert af sine elementer, så for eksempel:

$$[-5]_3 = [-2]_3 = [1]_3 = [4]_3 = [7]_3. \tag{9.8}$$

For overskuelighedens skyld vælger man ofte den mindste ikke-negative repræsentant for en restklasse, så man snarere skriver $[1]_3$ end $[1003]_3$, selv om de to symboler betyder den samme restklasse.

Sætning 327 *$\mathbb{Z}/n$ har n elementer nemlig $[0], [1], [2], ..., [n-1]$. Hvert af disse elementer er en mængde af hele tal.*

Eksempel 328 *Mængden af restklasser $\mathbb{Z}/24$ er god at bruge, når man angiver klokkeslæt. To timer efter klokken 23 plejer vi ikke at sige, at klokken er 25, men at den er 1. Men $1 \equiv 25$ (modulo 24) så de to klokkeslæt er ækvivalente. Sagt anderledes: $[25] = [1]$ i $\mathbb{Z}/24$. Det er altså praktisk at opfatte (hele) klokkeslæt som restklasser i $\mathbb{Z}/24$ snarere end som hele tal.*

Eksempel 329 *På samme måde er det praktisk at opfatte vinkelmål angivet i grader, som restklasser modulo* 360*.*

Bemærkning 330 *Når man regner med vinkler, kan man tillade sig at sige at* $270^\circ + 270^\circ = 180^\circ$*, fordi* $270 + 270 = 540$ *og* $540 \equiv 180$ *(mod* 360*). Vi regner altså som om to vinkler er "ens" når de er ækvivalente modulo* 360*. Ligeså regner vi også modulo* 24 *(eller* 12*) når vi regner på klokkeslæt). Et matematisk mere tilfredsstillende synspunkt er at regne med restklasserne. Vi skal nu vise at det er muligt at indføre addition og multiplikation på mængden af restklasser modulo* n*.*

Definition 331 *Lad* $n \in \mathbb{N}$*. Vi definerer da addition* $+$*, og multiplikation* $\cdot$ *af to restklasser* $[a], [b] \in \mathbb{Z}/n$ *ved*

$$[a] + [b] = [a + b] \tag{9.9}$$

$$[a] \cdot [b] = [a \cdot b] \tag{9.10}$$

Bemærkning 332 *Vi definerer altså addition og multiplikation af to restklasser ud fra addition og multiplikation af to repræsentanter for restklasserne. For at disse definitioner skal give mening må vi godtgøre, at resultatet ikke afhænger af valget af repræsentant. I så fald siger vi at definitionerne af kompositionsreglerne er* ***veldefineret.*** *Vi skal altså vise følgende sætning:*

Sætning 333 *Lad* $n \in \mathbb{N}$*. Hvis* $[a_1], [a_2], [b_1], [b_2] \in \mathbb{Z}/n$ *og* $[a_1] = [a_2]$ *og* $[b_1] = [b_2]$ *da er* $[a_1 + b_1] = [a_2 + b_2]$ *og* $[a_1 \cdot b_1] = [a_2 \cdot b_2]$*.*

Bevis. Vi viser blot at addition er repræsentantuafhængig; multiplikation går på samme vis.

Antag altså at

$$[a_1] = [a_2] \text{ og } [b_1] = [b_2], \tag{9.11}$$

dvs. iflg. 382 at

$$a_1 \equiv a_2 \pmod{n} \text{ og } b_1 \equiv b_2 \pmod{n}. \tag{9.12}$$

Pr. definition 346 8. betyder det, at

$$n \mid (a_1 - a_2) \text{ og } n \mid (b_1 - b_2), \tag{9.13}$$

hvorfor der findes hele tal m, l så

$$a_1 - a_2 = nm \text{ og } b_1 - b_2 = nl \tag{9.14}$$

eller

$$a_1 = a_2 + nm \text{ og } b_1 = b_2 + nl. \tag{9.15}$$

Men så ser vi, at

$$a_1 + b_1 = a_2 + nm + b_2 + nl = a_2 + b_2 + n(m + l). \tag{9.16}$$

Da nu $m + l$ er et helt tal, slutter vi heraf, at

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n}, \tag{9.17}$$

eller

$$[a_1 + b_1] = [a_2 + b_2]. \tag{9.18}$$

■

Eksempel 334 *Betragt restklasserne modulo 360. Der gælder* $[195] + [341] = [176]$ *(vis dette). Det betyder, at hvis et hjul først drejer* $195°$ *og dernæst* $341°$ *i samme retning, vil det indtage samme stilling, som hvis det bare havde drejet* $176°$*.*

Øvelse 335 *Hvad er klokken* 127 *timer efter kl.* 15*? Udtryk dine overvejelser som et regnestykke med restklasser.*

Sætning 336 *Lad* $n \in \mathbb{N}$*. Addition og multiplikation på* $\mathbb{Z}/n$ *er kommutative og associative og der gælder den distributive lov*

$$[a]([b] + [c]) = [a][b] + [a][c] \tag{9.19}$$

.

Bevis. Vi beviser at addition er associativ. Resten af beviset overlades til læseren.

Lad $[a], [b], [c] \in \mathbb{Z}/n$. På grund af den associative lov for addition på $\mathbb{Z}$ og definitionen af addition på $\mathbb{Z}/n$ gælder da:

$$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] \tag{9.20}$$

$$= [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c]). \tag{9.21}$$

■

Sætning 337 *Lad* $n \in \mathbb{N}$*. I* $\mathbb{Z}/n$ *gælder at*

- $[0]$ *er neutralt element for addition, og* $[1]$ *er neutralt element for multiplikation,*
- $[-a]$ *er det additivt inverse element til* $[a]$*.*

Bevis. Overlades til læseren. ■

Sætning 338 *Lad* $n \in \mathbb{N}$*. I* $\mathbb{Z}/n$ *gælder at:*

$[a]$ *har en multiplikativ invers* $\Leftrightarrow$ *a og n er indbyrdes primiske.* (9.22)

Bevis. Ifølge korollar 140 har vi følgende kæde af biimplikationer:

$$
\begin{aligned}
&[a] \text{ har en multiplikativ invers} && (9.23)\\
&\Leftrightarrow \exists m \in \mathbb{Z} : [a]\,[m] = [1] && (9.24)\\
&\Leftrightarrow \exists m \in \mathbb{Z} : [am] = [1] && (9.25)\\
&\Leftrightarrow \exists m, k \in \mathbb{Z} : am + nk = 1 && (9.26)\\
&\Leftrightarrow a \text{ og } n \text{ er indbyrdes primiske.} && (9.27)
\end{aligned}
$$

■

Bemærkning 339 *Af ovenstående bevis fremgår det at for at bestemme den multiplikative inverse til* $[a]$ *skal man bestemme hele tal* m *og* k *så*

$$am + nk = 1 \tag{9.28}$$

Hvis man har fundet sådanne hele tal er $[m] = [a]^{-1}$. *Sætning 137 og det efterfølgende eksempel viser hvordan man ved hjælp af Euklids algoritme kan bestemme sådanne* m *og* k, *når* $(a, n) = 1$. *Man kan altså bruge Euklids algoritme til at bestemme den multiplikative inverse til* $[a]$ *når* $(a, n) = 1$, *altså specielt hvis* n *er et primtal.*

Sætning 340 *Lad* $n \in \mathbb{N}$.

1. *Hvis* n *er et primtal har alle elementerne i* $\mathbb{Z}/n$ *på nær* $[0]$ *multiplikative inverse.*

2. *Hvis* n *er et sammensat tal findes der i* $\mathbb{Z}/n$ *andre elementer end* $[0]$, *som ikke har en multiplikativ invers.*

Bevis. 1. Hvis $[a] \neq [0]$, er a ikke et multiplum af n, og da n er et primtal, er a derfor indbyrdes primisk med n. Ifølge sætning 338 har $[a]$ derfor en multiplikativ invers.

2. Hvis n er et sammensat tal, har n en divisor a så $1 < a < n$. Da er $[a] \neq [0]$ og a er ikke indbyrdes primisk med n så ifølge sætning 338 har $[a]$ ingen multiplikativ invers. ■

Øvelse 341 *Bestem den multiplikativt inverse til alle elementerne i* $\mathbb{Z}/5$ *på nær* $[0]$.

Hvilke elementer i $\mathbb{Z}/6$ *har multiplikativt inverse?*

Vi kan sammenfatte de foregående sætninger i følgende sætning:

Sætning 342 *Lad* $n \in \mathbb{N}$.

1. $(\mathbb{Z}/n, +, \cdot)$ *er en ring med additivt neutralelement* $[0]_n$ *og multiplikativt neutralelement* $[1]_n$.

2. $(\mathbb{Z}/n, +, \cdot)$ *et legeme, hvis og kun hvis* n *er et primtal.*

Bemærkning 343 *Hvis* p *er et primtal er* $\mathbb{Z}/n$ *altså et legeme. I lighed med de komplekse tal kan* $\mathbb{Z}/n$ *ikke ordnes som et ordnet legeme. Vi kan altså regne med restklasser ganske som vi regner med reelle tal, så længe vi ikke bruger ordningen. Det kan vises at hvis* n *er en potens af et primtal, så findes et legeme med* n *elementer. Hvis* n *ikke er en potens af et primtal, findes derimod ingen legemer med* n *elementer. Og på nær omdøbning (isomorfi) er de endelige legemer entydigt bestemt ved antallet af deres elementer.*

Bemærkning 344 *Vi bruger potensnotation for restklasser, ligesom for reelle tal. Således betyder* $[a]_n^m$ *den restklasse, der fremkommer ved at gange* $[a]_n$ *med sig selv* m *gange.*

Eksempel 345 *Find det sidste ciffer i* 3^{100}*. Det svarer jo til at udregne den mindste ikke-negative repræsentant for* $\left[3^{100}\right]_{10}$ *eller* $[3]_{10}^{100}$*. Her er det ikke smart at udregne* 3^{100}*. I stedet bruger vi det frie valg af repræsentant ved regning med restklasser: Vi bemærker nemlig at* $[3]_{10}^{100} = [3]_{10}^{2\cdot 50} = \left([3]_{10}^2\right)^{50} = \left(\left[3^2\right]_{10}\right)^{50} = [9]_{10}^{50}$*. Nu er det smart at bruge repræsentanten* -1 *for restklassen* $[9]_{10}$ *for så bliver udregningerne simple:* $[9]_{10}^{50} = [-1]_{10}^{50} = \left[(-1)^{50}\right]_{10} = [1]_{10}$*. Dermed har vi på simpel vis udregnet, at det sidste ciffer i* 3^{100} *er* 1*. Vi bemærker at det i dette tilfælde var smartest at regne med den numerisk mindste repræsentant, i stedet for den mindste positive repræsentant. Det sker ofte.*

9.1 Opgaver

1. Hvad er klokken 10.000 timer efter kl. 16? Hvad er klokken 550 minutter efter kl. 22.15?

2. Bestem følgende restklasser i $\mathbb{Z}/n$ opskrevet som $[k]_n$ hvor $0 \leq k < n$:
(a) $[7]_5 \cdot [4]_5$.
(b) $[6]_7 \cdot [4]_7$.
(c) $([n-1]_n)^2$
(d) $([3]_8)^{1000}$.

Kapitel 10

Relationer. Ækvivalensrelationer

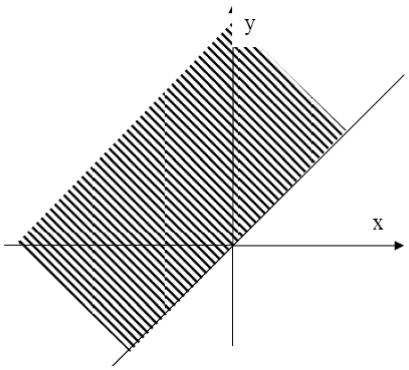
10.1 Relationer generelt

Eksempel 346 *For at give et indtryk af hvad man mener med en relation, skal vi give nogle eksempler:*

1. *"Person p har besøgt land l" er en relation mellem mængden af personer og mængden af lande.*
2. *"p_1 har samme efternavn som p_2" er en relation på mængden af mennesker.*
3. *"Trekant T har areal A" er en relation mellem mængden af trekanter og $\mathbb{R}_+$.*
4. *"$x \leq y$" er en relation på $\mathbb{R}$.*
5. *"$x = y$" er en relation på enhver mængde A.*
6. *"n går op i m", som også skrives "$n \mid m$", er en relation på $\mathbb{N}$.*
7. *"$A \subseteq B$" er en relation på $P(U)$.*
8. *"$a \equiv b \pmod{n}$" (for givet $n \in \mathbb{N}$) er en relation på $\mathbb{Z}$.*

Mere generelt definerer et prædikat $p(x, y)$ i de to frie variable $x \in A$ og $y \in B$ en relation mellem A og B, idet vi siger at x er relateret til y, hvis $p(x, y)$ er sand. Vi kan identificere en relation mellem A og B med en delmængde R af $A \times B$ nemlig mængden af de ordnede par (x, y), for hvilke x er relateret til y. Denne mængde er sandhedsmængden for $p(x, y)$ og kaldes også relationens graf.

Betragt for eksempel relationen $\leq$ mellem $\mathbb{R}$ og $\mathbb{R}$. Vi kan på sædvanlig vis illustrere $\mathbb{R}^2$ ved den cartesiske plan. Grafen for relationen $\leq$ er da den skraverede mængde på figuren 10.1



Figur 10.1: Grafen for relationen $\leq$

Den ovenstående beskrivelse indfanger den intuitive betydning af en relation. For at føre begrebet tilbage til de fundamentale begreber i mængdelæren vælger man dog at *definere* en relation ud fra grafen, altså som en delmængde af en produktmængde:

Definition 347 *Lad A og B være mængder. En delmængde R af $A \times B$ kaldes en* ***relation*** *mellem A og B. A kaldes* ***primærmængden*** *og B kaldes* ***sekundærmængden****. En delmængde af $A \times A$ kaldes en relation på A.*

Hvis $(x, y) \in R$ siger man at x er relateret til y, og man skriver xRy.

Bemærkning 348 *Selv om vi således formelt definerer en relation som en mængde, bruger vi normalt ikke mængdelærens sprog, når vi taler om relationer. For eksempel vil man ikke skrive $(< \cup =) = \leq$. Man vil i stedet skrive: $((x < y) \vee (x = y)) \Leftrightarrow x \leq y$.*

Notation 349 *Ofte vælger man andre betegnelser for relationer end xRy. I eksempel 4 ovenfor skriver man naturligvis $x \leq y$. Notationen $x \sim y$ bruges også ofte for en generel relation, men i denne bog skal vi fortrinsvis bruge denne notation om de såkaldte ækvivalensrelationer (se nedenfor).*

Definition 350 *En relation R på en mængde A siges at være*

- ***refleksiv****, hvis $\forall x \in A : xRx$*
- ***irrefleksiv****, hvis $\forall x \in A : \neg xRx$*
- ***symmetrisk****, hvis $xRy \Rightarrow yRx$*
- ***antisymmetrisk****, hvis $((xRy) \wedge (yRx)) \Rightarrow x = y$*
- ***transitiv****, hvis $(xRy) \wedge (yRz) \Rightarrow (xRz)$*

Eksempel 351 *Lad os undersøge om eksemplerne i 346 er refleksive, symmetriske, antisymmetriske og/eller transitive. Disse egenskaber er kun defineret for relationer, hvor primærmængden er lig sekundærmængden, hvilket udelukker eksempel 1 og 3.*

Relationerne i eksempel 2 og 8 er refleksive, symmetriske og transitive.

Relationerne i eksempel 4, 6 og 7 er refleksive, antisymmetriske og transitive.

Relationen i eksempel 5 er refleksiv, symmetrisk, antisymmetrisk og transitiv.

Øvelse 352 *Overvej at det forholder sig som påstået i eksempel 351.*

Eksempel 353 *I geometri betyder = mellem linjestykker ikke at linjestykkerne er identiske, men derimod at de er lige store. Denne lighedsrelation er transitiv.*

Definition 354 *Lad R være en relation mellem A og B, og lad $A_1 \subseteq A$. Da defineres* ***den til*** A_1 ***relaterede delmængde af*** B *som mængden af de elementer i B, som er relateret til et element i A_1 :*

$$R(A_1) = \{b \in B \mid \exists a \in A_1 : aRb\} \tag{10.1}$$

Hvis A_1 består af ét element $A_1 = \{a_1\}$, skriver man $R(a_1)$ i stedet for $R(\{a_1\})$.

Øvelse 355 *Bestem $R(a)$ når R er relationerne i eksempel 346 og a er "dig" i 1. og 2.; a er en retvinklet trekant med kateter 1 i 3.; $a = 5$ i 4.,5.,6. og 8.; og a er de positive reelle tal som delmængde af $U = \mathbb{R}$ i 7.*

Definition 356 *Lad R være en relation mellem A og B. Da defineres relationen R^{-1} mellem B og A ved*

$$bR^{-1}a \overset{def}{\Leftrightarrow} aRb. \tag{10.2}$$

R^{-1} kaldes den ***inverse relation*** *til R.*

Øvelse 357 *Bestem den inverse til relationerne i eksempel 346*

Bemærkning 358 *Lad R være en relation mellem A og B. Ifølge definition 354 og 356 har vi når $B_1 \subseteq B$ at*

$$R^{-1}(B_1) = \left\{a \in A \mid \exists b \in B_1 : bR^{-1}a\right\} = \{a \in A \mid \exists b \in B_1 : aRb\} \tag{10.3}$$

Øvelse 359 *Bestem $R^{-1}(30)$ når R er relationen i eksempel 346 6, og $R^{-1}(\{1,2,3\})$ når R er relationen defineret i eksempel 346 7.*

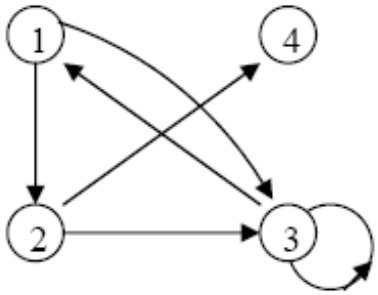
Vi skal i det følgende betragte to særligt vigtige slags relationer, nemlig ækvivalensrelationer og ordningsrelationer. Ordningsrelationer betragtes i et senere kapitel, medens ækvivalensrelationer behandles i dette kapitel. Men først skal vi se på en god måde at visualisere relationer.

10.2 Orienterede grafer

Hvis mængden A er endelig, kan vi illustrere er relation R på A på følgende måde: Tegn en lille cirkel for hvert element i A, og skriv elementets navn i cirklen. En sådan cirkel kaldes en **knude**. Tegn derefter en pil, kaldet en **(orienteret) kant**, fra knude a til knude b hvis aRb. Den resulterende illustration kaldes relationens **orienterede graf** eller **digraf** (directed graph på engelsk).

Bemærkning 360 *Man identificerer ofte elementerne i A med knuderne i den orienterede graf og identificerer de orienterede kanter i grafen med elementparrene i relationen. Man kalder således ofte elementerne i A for knuder og betegner normalt kanten fra a til b med (a, b).*

Eksempel 361 *I figur 10.2 er tegnet den orienterede graf for følgende relation på $\{1, 2, 3, 4\}$: $R = \{(1, 2), (1, 3), (2, 3), (2, 4), (3, 1), (3, 3)\}$*

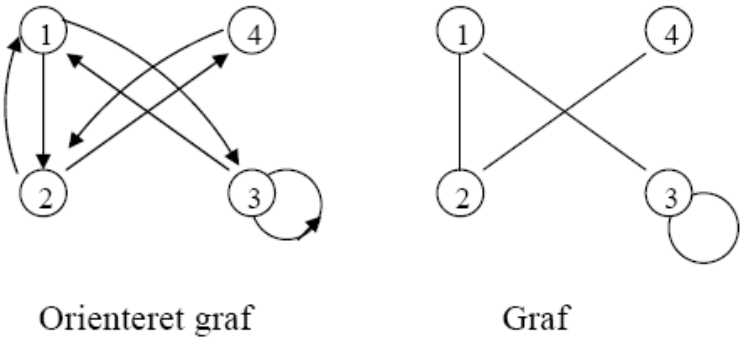


Figur 10.2: Digraf for relationen $\{(1, 2), (1, 3), (2, 3), (2, 4), (3, 1), (3, 3)\}$

Bemærkning 362 *Vi bemærker at en kant kan gå fra en knude tilbage til samme knude. I det tilfælde kalder man kanten for en **løkke**. Det kan også ske at der mellem to knuder går to kanter orienteret hver sin vej. I så fald taler vi om et **kantpar**. Bemærk også at en løkke kan opfattes som værende orienteret i begge retninger.*

Bemærkning 363 *Man kan aflæse visse egenskaber ved en relation direkte fra dens orienterede graf:*

1. *En relation er refleksiv hvis og kun hvis hver knude i dens orienterede graf er forsynet med en løkke.*
2. *En relation er irrefleksiv, hvis og kun hvis dens orienterede graf ikke har nogen løkker.*



Figur 10.3: Orienteret graf og graf for relation

3. *En relation er symmetrisk, hvis og kun kanterne i digrafen alle kommer som kantpar, altså: hvis en kant er med i grafen, så er den modsat orienterede kant også med i grafen.*

4. *En relation er transitiv, hvis og kun hvis dens orienterede graf har følgende egenskab: Hvis to orienterede kanter (a,b) og (b,c), hvor den første ender hvor den anden begynder, er kanter i R's orienterede graf, da er den orienterede kant (a,c) også en kant i R's orienterede graf. Der er altså ingen ufuldendte trekanter i grafen*

Bemærkning 364 *Hvis en relation er symmetrisk, kommer alle kanterne i dens orienterede graf altså i par. Man vælger da ofte at repræsentere kantparret ved en ikke orienteret kant uden pil. Den konfiguration, som derved fremkommer kaldes en graf. I kapitel 14 vil vi komme tilbage til teorien for grafer.*

Eksempel 365 *På figur 10.3 er tegnet digrafen og grafen for den symmetriske relation* $R = \{(1,2),(2,1),(2,4),(4,2),(1,3),(3,1),(3,3)\}$ *på* $\{1,2,3,4\}$.

Bemærkning 366 *Lad R være en relation på A. Den orienterede graf for relationen R^{-1} fås fra den orienterede graf for relationen R ved at vende alle pilene.*

Definition 367 *Lad R være en relation på mængden A og lad $a,b \in A$. En* ***rute*** *i R af længde $n \in \mathbb{N}$ fra a til b er en endelig følge $(a = a_0, a_1, a_2, ..., a_n = b)$ af ikke nødvendigvis forskellige elementer fra A så*

$$aRa_1, a_1Ra_2, ..., a_{n-1}Rb. \tag{10.4}$$

Vi siger, at ruten går fra a til b og vedtager, at der fra ethvert element går en rute af længde 0 til elementet selv.

Bemærkning 368 *I relationens orienterede graf repræsenteres en rute fra a til b af en følge af pile, som begynder i a og ender i b. Hvis der er n pile i følgen er den af længde n.*

Eksempel 369 *Betragt relationen illustreret med den orienterede graf i figur 10.2*

1. *I denne relation er der en rute fra* 2 *til* 4 *af længde* 1 *nemlig* $(2, 4)$*. Fra* 2 *til* 4 *er der også en rute af længde* 4 *nemlig* $(2, 3, 1, 2, 4)$*, og ruter af alle længder større eller lig med* 4*. For eksempel er ruten* $(2, 3, 3, 3, 1, 2, 4)$ *af længde* 6*. Her kører vi rundt i løkken ved* 3 *to gange .*

2. *Fra* 1 *til* 2 *er en rute af enhver længde på nær* 2 *(overvej dette).*

Definition 370 *Lad R være en relation på mængden A og lad n være et ikke negativt helt tal. Da defineres relationerne* R^n *og* R^∞ *på A på følgende måde: Lad* $a, b \in A$

- $aR^n b$ *hvis der findes en rute i R af længde n mellem a og b.*
- $aR^\infty b$ *hvis der findes en rute i R af en eller anden længde mellem a og b.*

Eksempel 371 *Lad A betegne mængden af byer i verden, og lad aRb, hvis der går et direkte fly fra a til b. Da gælder* $aR^n b$*, hvis det er muligt at flyve fra a til b med præcist* $n-1$ *mellemlandinger, og* $aR^\infty b$*, hvis det er muligt at komme fra a til b med fly.* $R^n(a)$ *betegner mængden af byer, som kan nås med fly fra a med præcist* $n-1$ *mellemlandinger.*

10.3 Ækvivalensrelationer

I matematik er man ofte i den situation, at forskellige objekter kan anses for ens i en vis forstand. For eksempel anser Euklid to linjestykker for ens, hvis de er lige lange. Ligeså, når man angiver vinkelmål i grader, vil man anse en vinkel på $270°$ for "den samme" vinkel som en på $-90°$. Mere generelt vil to vinkler på $a°$og $b°$ anses for "den samme" vinkel hvis $a-b$ er delelig med 360, eller sagt anderledes, at $a \equiv b \pmod{360}$. Man kan sige, at de to vinkler er ækvivalente. Denne ide om ækvivalens indfanges af begrebet en ækvivalensrelation.

Der er tradition for at man betegner ækvivalensrelationer med $\sim$ i stedet for R. Derfor skal vi i dette afsnit skrive $x \sim y$ i stedet for xRy.

Definition 372 *En relation* $\sim$ *på en mængde A kaldes en* ***ækvivalensrelation****, hvis den er refleksiv, symmetrisk og transitiv, altså hvis*

- *Refleksivitet:* $\forall x \in A : x \sim x$
- *Symmetri:* $x \sim y \Rightarrow y \sim x$
- *Transitivitet:* $(x \sim y) \wedge (y \sim z) \Rightarrow x \sim z$

Eksempel 373 *I eksempel 346 er 2.,5. og 8. de eneste ækvivalensrelationer.*

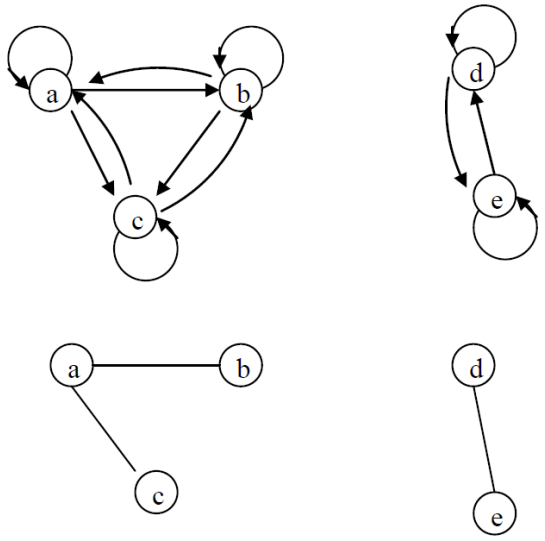
Øvelse 374 *Hvilke af nedenstående relationer er ækvivalensrelationer:*

1. *Relationen på $\mathbb{R}$ defineret ved: $x \cdot y \geq 0$*
2. *Relationen $\neq$ defineret på $\mathbb{R}$.*
3. *Relationen på mængden af rette linjer i planen defineret ved $l \sim m$, hvis (l er parallel med m eller $l = m$).*
4. *Relationen "l står vinkelret på m" defineret på mængden af rette linjer i planen.*
5. *Relationen på mængden af rette linjer i planen defineret ved $l \sim m$, hvis l og m har et fælles punkt.*
6. *Relationen på mængden af orienterede linjestykker $\overline{AB}$ (pile fra A til B) i planen defineret ved $\overline{AB} \sim \overline{CD}$ hvis $\overline{AB}$ og $\overline{CD}$ er ensrettede og lige lange.*

Bemærkning 375 *Den orienterede graf hørende til en ækvivalensrelation på en endelig mængde har løkker ved alle knuder, alle kanterne er kantpar, og når den indeholder en kant fra a til b og en kant fra b videre til c, da har den også en kant fra a til c. Denne orienterede graf giver et unødvendigt kompliceret billede af relationen. Hvis det udtrykkeligt er klart at en relation er en ækvivalensrelation, kan man jo udelade løkkerne og slå kanterne sammen, så relationen repræsenteres ved en graf. Det er det vi i et senere kapitel vil kalde en simpel graf. Desuden kan man vælge at udelade en række kanter. Hvis der er en kant fra a til b og en kant fra b videre til c, da ved vi jo at kanten fra a til c også tilhører grafen. Men så kan vi jo udelade den. Hvis vi på denne måde udelader alle de unødvendige kanter, får vi det, der kaldes den udspændende skov. Den er karakteriseret ved at der i denne graf er en rute fra a til b, hvis og kun hvis $a \sim b$. Vi vender tilbage til disse grafteoretiske begreber i næste kapitel.*

Øvelse 376 *Vis at hvis R er en ækvivalensrelation på A da gælder for alle $n \in \mathbb{N}$: $aR^n b \Leftrightarrow aRb$. Du kan bevise $\Rightarrow$ ved induktion efter n.*

En ækvivalensrelation på en mængde deler mængden op i delmængder bestående af elementer, som er indbyrdes ækvivalente. For eksempel deler ækvivalensrelationen 2. i eksempel 346 mennesker op i delmængder bestående af personer med samme efternavn. Ækvivalensrelationen "samme køn som" på mængden af mennesker deler menneskeheden op i kvinder og mænd. Ækvivalensrelationen "går på hold med" deler mængden af DisMat-studerende op i hold. Ækvivalensrelationen "$a \equiv b \pmod{n}$" (for givet $n \in \mathbb{N}$) deler de hele tal op i restklasser. Den følgende generelle definition er inspireret af definitionen af restklasser.



Figur 10.4: Øverst: Orienteret graf for en ækvivalensrelation. Nederst: dens udspændende skov.

Definition 377 *Lad $\sim$ være en ækvivalensrelation på mængden A. Hvis $a \in A$, betegner $[a]$ mængden af de elementer i A, som er ækvivalente med a, med andre ord*

$$[a] = \{x \in A \mid x \sim a\}\,. \tag{10.5}$$

*$[a]$ kaldes den til a hørende **ækvivalensklasse**. Hvis man eksplicit vil angive at ækvivalensklassen $[a]$ hører til relationen $\sim$ kan man skrive $[a]_\sim$*

Mængden af ækvivalensklasser betegnes $A/\sim$

Bemærkning 378 *I definition 354 brugte vi betegnelsen $\sim(a)$ for $[a]_\sim$. Når der er tale om ækvivalensrelationer er betegnelsen $[a]_\sim$ mere almindelig.*

Eksempel 379 *Betragt ækvivalensrelationen "samme køn" på mængden af mennesker. Da er [Mette Hansen] lig mængden af kvinder.*

Eksempel 380 *Den i Øvelse 374 eksempel 6 definerede relation er en ækvivalensrelation. Dens ækvivalensklasser kaldes vektorer i planen. Ækvivalensklassen $\left[\overline{AB}\right]$ betegnes også $\overrightarrow{AB}$.*

Eksempel 381 *Ækvivalensklasserne hørende til ækvivalensrelationen "$a \equiv b \pmod n$" på $\mathbb{Z}$ er netop restklasserne defineret i foregående kapitel. De følgende sætninger er generalisationer til vilkårlige ækvivalensrelationer og -klasser af sætninger vi tidligere har bevist for restklasser.*

Sætning 382 *Lad $\sim$ være en ækvivalensrelation på mængden A, og lad $a, b \in A$. Da gælder at*

$$[a] = [b]\,, \tag{10.6}$$

hvis og kun hvis

$$a \sim b. \tag{10.7}$$

Bevis. Først vises, at $a \sim b \Rightarrow [a] = [b]$. Antag altså, at $a \sim b$. Vi skal vise, at $[a] = [b]$. Først viser vi, at $[a] \subseteq [b]$. Lad derfor $c \in [a]$. Det betyder pr. definition 377 at $c \sim a$. Og da vi havde antaget, at $a \sim b$ følger af transitiviteten, at $c \sim b$, hvoraf vi slutter, at $c \in [b]$. Altså gælder $[a] \subseteq [b]$. Dernæst skal det vises, at $[b] \subseteq [a]$. Det kan gøres helt som ovenfor. Man kan også bemærke at symmetrien medfører at $b \sim a$ hvorved inklusionen $[b] \subseteq [a]$ følger, af det netop gennemførte argument.

Dernæst vises at $[a] = [b] \Rightarrow a \sim b$. Antag altså, at $[a] = [b]$, og vi vil vise at $a \sim b$. Da relationen er refleksiv, ved vi, at $a \sim a$. Det betyder, at $a \in [a]$. Da $[a] = [b]$, har vi også, at $a \in [b]$. Men det betyder pr. definition, at $a \sim b$. ■

Korollar 383 *Lad $\sim$ være en ækvivalensrelation på mængden A, og lad $a, b \in A$. Da gælder at*

$$a \in [b] \Leftrightarrow [a] = [b] \tag{10.8}$$

Bevis. Under de angivne forudsætninger gælder følgende biimplikationer:

$$a \in [b] \Leftrightarrow a \sim b \Leftrightarrow [a] = [b] \tag{10.9}$$

Den første biimplikation skyldes definitionen af $[b]$, og den sidste er sætning 382. ■

Det følger af korollaret, at hvis a ligger i en ækvivalensklasse, så kan denne ækvivalensklasse betegnes med $[a]$. Vi kalder derfor ethvert element i en ækvivalensklasse for en **repræsentant** for ækvivalensklassen.

For at få en god forståelse af ækvivalensklasserne for en ækvivalensrelation indfører vi begrebet en klasseinddeling af en mængde.

Definition 384 *En familie Ω af ikke tomme delmængder af en mængde M kaldes en **klassedeling** (eller en partition) af M, hvis mængderne i Ω er parvist disjunkte, og deres foreningsmængde er hele M, med andre ord hvis*

1. *For alle mængder A og B i Ω gælder enten, at $A = B$ eller at $A \cap B = \emptyset$.*
2. $\bigcup_{A \in \Omega} A = M$

Eksempel 385 *på klassedelinger:*

1. *Opdelingen af eleverne i en skole i klasser er en klassedeling*
2. *Inddelingen af dyr i arter er en klassedeling.*
3. *Inddelingen af mennesker i mænd og kvinder er en klassedeling.*

4. Opdelingen af de hele tal i restklasser modulo $n \in \mathbb{N}$ er en klassedeling.

Vi vil nu vise to sætninger, som til sammen siger at ækvivalensrelationer og klassedelinger er to sider af samme sag. Sagt med andre ord: En ækvivalensrelation giver anledning til en klassedeling, og en klassedeling giver anledning til en ækvivalensrelation. Disse to sætninger er hovedsætningerne i dette afsnit.

Sætning 386 *Lad $\sim$ være en ækvivalensrelation på en mængde M. Da er familien af ækvivalensklasser $M/\sim$ en klassedeling af M.*

Bevis. Lad $\sim$ være en ækvivalensrelation på mængden M. Vi skal da bevise at familien af ækvivalensklasser $M/\sim$ består af ikke tomme mængder som opfylder de to definerende egenskaber i 384. Da mængden af ækvivalensklasser består af mængderne $[a]$ for $a \in M$, skal vi altså vise

0. For ethvert $a \in M$ gælder $[a] \neq \emptyset$
1. For $a, b \in M$, gælder enten $[a] = [b]$ eller $[a] \cap [b] = \emptyset$
2. $\bigcup_{a \in M} [a] = M$

Ad. 0. Da $\sim$ er refleksiv er $a \sim a$ så $a \in [a]$. Altså er $[a]$ ikke tom.

Ad.1. Lad $a, b \in M$. Vi vil vise egenskab 1, ved at vise, at hvis $[a] \cap [b] \neq \dot{\emptyset}$, så er $[a] = [b]$. Antag altså, at $[a] \cap [b] \neq \emptyset$. Så findes der et $c \in [a] \cap [b]$. Da $c \in [a]$, følger af definition 377 at $c \sim a$, og da $c \in [b]$ gælder, at $c \sim b$. Da nu $\sim$ er en ækvivalensrelation, er den specielt symmetrisk, så vi kan slutte at $a \sim c$. Og da $\sim$ også er transitiv, kan vi fra $a \sim c$ og $c \sim b$ slutte, at $a \sim b$. Sætning 382 fortæller da at $[a] = [b]$.

Ad. 2. Da enhver ækvivalensklasse pr. definition er en delmængde af M, vil $\bigcup_{a \in M} [a] \subseteq M$. Vi skal altså vise at $\bigcup_{a \in M} [a] \supseteq M$. Lad derfor $a \in M$. Da $\sim$ er refleksiv er $a \sim a$, så $a \in [a]$ (iflg. sætning 382) hvorfor $a \in \bigcup_{a \in M} [a]$ ■

Bemærkning 387 *Bemærk at vi i ovenstående bevis brugte alle de tre definerende egenskaber ved en ækvivalensrelation.*

Eksempel 388 *Mængden af restklasser modulo n er altså en klassedeling af de naturlige tal.*

Definition 389 *Lad Ω være en klassedeling af en mængde M. Vi definerer da en relation $\sim_\Omega$ på M ved:*

$a \sim_\Omega b$, hvis der findes en mængde $A \in \Omega$, så $a, b \in A$.

Sætning 390 *Lad Ω være en klassedeling af en mængde M. Da er relationen $\sim_\Omega$ defineret ovenfor en ækvivalensrelation på M.*

Bevis. Antag at Ω er en klassedeling af M. Vi skal da vise, at $\sim_\Omega$ er refleksiv, symmetrisk og transitiv.

Refleksivitet: Lad $a \in M$. Da Ω er en klassedeling af M, gælder specielt at $\bigcup_{A \in \Omega} A = M$. Altså findes der et $A \in \Omega$, så $a \in A$ (dvs. så $a, a \in A$), hvorfor $a \sim_\Omega a$ ifølge definitionen af $\sim_\Omega$.

Symmetri: Lad $a, b \in M$, og antag, at $a \sim_\Omega b$. Da findes pr. definition en mængde $A \in \Omega$, så $a, b \in A$; men så gælder jo ligeså, at $b, a \in A$, hvorfor $b \sim_\Omega a$.

Transitivitet: Lad $a, b, c \in M$, og antag at $a \sim_\Omega b$ og at $b \sim_\Omega c$. Vi skal bevise, at $a \sim_\Omega c$. Da $a \sim_\Omega b$, findes en mængde $A \in \Omega$, så $a, b \in A$, og da $b \sim_\Omega c$ findes en mængde $B \in \Omega$, så $b, c \in B$. Da $b \in A$ og $b \in B$ er $A \cap B \neq \emptyset$, men da Ω er en klassedeling, ved vi fra den første definerende egenskab, at når $A \cap B \neq \emptyset$, er $A = B$. Men så gælder, at $a \in A$ og $c \in A$, og da $A \in \Omega$ betyder det at $a \sim_\Omega c$. ■

Bemærkning 391 *Bemærk at vi i ovenstående bevis brugte begge de to definerende egenskaber ved en klassedeling.*

Eksempel 392 *Opdelingen af eleverne i en skole i klasser, giver anledning til en ækvivalensrelation mellem eleverne. To elever er relateret, hvis de går i samme klasse.*

Sætning 393

1. *Givet en ækvivalensrelation $\sim$ på en mængde M. Den giver anledning til en klassedeling $M/\sim$ af M. Denne klassedeling giver så igen anledning til en ækvivalensrelation $\sim_{M/\sim}$. Denne ækvivalensrelation er den samme som $\sim$.*

2. *Givet en klassedeling Ω af en mængde M. Den giver anledning til en ækvivalensrelation $\sim_\Omega$ på M. Denne ækvivalensrelation giver så igen anledning til en klassedeling $M/\sim_\Omega$. Denne klassedeling er den samme som Ω.*

Øvelse 394 *Bevis sætning 393*

Bemærkning 395 *Betragt ækvivalensrelationen, hvis orienterede graf er afbildet i figur 10.4. Grafen ses at bestå af to sammenhængende komponenter. Det er netop relationens ækvivalensklasser. Den udspændende skov derunder består af to træer, som er udspændende træer for ækvivalensklasserne.*

10.4 Opgaver

1. På $\mathbb{R}$ defineres relationen xRy ved

$$xRy \Leftrightarrow xy > 0 \tag{10.10}$$

Undersøg, om relationen er refleksiv, symmetrisk, antisymmetrisk eller transitiv.

Besvar samme spørgsmål, når xRy har betydningen

(a) $xy \geq 0$
(b) $xy^2 > 0$
(c) $xy^2 \geq 0$
(d) $x^2y^2 > 0$
(e) $x^2y^2 \geq 0$
(f) $x^2 - y^2 \geq 0$

2. Lad R være en symmetrisk og transitiv relation på en mængde M. Hvori består fejlen i følgende "bevis" for, at R er refleksiv:

Hvis aRb, gælder det at bRa, da R er symmetrisk. Men da R er transitiv, følger det fra aRb og bRa, at aRa. Altså er R refleksiv.

Giv et eksempel på en relation, der er symmetrisk og transitiv, men ikke refleksiv.

3. Lad P være et givet punkt i planen. Definer relationen $\sim$ på mængden af punkter i planen ved:

$$A \sim B \Leftrightarrow |PA| = |PB| \,. \tag{10.11}$$

Vis, at $\sim$ er en ækvivalensrelation, og beskriv dens ækvivalensklasser.

4. Lad F betegne mængden af reelle funktioner definerede på et interval I. På F defineres relationerne $R_1, ..., R_4$ på følgende måde:

(a) $fR_1g \dot{\Leftrightarrow} f - g$ er konstant på I

(b) $fR_2g \dot{\Leftrightarrow} f - g$ er et førstegradspolynomium

(c) $fR_3g \dot{\Leftrightarrow} f - g$ er et andengradspolynomium

(d) $fR_4g \dot{\Leftrightarrow} (f-g)(x) \neq 0$ for højst endeligt mange x i I.

Undersøg hvilke af relationerne, der er ækvivalensrelationer.

5. Lad $M = \{1, 2, 3, 4, 5, 6\}$. Betragt følgende relation på M :

$$\sim \; = \left\{ \begin{array}{c} (1,1)\,,(2,2)\,,(3,3)\,,(4,4)\,,(5,5)\,,(6,6)\,,(1,2)\,, \\ (1,4)\,,(2,1)\,,(2,4)\,,(4,1)\,(4,2)\,,(3,6)\,,(6,3) \end{array} \right\}. \tag{10.12}$$

Bevis at $\sim$ er en ækvivalensrelation.

Bestem $[a]$ for ethvert element $a \in M$, og angiv $M \diagup \sim$

6. Vis at de følgende relationer på de angivne mængder er ækvivalensrelationer. Gør det i hvert tilfælde på to måder:

- Ved at bestemme ækvivalensklasserne og vise at de giver en klassedeling af mængden
- Ved at vise direkte, at $\sim$ er refleksiv, symmetrisk og transitiv.

(a) På mængden af danskere defineres $A \sim B$, hvis A og B er født samme år.

(b) På $\mathbb{Z}$ defineres $a \sim b$, hvis $|a| = |b|$.

7. Bevis at følgende relationer er ækvivalensrelationer på de angivne mængder, og beskriv deres ækvivalensklasser:

(a) $M = \mathbb{R}$, $a \sim b \dot{\Leftrightarrow} a - b \in \mathbb{Z}$

(b) $M = \mathbb{R}$, $a \sim b \dot{\Leftrightarrow} \lfloor a \rfloor = \lfloor b \rfloor$, hvor $\lfloor a \rfloor$ betegner heltalsdelen af a, dvs. det største hele tal mindre eller lig med a.

(c) $M = \mathbb{R}^2$, $(x_1, y_1) \sim (x_2, y_2) \dot{\Leftrightarrow} x_1^2 + y_1^2 = x_2^2 + y_2^2$.

8. Lad Q betegne den følgende delmængde af $\mathbb{Z} \times \mathbb{Z}$:

$$Q = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0\} \,. \tag{10.13}$$

Definer relationen $\sim$ på Q ved

$$(a, b) \sim (c, d) \dot{\Leftrightarrow} ad = bc. \tag{10.14}$$

Bevis, at $\sim$ er en ækvivalensrelation, og angiv ækvivalensklassen $[(2, 3)]$ og mere generelt ækvivalensklassen $[(a, b)]$.

Prøv at give en beskrivelse af $Q/\sim$.

Kapitel 11

Afbildninger, funktioner

I dette kapitel skal vi præcisere det funktionsbegreb, I har brugt i gymnasiet og de indledende matematikkurser. Vi skal indføre grundlæggende begreber om funktioner og vise nogle sætninger om disse begreber.

I gymnasiet har I mødt reelle funktioner. En reel funktion er måske blevet indført som en forskrift eller en regel, som afbilder et reelt tal over i et andet reelt tal. For eksempel afbilder funktionen x^2 et reelt tal x over i det reelle tal x^2. Men hvad betyder det at afbilde, og hvad skal vi forstå ved en regel eller en forskrift? For at præcisere disse begreber, vil vi føre dem tilbage til de basale begreber i mængdelæren. Desuden vil vi generalisere funktionsbegrebet til andre mængder end mængder af reelle tal.

Ideen til hvordan funktionsbegrebet skal præciseres og generaliseres kan vi få ved at bemærke, at en funktion kan opfattes som en relation. For eksempel kan funktionen x^2 opfattes som den relation R på $\mathbb{R}$, som er defineret ved at xRy hvis $x^2 = y$. Vi vil derfor definere en funktion som en speciel slags relation. Ved at betragte relationer mellem andre mængder end $\mathbb{R}$, vil vi kunne generalisere funktionsbegrebet til funktioner fra en vilkårlig mængde A ind i en vilkårlig anden mængde B. Og da vi jo formelt har defineret en relation mellem to mængder A og B som en delmængde af produktmængden $A \times B$, vil vi derved få defineret funktionsbegrebet i rent mængdeteoretiske termer, uden brug af uldne ord som "forskrift" eller "regel".

Det er ikke enhver relation, som kan opfattes som en funktion. For at definere en funktion som en bestemt slags relation, skal vi altså have fat i den eller de egenskaber, som udmærker de relationer, der definerer funktioner. Betragt derfor en relation xRy, som er defineret ud fra en reel funktion f ved at $xRy \Leftrightarrow y = f(x)$. Denne relation har to særlige egenskaber:

1. Ethvert reelt x har et reelt billede $y = f(x)$, eller udtrykt i relationssprog: For ethvert $x \in \mathbb{R}$ findes et $y \in \mathbb{R}$, så xRy.

2. Ethvert reelt x har kun ét reelt billede, altså der er kun ét reelt y så $y = f(x)$. Udtrykt i relationssprog betyder det, at for ethvert $x \in \mathbb{R}$

findes der højst ét $y \in \mathbb{R}$ så xRy. Det kan også udtrykkes således: Hvis xRy_1 og xRy_2, da er $y_1 = y_2$.

Efter denne analyse kan vi nu formulere den formelle definition af en funktion eller en afbildning:

Definition 396 *Lad A og B være ikke tomme mængder. En relation f mellem A og B kaldes en **afbildning** eller en **funktion** fra A ind i B (og vi skriver $f : A \longrightarrow B$), hvis følgende to krav er opfyldt:*

1. *For alle $x \in A$ findes et $y \in B$, så at xfy (eller $(x, y) \in f$).*
2. *Hvis xfy_1 og xfy_2 (eller $(x, y_1) \in f$ og $(x, y_2) \in f$), da gælder at $y_1 = y_2$.*

Øvelse 397 *Lad $A = \{1, 2, 3, 4\}$ og $B = \{a, b, c, d\}$. Afgør, om følgende delmængder af $A \times B$ er afbildninger fra A ind i B.*

1. $\{(1, a), (2, b), (3, c), (4, d)\}$.
2. $\{(1, a), (2, a), (3, b), (4, b)\}$
3. $\{(1, a), (1, b), (2, c), (2, d), (3, a), (4, d)\}$
4. $\{(1, a), (2, c), (3, b)\}$

Notation 398 *Hvis f er en afbildning fra A ind i B og $x \in A$, da findes altså et entydigt $y \in B$, så xfy. Dette element y betegnes med $f(x)$ (siges:"f af x"). I stedet for xfy eller $(x, y) \in f$ skriver man derfor sædvanligvis $y = f(x)$.*

Bemærkning 399 *Hvis A og B er mængder af reelle tal, kan vi illustrere afbildningen f ved at indtegne mængden i et retvinklet koordinatsystem i planen. At en delmængde C af $A \times B$ af planen er en funktion, betyder da geometrisk, at enhver lodret linje, der skærer x-aksen i et punkt af A, har præcist ét punkt fælles med C. Det betyder nemlig, at der til ethvert $x \in A$ findes ét $y \in B$ så $(x, y) \in C$.*

Eksempel 400 *I $[-1, 1] \times [-1, 1]$ betragtes de fire mængder:*

1. *Enhedscirkelskiven: $D = \left\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\right\}$*
2. *Enhedscirklen: $C = \left\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\right\}$*
3. *Den højre del af enhedscirklen: $C_h = \left\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \wedge x \geq 0\right\}$*
4. *Den øvre del af enhedscirklen: $C_o = \left\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \wedge y \geq 0\right\}$.*

Den sidste mængde "er" en afbildning fra $[-1, 1]$ ind i sig selv, da der til hvert x i $[-1, 1]$ findes netop et $y \in [-1, 1]$, så $(x, y) \in C_o$.

D er ikke en afbildning fra $[-1, 1]$ ind i sig selv, da der til alle x'er i $]-1, 1[$ svarer mere end et $y \in [-1, 1]$ så $(x, y) \in D$. Det samme gælder C. C_h er heller ikke en afbildning fra $[-1, 1]$ ind i sig selv, da der til negative x'er ikke svarer noget $y \in [-1, 1]$, så $(x, y) \in C_h$.

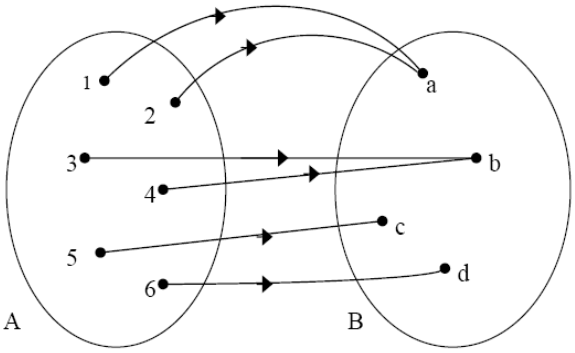
Eksempel 401 *Lad $\mathcal{C}$ betegne mængden af cirkler i planen Π. Lad f betegne følgende delmængde af $\mathcal{C} \times \Pi$: $f = \{(C, p) \in \mathcal{C} \times \Pi \mid p \text{ er centrum for } C\}$. Da er f en afbildning, og $f(C) =$ centrum for C. f er altså den afbildning, som afbilder en cirkel i sit centrum.*

Bemærkning 402 *I dansksproget litteratur bruges ordene funktion og afbildning ofte i flæng. Dog bruges ordet funktion fortrinsvist om en afbildning, som afbilder ind i de reelle eller komplekse tal. Vi vil i disse noter følge denne tradition. Afbildninger af planen eller rummet ind i sig selv kaldes også transformationer, og afbildninger mellem mængder af funktioner kaldes normalt operatorer.*

Selv om vi formelt har defineret en funktion eller afbildning $f : A \longrightarrow B$ som en relation mellem A og B, dvs. som en delmængde af $A \times B$, så er det nyttigt at bibeholde den intuitive idé af en funktion eller afbildning som en "maskine", som sender elementer x fra A over i elementer $f(x)$ i B. Den almindelige sprogbrug om funktioner og afbildninger afspejler bedre denne intuitive, men upræcise opfattelse af funktioner. Vi kalder for eksempel $f(x)$ for billedet (eller funktionsværdien) af x, og vi kan tale om at "anvende" funktionen f på x. Den delmængde af $A \times B$ som ifølge definitionen "er" funktionen f, kalder man sædvanligvis funktionens **graf**.

Det er derimod ikke hensigtsmæssigt at tænke på en funktion som en regneforskrift. Selv om reelle funktioner ofte er defineret ved at angive y som en formel i x, så kan mange (selv reelle) funktioner ikke angives på denne form.

Ofte illustrerer man afbildninger ved figurer i stil med Figur 11.1.



Figur 11.1: Afbildning af $A = \{1, 2, 3, 4, 5, 6\}$ ind i $B = \{a.b.c.d.e\}$

Lad f være en afbildning fra A ind i B. Da kaldes A for **definitionsmængden** og B kaldes **sekundærmængden** for f.

Definition 403 *Mængden af funktionsværdier $\{y \in B \mid \exists x \in A : y = f(x)\}$ kaldes afbildningens **billedmængde** eller **værdimængde**.*

Bemærkning 404 *I dansksproget litteratur hersker der en vis forvirring om betydningen af ordene billedmængde og værdimængde. I nogle fremstillinger (f.eks. tidligere noter til MatM) er det mængden B, som betegnes billedmængden eller værdimængden.*

Bemærkning 405 *Når man skal definere en afbildning, skal man altså angive tre ting:*

1. *Definitionsmængden A.*
2. *Sekundærmængden B.*
3. *Funktionsværdien $f(x)$ for ethvert $x \in A$.*

Bemærkning 406 *To afbildninger f og g er lig med hinanden hvis*

1. *de har samme definitionsmængde,*
2. *de har samme sekundærmængde,*
3. *og for alle x i definitionsmængden gælder $f(x) = g(x)$*

Ofte sjusker man når man angiver funktioner. Det er således meget almindeligt at tale om funktionen x^2. Dette er upræcist, fordi man ikke har angivet definitionsmængden og sekundærmængden. Det vil dog ofte være klart fra sammenhængen, hvad disse mængder er (f.eks. $\mathbb{R}$ eller $\mathbb{C}$). Når man i reel analyse taler om funktionen $1/x$ eller andre funktioner, som ikke naturligt er defineret på hele $\mathbb{R}$, så underforstås det ofte, at man som definitionsmængde skal tage den største mængde, hvor funktionen er defineret, altså i dette tilfælde $\mathbb{R} \setminus \{0\}$.

Angivelsen af en funktion ved udtrykkene x^2 og $1/x$ illustrerer også en anden unøjagtighed, som man ofte tillader sig ved omtalen af funktioner. I den generelle definition skelner vi mellem funktionen f og dens værdi $f(x)$ i et givet element $x \in A$. Men ofte omtaler man funktionen som $f(x)$ i stedet for som f. Det er for eksempel tilfældet med funktionerne x^2 og $1/x$, som jo vanskeligt lader sig angive uden at skrive x'et. Hvis man vil angive disse funktioner med en notation, der tydeliggør, at der er tale om funktionen, og ikke dens værdi i punktet x, kan man skrive: "funktionen $x \longrightarrow x^2$", men det gøres sjældent.

11.1 Injektivitet og surjektivitet

Definition 407 *1. En afbildning $f : A \longrightarrow B$ kaldes **surjektiv** (udtales "syrjektiv"), hvis værdimængden er hele B, altså hvis ethvert y i B er en funktionsværdi, eller udtrykt formelt:*

$$\forall y \in B \exists x \in A : y = f(x) \tag{11.1}$$

*Man siger da at f afbilder A **på** B.*

2. *En afbildning $f : A \longrightarrow B$ kaldes* ***injektiv (eller en-entydig)****, hvis ethvert y i B højst er billede af ét x i A, dvs. hvis*

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \tag{11.2}$$

3. *En afbildning $f : A \longrightarrow B$ kaldes* ***bijektiv,*** *hvis den er både surjektiv og injektiv, altså hvis ethvert $y \in B$ er billede af præcist ét $x \in A$. En bijektiv afbildning kaldes også en* ***bijektion****.*

Bemærkning 408 *Et bevis for at en afbildning er surjektiv er et eksistensbevis. Et bevis for at en afbildning er injektiv er et entydighedsbevis.*

Øvelse 409 *Hvilke af afbildningerne i 397 er surjektive og hvilke er injektive?*

Øvelse 410 *Tegn figurer med boller og pile, som illustrerer afbildninger som er surjektive og injektive, og afbildninger, som ikke er surjektive og injektive. Forklar, hvordan man på figurerne kan se om en afbildning er injektiv, og hvordan man ser at den er surjektiv.*

Bemærkning 411 *Hvis en funktion $f : A \longrightarrow B$ mellem to reelle talmængder repræsenteres ved sin graf i et retvinklet koordinatsystem i planen, da er den surjektiv, hvis enhver vandret linje gennem et punkt i B på y-aksen skærer grafen mindst en gang. Den er injektiv, hvis enhver vandret linje højst skærer grafen i ét punkt med x-koordinat i A.*

Eksempel 412 *Overvej at følgende påstande er sande:*

1. *Funktionen* $\sin : \mathbb{R} \longrightarrow \mathbb{R}$ *er hverken surjektiv eller injektiv.*
2. *Funktionen* $\sin : \mathbb{R} \longrightarrow [-1, 1]$ *er surjektiv men ikke injektiv.*
3. *Funktionen* $\sin : [-\pi/2, \pi/2] \longrightarrow \mathbb{R}$ *er injektiv men ikke surjektiv.*
4. *Funktionen* $\sin : [-\pi/2, \pi/2] \longrightarrow [-1, 1]$ *er bijektiv.*

Bemærkning 413 *Når man skal afgøre om en afbildning er surjektiv og injektiv, er det altså vigtigt at specificere definitionsmængden og sekundærmængden præcist. Generelt kan en vilkårlig funktion gøres surjektiv ved at indskrænke sekundærmængden til billedmængden.*

Eksempel 414 *Funktionen $f : \mathbb{R} \longrightarrow \mathbb{R}$ defineret ved $f(x) = 2x + 7$ er injektiv.*

Bevis. Der gælder følgende implikationer:

$$\begin{aligned} f(x_1) &= f(x_2) && (11.3)\\ &\Leftrightarrow 2x_1 - 7 = 2x_2 - 7 && (11.4)\\ &\Leftrightarrow 2x_1 = 2x_2 && (11.5)\\ &\Leftrightarrow x_1 = x_2 && (11.6) \end{aligned}$$

■

Eksempel 415 *Funktionen $f : \mathbb{R} \longrightarrow \mathbb{R}$ defineret ved $f(x) = x^3 - x$ er ikke injektiv.*

Bevis. For at vise at funktionen ikke er injektiv skal vi finde to forskellige x'er, som afbildes i den samme værdi. Her kan vi betragte tallene 0 og 1. Der gælder jo at $0 \neq 1$ men $f(0) = f(1) = 0$. ■

11.2 Billeder og urbilleder

Definition 416 *Lad A, B være mængder, og $f : A \longrightarrow B$ en afbildning. Lad endvidere $T \subseteq A$. Delmængden $f(T)$ af B defineret ved*

$$f(T) = \{y \in B \mid \exists t \in T : y = f(t)\} \tag{11.7}$$

*kaldes for **billedet** af T under f.*

Bemærkning 417 *Billedet af definitionsmængden $f(A)$ er altså billedmængden.*

Eksempel 418 *Betragt funktionen $f : \mathbb{R} \longrightarrow \mathbb{R}$ defineret ved $f(x) = x^2$. Da er $f(]-2, 10[) = [0, 100[$.*

Sætning 419 *Lad A og B være mængder, og lad $f : A \to B$ være en afbildning.*
Lad $\{T_\alpha\}_{\alpha\in\Lambda}$ være en familie af delmængder af A.
Da gælder følgende:

1. $f(\bigcup_{\alpha\in\Lambda} T_\alpha) = \bigcup_{\alpha\in\Lambda} f(T_\alpha)$.
2. $f(\bigcap_{\alpha\in\Lambda} T_\alpha) \subseteq \bigcap_{\alpha\in\Lambda} f(T_\alpha)$.

Bevis. *Bevis for 1.* Lad $y \in f(\bigcup_{\alpha\in\Lambda} T_\alpha)$. Der findes da $x \in \bigcup_{\alpha\in\Lambda} T_\alpha$, så $y = f(x)$. Da $x \in \bigcup_{\alpha\in\Lambda} T_\alpha$, findes $\alpha \in \Lambda$, så $x \in T_\alpha$. Da $y = f(x)$, er dermed $y \in f(T_\alpha)$.

Vi har altså påvist eksistensen af et $\alpha \in \Lambda$, så $y \in f(T_\alpha)$, hvormed vi har vist, at $y \in \bigcup_{\alpha\in\Lambda} f(T_\alpha)$.

Altså gælder $f(\bigcup_{\alpha\in\Lambda} T_\alpha) \subseteq \bigcup_{\alpha\in\Lambda} f(T_\alpha)$. Den omvendte inklusion vises, idet man ser, at ovenstående ræsonnement kan "vendes om" (overvej dette).

Bevis for 2. Lad $y \in f(\bigcap_{\alpha\in\Lambda} T_\alpha)$. der findes da $x \in \bigcap_{\alpha\in\Lambda} T_\alpha$, så $y = f(x)$. Da $x \in \bigcap_{\alpha\in\Lambda} T_\alpha$, gælder for ethvert $\alpha \in \Lambda$, at $x \in T_\alpha$. Da $y = f(x)$, haves dermed $y \in f(T_\alpha)$, for ethvert $\alpha \in \Lambda$. Med andre ord gælder $y \in \bigcap_{\alpha\in\Lambda} f(T_\alpha)$.
■

Bemærkning 420 *Som øvelse bør man overveje, hvorfor beviset for (2) i den foregående sætning ikke også kan 'vendes om'. Man bør også konstruere et modeksempel til påstanden om, at den omvendte inklusion i (2) skulle være alment gyldig (det er den nemlig ikke).*

Bemærkning 421 *Sætning 419 er faktisk et resultat af Sætning 35 (1.28) og (1.30) og den manglende inklusion er et resultat af bemærkning 36. Hvis vi bruger implikationerne i Sætning 35, kan beviset for sætning 419 nemlig føres i næsten ren symbolsk form som følger:*

Bevis. *Bevis for sætning 419, 1. For ethvert* $y \in B$ gælder følgende biimplikationer:

$$
\begin{array}{l}
y \in f(\bigcup_{\alpha\in\Lambda} T_\alpha) \\
\Updownarrow \\
\exists x \in A \ : \ \ x \in \bigcup_{\alpha\in\Lambda} T_\alpha \ \wedge \ y = f(x) \\
\Updownarrow \\
\exists x \in A \ \exists \alpha \in \Lambda \ : \ \ x \in T_\alpha \ \wedge \ y = f(x) \\
\Updownarrow \\
\exists \alpha \in \Lambda \ \exists x \in A \ : \ \ x \in T_\alpha \ \wedge \ y = f(x) \\
\Updownarrow \\
\exists \alpha \in \Lambda \ : \ \ y \in f(T_\alpha) \\
\Updownarrow \\
y \in \bigcup_{\alpha\in\Lambda} f(T_\alpha) \ ,
\end{array}
$$

hvoraf påstanden følger.

Bevis for sætning 419, 2. For ethvert $y \in B$ har vi følgende implikationer:

$$
\begin{array}{l}
y \in f(\bigcap_{\alpha\in\Lambda} T_\alpha) \\
\Updownarrow \\
\exists x \in A \ : \ \ x \in \bigcap_{\alpha\in\Lambda} T_\alpha \ \wedge \ y = f(x) \\
\Updownarrow \\
\exists x \in A \ \forall \alpha \in \Lambda \ : \ \ x \in T_\alpha \ \wedge \ y = f(x) \\
\Downarrow \\
\forall \alpha \in \Lambda \ \exists x \in A \ : \ \ x \in T_\alpha \ \wedge \ y = f(x) \\
\Updownarrow \\
\forall \alpha \in \Lambda \ : \ \ y \in f(T_\alpha) \\
\Updownarrow \\
y \in \bigcap_{\alpha\in\Lambda} f(T_\alpha) \ ,
\end{array}
$$

og det ønskede følger. ■

Definition 422 *Lad A, B være mængder, og $f : A \longrightarrow B$ en afbildning. Lad endvidere $S \subseteq B$. Delmængden $f^{-1}(S)$ af A defineret ved*

$$f^{-1}(S) = \{x \in A \mid f(x) \in S\} \tag{11.8}$$

kaldes ***urbilledet*** *(eller originalmængden) af S under f.*

Øvelse 423 *Tegn en figur med boller og pile til at illustrere urbilledet af en mængde.*

Det følger direkte fra definitionen af urbilledet at elementerne i $f^{-1}(S)$ kan karakteriseres som følger:

Sætning 424 *Lad A, B være mængder og $f : A \longrightarrow B$ en afbildning. Lad endvidere $S \subseteq B$. Da gælder:*

$$x \in f^{-1}(S) \Leftrightarrow f(x) \in S \tag{11.9}$$

Eksempel 425 *Betragt funktionen $f : \mathbb{R} \longrightarrow \mathbb{R}$ defineret ved $f(x) = x^2$. Da er*

1. $f^{-1}(\{4\}) = \{-2, 2\}$,
2. $f^{-1}([4, 9]) = [2, 3] \cup [-3, -2]$
3. $f^{-1}(\{-4\}) = \emptyset$

Bemærkning 426 *En funktion er specielt en relation. I definition 356 har vi defineret den inverse relation R^{-1} til en relation R. Vi har også i definition 354 defineret $R(A)$ for en delmængde af primærmængden, og vi bemærkede i bemærkning 358 at når S er en delmængde af sekundærmængden så gælder:*

$$R^{-1}(S) = \{a \in A \mid \exists b \in S : aRb\}. \tag{11.10}$$

Når R er en funktion f findes der netop ét $b \in B$, så aRb nemlig $b = f(a)$. Vi kan derfor omformulere (11.10) til

$$R^{-1}(S) = \{a \in A \mid f(a) \in S\} \tag{11.11}$$

Ved sammenligning med (11.8) ses at denne mængde er den samme, som den vi her har defineret som $f^{-1}(S)$. Vores definition af urbilledet er altså helt i overensstemmelse med den tidligere definition af det vi kaldte den til A_1 relaterede delmængde af B.

Sætning 427 *Lad A og B være mængder, og lad $f : A \to B$ være en afbildning.*

Lad $\{S_\alpha\}_{\alpha\in\Lambda}$ være en familie af delmængder af B, og lad S være en delmængde af B.

Da gælder følgende:

1. $f^{-1}(\bigcup_{\alpha\in\Lambda} S_\alpha) = \bigcup_{\alpha\in\Lambda} f^{-1}(S_\alpha)$.

2. $f^{-1}(\bigcap_{\alpha\in\Lambda} S_\alpha) = \bigcap_{\alpha\in\Lambda} f^{-1}(S_\alpha)$.

3. $f^{-1}(B\backslash S) = A \setminus f^{-1}(S)$.

Bevis. *Bevis for 1: For ethvert* $x \in A$ gælder følgende biimplikationer:

$$x \in f^{-1}(\bigcup_{\alpha\in\Lambda} S_\alpha) \tag{11.12}$$

$$\Leftrightarrow f(x) \in \bigcup_{\alpha\in\Lambda} S_\alpha \tag{11.13}$$

$$\Leftrightarrow \exists\alpha \in \Lambda : f(x) \in S_\alpha \tag{11.14}$$

$$\Leftrightarrow \exists\alpha \in \Lambda : x \in f^{-1}(S_\alpha) \tag{11.15}$$

$$\Leftrightarrow x \in \bigcup_{\alpha\in\Lambda} f^{-1}(S_\alpha), \tag{11.16}$$

hvilket viser påstanden.

Bevis for 2: analogt med beviset for 1.

Bevis for 3: For ethvert $x \in A$ gælder følgende biimplikationer:

$$x \in f^{-1}(B\backslash S) \tag{11.17}$$

$$\Leftrightarrow f(x) \in B\backslash S \tag{11.18}$$

$$\Leftrightarrow \neg f(x) \in S \tag{11.19}$$

$$\Leftrightarrow \neg x \in f^{-1}(S) \tag{11.20}$$

$$\Leftrightarrow x \in A \setminus f^{-1}(S), \tag{11.21}$$

hvilket viser påstanden. ■

11.3 Sammensætning af afbildninger, invers afbildning

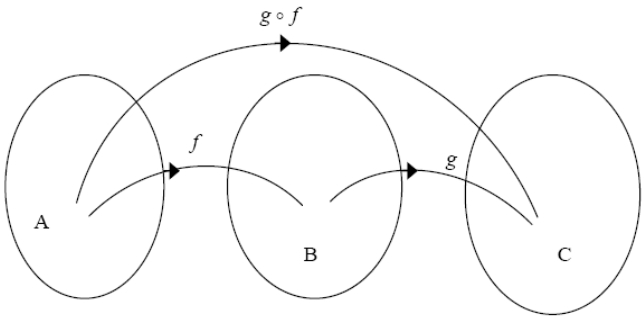
Definition 428 *Lad* A, B *og* C *være mængder og lad* $f : A \longrightarrow B$ *og* $g : B \longrightarrow C$ *være afbildninger. Da defineres den* ***sammensatte afbildning*** $g \circ f : A \longrightarrow C$ *ved:*

$$\text{For alle } x \in A \text{ er } g \circ f(x) = g(f(x)). \tag{11.22}$$

Bemærkning 429 *Funktionen* $g \circ f$ *fås altså ved først at anvende* f *og dernæst anvende* g*. Funktionerne skal altså anvendes i omvendt rækkefølge. Man har valgt denne skrivemåde fordi man derved får den simple definition:* $g \circ f(x) = g(f(x))$.

Eksempel 430 *Definer funktionerne* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *og* $g : \mathbb{R} \longrightarrow \mathbb{R}$ *ved* $f(x) = 2x + 7$ *og* $g(x) = x^2$*. Da er funktionerne* $g \circ f : \mathbb{R} \longrightarrow \mathbb{R}$ *og* $f \circ g : \mathbb{R} \longrightarrow \mathbb{R}$ *beskrevet ved*

$$(g \circ f)(x) = g(2x + 7) = (2x + 7)^2 \tag{11.23}$$



Figur 11.2: Den sammensatte funktion $g \circ f$

og

$$(f \circ g)(x) = f(x^2) = 2x^2 + 7 \tag{11.24}$$

Øvelse 431 *Lad $A = \{1,2,3,4\}$ og $B = \{a,b,c,d\}$. Definer $f : A \longrightarrow B$ og $\dot{g} : B \longrightarrow A$ ved deres grafer på følgende vis:*

$$f = \{(1,a),(2,a),(3,b),(4,b)\} \tag{11.25}$$

$$g = \{(a,2),(b,3),(c,4),(d,4)\} \tag{11.26}$$

Bestem graferne for $g \circ f$ og $f \circ g$.

Sætning 432 *Lad A, B og C være mængder og lad $f : A \longrightarrow B$ og $g : B \longrightarrow C$ være afbildninger. Da gælder følgende:*

1. *Hvis f og g begge er surjektive, da er $g \circ f : A \longrightarrow C$ surjektiv.*
2. *Hvis f og g begge er injektive, da er $g \circ f : A \longrightarrow C$ injektiv.*
3. *Hvis f og g begge er bijektive, da er $g \circ f : A \longrightarrow C$ bijektiv.*

Bevis. *Bevis for 1*: Antag at f og g begge er surjektive, og lad $z \in C$. Da g er surjektiv, findes et $y \in B$ så $z = g(y)$. Da f er surjektiv, findes endvidere et $x \in A$ så $y = f(x)$. Alt i alt har vi altså

$$z = g(y) = g(f(x)) = g \circ f(x) \tag{11.27}$$

Vi har altså vist, at der til ethvert $z \in C$, findes et $x \in A$, så $z = g \circ f(x)$. Det betyder netop at $g \circ f$ er surjektiv.

Bevis for 2: Antag, at f og g begge er injektive. Lad $x_1, x_2 \in A$, og antag at $g \circ f(x_1) = g \circ f(x_2)$. Vi skal vise at $x_1 = x_2$.

Da g er injektiv, og $g(f(x_1)) = g(f(x_2))$, kan vi slutte at $f(x_1) = f(x_2)$, og da f er injektiv, kan vi herfra slutte at $x_1 = x_2$.

Bevis for 3: Følger af 1. og 2. ■

Der gælder en delvis omvending af denne sætning:

Sætning 433 *Lad A, B og C være mængder, og lad $f : A \longrightarrow B$ og $g : B \longrightarrow C$ være afbildninger. Da gælder følgende:*

1. *Hvis $g \circ f : A \longrightarrow C$ er surjektiv, da er g surjektiv.*
2. *Hvis $g \circ f : A \longrightarrow C$ er injektiv, da er f injektiv.*

Bevis. *Bevis for 1*: Antag at $g \circ f : A \longrightarrow C$ er surjektiv. Vi skal vise, at g er surjektiv. Lad derfor $z \in C$. Da $g \circ f$ er surjektiv, findes et $x \in A$, så $z = g \circ f(x) = g(f(x))$. Men så findes jo et $y \in B$, så $z = g(y)$, nemlig $y = f(x)$.

Bevis for 2: Antag at $g \circ f : A \longrightarrow C$ er injektiv. Vi skal vise, at f er injektiv. Lad $x_1, x_2 \in A$, og antag at $f(x_1) = f(x_2)$. Vi skal vise at $x_1 = x_2$.

Da $f(x_1) = f(x_2)$, gælder

$$g \circ f(x_1) = g(f(x_1)) = g\left(f(x_2)\right) = g \circ f(x_2), \tag{11.28}$$

og da $g \circ f$ var antaget injektiv, slutter vi heraf at $x_1 = x_2$. ■

Øvelse 434 *Angiv eksempler på situationer, hvor A, B og C er mængder, og hvor $f : A \longrightarrow B$ og $g : B \longrightarrow C$ er afbildninger, og hvor*

1. *g er surjektiv, men $g \circ f$ ikke er surjektiv.*
2. *f er injektiv, men $g \circ f$ ikke er injektiv.*
3. *$g \circ f$ er surjektiv men f er ikke surjektiv.*
4. *$g \circ f$ er injektiv, men g er ikke injektiv.*

Giv to slags eksempler: dels eksempler, illustreret med mængdeboller og pile, i tilfælde hvor mængderne er endelige, og dels eksempler hvor mængderne A, B, og C alle er de reelle tal.

Sætning 435 *Lad A, B, C og D være mængder, og lad $f : A \longrightarrow B$ og $g : B \longrightarrow C$ og $h : C \longrightarrow D$ være afbildninger. Da gælder:*

$$h \circ (g \circ f) = (h \circ g) \circ f \tag{11.29}$$

Bevis. Overlades til læseren. ■

På grund af denne sætning kan vi tillade os at skrive $h \circ g \circ f$ i stedet for $h \circ (g \circ f)$ eller $(h \circ g) \circ f$. Lignende betragtninger gælder naturligvis ved sammensætning af flere end tre afbildninger.

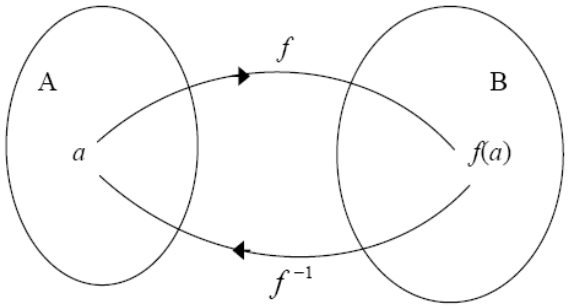
Definition 436 *Lad A være en mængde. Med 1_A betegnes den* ***identiske afbildning*** *på A, dvs. afbildningen givet ved*

$$1_A(a) = a \text{ for alle } a \in A \tag{11.30}$$

Afbildningen 1_A er naturligvis bijektiv.

Definition 437 *Lad A og B være mængder og lad $f : A \to B$ være en afbildning. En afbildning $g : B \longrightarrow A$ kaldes*

1. *en **venstreinvers** til f, hvis $g \circ f = 1_A$,*
2. *en **højreinvers** til f, hvis $f \circ g = 1_B$,*
3. *en **invers** til f, hvis g er både højre og venstreinvers til f, altså hvis $g \circ f = 1_A$ og $f \circ g = 1_B$.*



Figur 11.3: Den inverse funktion

Øvelse 438 *Overvej, om følgende funktioner har en højreinvers og en venstreinvers, og angiv en eller flere sådanne, hvis de findes:*

1. Funktionen $f : \mathbb{R} \longrightarrow \mathbb{R}$ defineret ved $f(x) = 4x - 3$.
2. Funktionen $f : \mathbb{R} \longrightarrow \mathbb{R}$ defineret ved $f(x) = x^2$.
3. Funktionen $f : \mathbb{R} \longrightarrow \mathbb{R}_+ \cup \{0\}$ defineret ved $f(x) = x^2$.
4. Funktionen $f : \mathbb{R} \longrightarrow [-1, 1]$ defineret ved $f(x) = \sin x$.

Sætning 439 *Lad A og B være mængder, og lad $f : A \to B$ være en afbildning. Hvis f har en invers afbildning, da er den entydigt bestemt.*

Bevis. Antag at $g : B \longrightarrow A$ og $h : B \longrightarrow A$ begge er inverse til f. Da gælder

$$g = g \circ 1_B = g \circ (f \circ h) = (g \circ f) \circ h = 1_A \circ h = h \tag{11.31}$$

■

Bemærkning 440 *Derimod er højre- og venstreinverser ikke nødvendigvis entydige. Hvis du ikke allerede har indset dette i forbindelse med Øvelse 438, bør du gøre det nu.*

Sætning 441 *Lad A og B være mængder, og lad $f : A \to B$ være en afbildning. Der gælder følgende:*

1. *f har en venstreinvers, hvis og kun hvis f er injektiv.*
2. *f har en højreinvers, hvis og kun hvis f er surjektiv.*
3. *f har en invers, hvis og kun hvis f er bijektiv.*

Bevis. *Bevis for 1*: Antag først, at f har en venstreinvers g. Da gælder pr. definition $g \circ f = 1_A$. Da 1_A er injektiv, følger det af sætning 433.2 at f er injektiv.

Antag omvendt, at f er injektiv. Vi skal da vise, at der findes en venstreinvers g til f. Vi skal med andre ord konstruere en afbildning $g : B \longrightarrow A$, så $g \circ f = 1_A$.

Vi bemærker, at hvis b ligger i $f(A)$, findes netop ét $a \in A$ så $f(a) = b$. For da f er injektiv, findes der højst et sådant a, og da $b \in f(A)$ findes der mindst et sådant a. Vælger vi nu et eller andet element $a_0 \in A$, kan vi dermed definere en afbildning $g : B \longrightarrow A$ ved:

$$g(b) = \begin{cases} a, & \text{hvis} \quad b = f(a) \text{ for et } a \in A \\ a_0, & \text{hvis} \quad b \notin f(A) \end{cases} \tag{11.32}$$

Vi får da for $a \in A$, at $g(f(a)) = a$, altså at $g \circ f = 1_A$.

Bevis for 2: Hvis f har en højreinvers $g : B \longrightarrow A$, så gælder at $f \circ g = 1_B$, og da 1_B er surjektiv, følger det af 433, at f er surjektiv.

Antag omvendt at f er surjektiv. Vi skal da vise, at der findes en højreinvers g til f. Vi skal med andre ord konstruere en afbildning $g : B \longrightarrow A$, så $f \circ g = 1_B$.

Når f er surjektiv betyder det at $f^{-1}(\{b\}) \neq \emptyset$ for ethvert $b \in B$. Vælg da for $b \in B$ et element $a_b \in f^{-1}(\{b\})$.[1] Ifølge sætning 424 gælder da, at $f(a_b) = b$ for ethvert $b \in B$. Defineres derfor en afbildning $g : B \longrightarrow A$ ved:

$$g(b) = a_b, \tag{11.33}$$

fås at

$$(f \circ g)(b) = f(g(b)) = f(a_b) = b \text{ for ethvert } b \in B, \tag{11.34}$$

dvs. at $f \circ g = 1_B$.

Bevis for 3: Hvis f har en invers, er denne både en højre- og venstreinvers, så af 1. og 2. fås, at f er både surjektiv og injektiv, altså bijektiv.

Omvendt hvis f er bijektiv er den både surjektiv og injektiv og har derfor både en venstreinvers g og en højreinvers h som opfylder

$$g \circ f = 1_A \text{ og } f \circ h = 1_B \tag{11.35}$$

[1] Her bruger vi et omdiskuteret aksiom i mængdelæren, det såkaldte udvalgsaksiom.

Hvis vi nu kan vise at der nødvendigvis må gælde $g = h$, så har vi bevist eksistensen af en afbildning, som er både højre- og venstreinvers, altså af en invers. Men at $g = h$ følger af følgende udregning:

$$g = g \circ 1_B = g \circ (f \circ h) = (g \circ f) \circ h = 1_A \circ h = h \tag{11.36}$$

■

Definition 442 *Hvis $f : A \to B$ er bijektiv, betegnes dens entydigt bestemte inverse afbildning med f^{-1}. Der gælder altså:*

$$f^{-1} \circ f = 1_A \text{ og } f \circ f^{-1} = 1_B \tag{11.37}$$

Man kalder også f's inverse for den ***omvendte afbildning****.*

Sætning 443 *Lad M være en ikke tom mængde. Da udgør mængden af bijektive afbildninger på M med kompositionsreglen $\circ$ en gruppe.*

Øvelse 444 *Bevis dette ud fra de foregående sætninger.*

Bemærkning 445 *Når $f : A \to B$ er en bijektiv afbildning, er f^{-1} karakteriseret ved, at der for alle $(x, y) \in A \times B$ gælder:*

$$x = f^{-1}(y) \Leftrightarrow f(x) = y. \tag{11.38}$$

Øvelse 446 *Lad $f : A \to B$ være en bijektiv afbildning. Bevis, at*

$$\left(f^{-1}\right)^{-1} = f \tag{11.39}$$

Øvelse 447 *Lad $f : A \to B$ og $g : B \longrightarrow C$ være bijektive afbildninger. Bevis, at*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1} \tag{11.40}$$

Det er en del af opgaven at bevise, at de angivne funktioner eksisterer.

Bemærkning 448 *Når $f : A \to B$ er en afbildning, har vi i dette kapitel brugt symbolet f^{-1} i to forskellige betydninger: 1. som betegnelsen for den inverse afbildning og. 2. i betegnelsen for urbilledet $f^{-1}(S)$ af en delmængde $S \subseteq B$. Disse to brug af symbolet f^{-1} må ikke forveksles. Man kan danne $f^{-1}(S)$, uanset om f er bijektiv eller ej, hvorimod man kun kan tale om den inverse afbildning f^{-1}, når f er bijektiv. Men hvis f er bijektiv, er der et potentielt problem: symbolet $f^{-1}(S)$ kan jo læses på to forskellige måder:*

1. *Som urbilledet af S under f.*
2. *Som billedet ved f^{-1} af S.*

Heldigvis bliver $f^{-1}(S)$ samme delmængde af A, uanset hvordan man opfatter symbolet.

Bemærkning 449 *I definition 356 definerede vi den inverse relation R^{-1} mellem B og A, når R er en relation mellem A og B. En funktion $f : A \longrightarrow B$ er specielt en relation mellem A og B. For ikke at øge forvirringen vil vi et øjeblik kalde denne relation for R_f. Altså har R_f en invers relation R_f^{-1}. Denne inverse relation er dog ikke altid en funktion, men hvis den er en funktion er den heldigvis lig med funktionen f^{-1}, som vi har defineret i dette kapitel. Det fremgår af følgende sætninger:*

Sætning 450 *Lad $f : A \longrightarrow B$ være en funktion, og kald dens tilhørende relation R_f. Da er R_f^{-1} en funktion på $f(A)$, hvis og kun hvis f er injektiv. Hvis f er injektiv, er funktionen R_f^{-1} en invers til funktionen $f : A \longrightarrow f(A)$.*

Bevis. Antag at $f : A \longrightarrow B$ er en funktion. At $R_f^{-1} : f(A) \longrightarrow A$ er en funktion betyder ifølge definition 396 at

1. For alle $y \in f(A)$ findes et $x \in A$, så at $yR_f^{-1}x$.

2. Hvis $yR_f^{-1}x_1$ og $yR_f^{-1}x_2$, da gælder at $x_1 = x_2$.

Men $yR_f^{-1}x$ betyder pr definition af R^{-1}, at xR_fy, eller ifølge definitionen af R_f, at xfy eller $y = f(x)$.

Altså kan de to betingelser omskrives til

1. For alle $y \in f(A)$ findes et $x \in A$, så at $y = f(x)$.

2. Hvis $f(x_1) = f(x_2) = y$ så er $x_1 = x_2$.

Det første betingelse er simpelthen definitionen af $f(A)$, og det andet punkt er ensbetydende med at f er injektiv.

Antag nu, at f er injektiv, så $R_f^{-1} : f(A) \longrightarrow A$ er en funktion. Vi skal da bevise, at R_f^{-1} er den inverse funktion til den bijektive afbildning $f : A \longrightarrow f(A)$. Ifølge bemærkning 445 skal vi bare vise at

$$x = R_f^{-1}(y) \Leftrightarrow f(x) = y. \tag{11.41}$$

Men det følger af definitionen på R_f^{-1} thi

$$x = R_f^{-1}(y) \Leftrightarrow yR_f^{-1}x \Leftrightarrow xR_fy \Leftrightarrow xfy \Leftrightarrow f(x) = y. \tag{11.42}$$

■

Sætning 451 *Lad $f : A \longrightarrow B$ være en funktion og kald dens tilhørende relation R_f. Da er R_f^{-1} en funktion på B hvis og kun hvis f er bijektiv. Hvis f er bijektiv er funktionen R_f^{-1} den inverse til funktionen $f : A \longrightarrow B$.*

Bevis. Følger af den forregående sætning. ■

11.4 Opgaver

1. Betragt mængderne

$$A = \{1, 2, 3, 4, 5\} \tag{11.43}$$

og

$$B = \{a, b, c, d\} \tag{11.44}$$

Hvilke af følgende mængder repræsenterer relationer, som er afbildninger fra den ene mængde ind i den anden:

(a) $\{(1, a), (2, b), (3, d), (4, d), (5, d)\}$
(b) $\{(1, a), (b, 3), (c, 4), (5, d), (2, a)\}$
(c) $\{(a, 3), (b, 4), (c, 5), (d, 1), (a, 2)\}$
(d) $\{(a, 3), (b, 2), (c, 2), (d, 5)\}$
(e) $\{(1, a), (2, b), (3, c), (4, d)\}$

Tegn boller med pile til at illustrere disse funktioner.

2. Betragt afbildningen på Figur 11.1:
Bestem følgende elementer og mængder
(a) $f(3)$ og $f(6)$
(b) $f(\{1, 2, 3\})$ og $f(\{4, 5, 6\})$
(c) $f^{-1}(\{a, e\})$, $f^{-1}(\{b\})$, $f^{-1}(\{c, d\})$ og $f^{-1}(\{c\})$.

3. Giv eksempler på endelige mængder A og B og afbildninger $f : A \longrightarrow B$ så:
(a) f er injektiv, men ikke surjektiv
(b) f er surjektiv men ikke injektiv
(c) f er både surjektiv og injektiv
(d) f er hverken surjektiv eller injektiv.

4. Giv eksempler på afbildninger $f : \mathbb{R} \longrightarrow \mathbb{R}$, som opfylder de fire punkter i opgave 3.

5. Lad U være en given grundmængde. For enhver delmængde M af U definerer vi en afbildning $k_M : U \longrightarrow \{0, 1\}$, kaldet den karakteristiske afbildning, ved:

$$k_M(x) = \begin{cases} 1 & \text{når} \quad x \in M \\ 0 & \text{når} \quad x \in \complement M \end{cases} \tag{11.45}$$

Vis at når A og B er vilkårlige delmængder af U, gælder:

$$k_{A \cap B} = k_A \cdot k_B, \quad \text{og} \quad k_{A \cup B} = k_A + k_B - k_A \cdot k_B. \tag{11.46}$$

Angiv afbildningerne

$$k_\emptyset, \quad k_U \quad \text{og} \quad k_{\complement A}. \tag{11.47}$$

Hvad kan man sige om mængderne A og B, når det for alle $x \in U$ gælder

$$k_A(x) \leq k_B(x)? \tag{11.48}$$

6. Bevis hvorvidt hver af de nedenstående funktioner $\mathbb{R} \longrightarrow \mathbb{R}$ er injektive og surjektive:

(a) $f(x) = \frac{1}{2}x - 5$
(b) $f(x) = 543x^3$
(c) $f(x) = x^5 - x$
(d) $f(x) = e^x$
(e) $f(x) = \cos x$

7. Betragt funktionen $f = \sin : \mathbb{R} \longrightarrow \mathbb{R}$. Bestem

$$f(\mathbb{R}_+) \quad \text{og} \quad f^{-1}(\mathbb{R}_+) \tag{11.49}$$

8. Lad funktionerne f og g $\mathbb{R} \longrightarrow \mathbb{R}$ være givet ved

$$f(x) = x^2 - 1 \quad \text{og} \quad g(x) = x^4 - 1. \tag{11.50}$$

Bevis, at

$$g(\mathbb{Q}) \subset f(\mathbb{Q}) \subset \mathbb{Q}. \tag{11.51}$$

Vis endvidere at hvis $x \in g(\mathbb{Q})$ er $\sqrt{x+1}$ rational.

9. Vis, at når $y \neq 1$, har ligningen

$$\frac{x}{x+1} = y \tag{11.52}$$

netop én løsning; og når $y = 1$ har ligningen ingen løsning.

Vis derved, at funktionen

$$f(x) = \frac{x}{x+1} \tag{11.53}$$

er en bijektion af mængden $\mathbb{R} \setminus \{-1\}$ på $\mathbb{R} \setminus \{1\}$, og angiv den inverse funktion.

10. Givet funktionen $f : \mathbb{R} \longrightarrow \mathbb{R}$ defineret ved

$$f(x) = \frac{x}{|x|+1}. \tag{11.54}$$

Bestem $f(\mathbb{R})$, og vis at f er bijektiv $\mathbb{R} \longrightarrow f(\mathbb{R})$

Find $f^{-1}(y)$ for $y \geq 0$ og for $y < 0$, og vis at f^{-1} kan angives ved

$$f^{-1}(y) = \frac{y}{1-|y|}. \tag{11.55}$$

11. Lad $f : A \longrightarrow B$ være en afbildning. Definer en relation på A ved

$$x \sim y \dot{\Leftrightarrow} f(x) = f(y). \tag{11.56}$$

Bevis at $\sim$ er en ækvivalensrelation. Beskriv ækvivalensklasserne.

12. Lad $f : A \longrightarrow B$ være en afbildning.

(a) Vis at for alle delmængder M af A gælder

$$M \subseteq f^{-1}(f(M)). \tag{11.57}$$

(b) Giv et eksempel på at $f^{-1}(f(M))$ ikke behøver være lig med M.

Kapitel 12

Tællemetoder. Kombinatorik

Inden vi går i gang med at tælle elementer i mængder, skal vi definere hvad "antallet af elementer i en mængde" overhovedet betyder:

12.1 Kardinalitet

Dette afsnit kradser kun lige lidt i overfladen af et stort og spændende emne.

Definition 452 *To mængder siges at have samme* ***kardinalitet*** *eller* ***mægtighed****, hvis der findes en bijektion mellem dem.*

Sætning 453 *Om vilkårlige mængder A, B og C gælder:*

1. *A har samme kardinalitet som A.*
2. *Hvis A har samme kardinalitet som B, har B samme kardinalitet som A.*
3. *Hvis A har samme kardinalitet som B og B har samme kardinalitet som C, så har A samme kardinalitet som C.*

Ovenstående sætning siger i en vis forstand at: relationen "har samme kardinalitet som" er en ækvivalensrelation. Det er dog ikke helt korrekt at udtrykke det sådan, for hvis den skulle være en ækvivalensrelation på en mængde, skulle det jo være på mængden af alle mængder, men samlingen af alle mængder er faktisk ikke en mængde.
Bevis. Ses af Sætning 433 og 441. ■

Sætning 454 *Hvis $m, n \in \mathbb{N}$ og $m \neq n$, så har $\{1, 2, 3, ..., n\}$ og $\{1, 2, 3, ..., m\}$ ikke samme kardinalitet.*

Denne sætning vil vi anse for intuitivt indlysende

Definition 455 *Lad M være en mængde.*

*Hvis der findes et $n \in \mathbb{N}$, og en bijektion mellem M og $\{1, 2, 3, ..., n\}$, siges M at være **endelig**, og n kaldes antallet af M's elementer (eller M's kardinalitet) og det betegnes med $n = |M|$. Vi siger også at den tomme mængde er endelig og at den har 0 elementer: $|\emptyset| = 0$.*

Definition 456 *Hvis M ikke er endelig, kaldes den **uendelig**.*

Bemærkning 457 *Hvis A har n elementer findes altså en bijektiv afbildning $f : A \longrightarrow \{1, 2, 3, ..., n\}$. Hvis vi definerer a_i $(i = 1, 2, ..., n)$ som $a_i = f^{-1}(i)$ så kan A skrives som $A = \{a_1, a_2, ..., a_n\}$. Omvendt ses det let at mængden $\{a_1, a_2, ..., a_n\}$ har n elementer. Altså er A endelig og har n elementer hvis og kun hvis den kan opskrives på formen $A = \{a_1, a_2, ..., a_n\}$*

Sætning 458 *To endelige mængder har samme kardinalitet, hvis og kun hvis de har samme antal elementer.*

En endelig og en uendelig mængde har ikke samme kardinalitet.

Bevis. Det følger af sætning (454) og definitionen af en uendelig mængde. ■

Bemærkning 459 *Også for uendelige mængder bruges betegnelsen $|M|$ for M's kardinalitet. $|M| = |N|$ betyder altså at M og N har samme kardinalitet.*

Sætning 460 *Hvis A er en endelig mængde, og $B \subseteq A$, så er B også endelig.*

Bevis. Beviset overlades til læseren ■

Inden vi går over til de endelige mængder skal uden bevis nævnes nogle resultater om kardinaliteten af de kendte uendelige talmængder:

Sætning 461 *$\mathbb{N}$, $\mathbb{Z}$, og $\mathbb{Q}$ har samme kardinalitet. Man siger, de er **tællelige**.*

Sætning 462 *$\mathbb{N}$ og $\mathbb{R}$ har ikke samme kardinalitet.*

Sætning 463 *$\mathbb{R}$ har samme kardinalitet som $\mathbb{C}$ og som $\mathbb{R}^n$ for alle $n \in \mathbb{N}$. Man siger, de har **kontinuets kardinalitet**.*

Sætning 464 *Lad M være en mængde. Da har potensmængden $P(M)$ ikke samme kardinalitet som M.*

12.2 Tællemetoder

I resten af kapitlet vil vi angive nogle metoder til at besvare spørgsmål om "hvor mange", altså metoder til at bestemme antal elementer i en endelig mængde. Læren om at tælle elementer i endelige mængder hedder **kombinatorik**. Man skulle tro, at det er et simpelt problem, at bestemme antallet af elementer i en mængde; men hvis bare mængden er moderat stor eller den er beskrevet på en lidt indviklet måde, kan det være svært at overskue tælleproblemet. Det

vanskelige er ofte at sørge for, at man får alt talt med, og at man ikke kommer til at tælle det samme element med flere gange.

Når man skal tælle, hvor mange vingummier der er i en slikpose, går det uværgerligt galt, fordi vingummierne ligger uordnet i posen. For at få styr på tælleprocessen skal man først ordne vingummierne på en eller anden måde. Man kan lægge dem op i en lang række, så man kan tælle dem forfra. Derved etablerer man jo den bijektive afbildning mellem rækken af vingummi og et afsnit $\{1, 2, 3, ..., n\}$ af de naturlige tal. En anden metode er at reducere tælleproblemet til simplere tælleproblemer. For eksempel kunne man dele vingummierne op i nogle mindre bunker, som lettere kan tælles, og så lægge antallene sammen. Dette er et eksempel på det additive tællemetode:

Sætning 465 ***Den additive tællemetode****: Hvis A og B er to disjunkte endelige mængder, så gælder*

$$|A \cup B| = |A| + |B| . \tag{12.1}$$

Bevis. Hvis A eller B er tom er sætningen triviel (overvej). Vi antager derfor at $A, B \neq \emptyset$. Da A og B er endelige mængder findes der to naturlige tal m og n (deres elementantal) og to bijektive afbildninger $f : A \longrightarrow \{1, 2, ..., m\}$ og $g : B \longrightarrow \{1, 2, ..., n\}$. For at vise sætningen skal vi bestemme en bijektiv afbildning $h : A \cup B \longrightarrow \{1, 2, ..., m + n\}$. Vi kan definere h ved følgende regel:

$$h(x) = \begin{cases} f(x) & \text{for } x \in A \\ m + g(x) & \text{for } x \in B \end{cases} \tag{12.2}$$

Denne afbildning h er veldefineret på $A \cup B$, da ethvert element i denne mængde netop er element i A eller i B. Afbildningen h afbilder $A \cup B$ på $\{1, 2, ..., m + n\}$ (overvej), og den er injektiv (overvej). Dermed er det vist at $|A \cup B| = m + n = |A| + |B|$. ■

Eksempel 466 *Hvor mange tal mellem 100 og 999 (begge inklusive) er delelige med 5?*

Dette tælleproblem kan løses ved at observere at tal, som er delelige med 5, ender på enten 0 eller 5, når de skrives i det almindelige 10-talsystem. Hvis vi lader A betegne mængden af tal mellem 100 og 999, som er delelige med 5, så kan den derfor opdeles i to disjunkte delmængder, nemlig den delmængde A_0, som består af tallene i A, som ender på 0, og delmængden A_5, som består af tallene i A, som ender på 5.

Tallene der ender på 0 er entydigt bestemt af de to første cifre i tallet. Når tallet skal ligge mellem 100 og 999, skal de to første cifre ligge mellem 10 og 99 og dem er der 90 af. Altså er $|A_0| = 90$. På samme måde ses det, at $|A_5| = 90$. Så ifølge den additive tællemetode ses at $|A| = |A_0 \cup A_5| = |A_0| + |A_5| = 90 + 90 = 180$.

Bemærkning 467 *Man kan tænke på den additive tællemetode på følgende måde. Hvis vi skal foretage et valg hvor vi kan vælge mellem m muligheder og n andre muligheder, så har vi $m + n$ muligheder at vælge blandt.*

Sætning 468 ***Subtraktionsreglen****: Hvis A er en endelig mængde og $B \subseteq A$, så gælder*

$$|A \setminus B| = |A| - |B| . \tag{12.3}$$

Bevis. $A \setminus B$ og B er to disjunkte mængder og $(A \setminus B) \cup B = A$. Den additive tællemetode giver derfor at

$$|A| = |B| + |A \setminus B| , \tag{12.4}$$

hvoraf det ønskede følger. ■

Sætning 469 *Hvis A og B er to endelige mængder (ikke nødvendigvis disjunkte), da gælder*

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{12.5}$$

Bevis. Mængderne A og $B \setminus (A \cap B)$ er disjunkte og $A \cup (B \setminus (A \cap B)) = A \cup B$. Derfor giver den additive tællemetode og subtraktionsreglen at

$$|A \cup B| = |A \cup (B \setminus (A \cap B))| \tag{12.6}$$

$$= |A| + |B \setminus (A \cap B)| = |A| + |B| - |A \cap B| . \tag{12.7}$$

■

Bemærkning 470 *Et mere uformelt argument for ovenstående sætning kunne lyde: Hvis vi lægger antallene af elementer i de to mængder A og B sammen, så har vi talt de elementer, som ligger i begge mængder, med to gange. Dem skal vi derfor trække fra én gang.*

Eksempel 471 *Hvor mange tal mellem 1 og 99 har mindst ét ciffer lig med 2?*

Tal med et 2-tal på en af pladserne kan deles ind i dem, der har et 2-tal på ener-pladsen, og dem, der har et 2-tal på tier-pladsen. Der er 10 af hver. Men et af tallene (nemlig 22) optræder i begge mængder. Derfor er der $10+10-1 = 19$ tal med den ønskede egenskab.

Overvej selv hvordan sætning 469 blev brugt i dette eksempel.

Sætning 472 *Hvis $A_1, A_2, ..., A_k$ er parvist disjunkte mængder, så gælder*

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots |A_k| . \tag{12.8}$$

Øvelse 473 *Vis ovenstående sætning ved induktion ud fra den additive tællemetode.*

Sætning 474 *Hvis A, B og C er tre endelige mængder (ikke nødvendigvis disjunkte), da gælder*

$$|A \cup B \cup C| = |A|+|B|+|C|-|A \cap B|-|A \cap C|-|B \cap C|+|A \cap B \cap C| . \tag{12.9}$$

Øvelse 475 *Bevis ovenstående sætning først uformelt, ved at argumentere på et Venn-diagram, og dernæst formelt ud fra de ovenstående sætninger.*

Øvelse 476 *I biblioteksdatabasen på et (lille) matematikbibliotek er de* 90 *bøger opført under emnebetegnelserne algebra, geometri og analyse. Hver bog har mindst en af disse emnebetegnelser, men nogle af dem har to eller alle tre emnebetegnelser. Databasen tillader én at søge på en eller to af disse emnebetegnelser. Det viser sig at der er* 55 *bøger med emnebetegnelsen algebra,* 30 *med emnebetegnelsen geometri og* 45 *med emnebetegnelsen analyse. Endvidere er der* 15 *bøger, som både har emnebetegnelsen algebra og geometri,* 15 *der både har emnebetegnelsen analyse og geometri og* 20 *der både har emnebetegnelsen analyse og algebra. Hvor mange bøger har alle tre emnebetegnelser?*

Sætning 477 *Lad A og B være to endelige mængder. Da gælder*

$$|A \times B| = |A|\,|B|\,. \tag{12.10}$$

Bevis. Hvis A eller B er tom er sætningen triviel (overvej). Vi antager derfor at $A, B \neq \emptyset$. Da A og B er endelige mængder findes der to naturlige tal $m = |A|$ og $n = |B|$, og to bijektive afbildninger $f : A \longrightarrow \{1, 2, ..., m\}$ og $g : B \longrightarrow \{1, 2, ..., n\}$. For at vise sætningen skal vi bestemme en bijektiv afbildning $h : A \times B \longrightarrow \{1, 2, ..., mn\}$. Vi kan definere h ved følgende regel:

$$h((a, b)) = (g(b) - 1)m + f(a). \tag{12.11}$$

Det ses let, at denne afbildning h afbilder $A \times B$ ind i $\{1, 2, ..., mn\}$. For at bevise at h er bijektiv benytter vi sætningen om division med rest (sætning 132). Ifølge denne sætning kan ethvert helt tal i på entydig måde skrives på formen

$$i = q \cdot m + r \quad \text{hvor} \quad q, r \in \mathbb{Z} \quad \text{og} \quad 0 \leq r < m. \tag{12.12}$$

Sættes nu $k = q + 1$, $j = i + 1$, og $l = r + 1$ kan dette omskrives til

$$j - 1 = (k - 1) \cdot m + (l - 1) \quad \text{hvor} \quad k, l \in \mathbb{Z} \quad \text{og} \quad 1 \leq l \leq m, \tag{12.13}$$

eller

$$j = (k - 1) \cdot m + l \quad \text{hvor} \quad k, l \in \mathbb{Z} \quad \text{og} \quad 1 \leq l \leq m. \tag{12.14}$$

For ethvert helt tal j findes altså entydigt bestemte hele tal k, l så (12.14) er opfyldt.

Nu kan vi vise at afbildningen h er bijektiv fra $A \times B$ på $\{1, 2, ..., mn\}$. Lad nemlig j være et tal i mængden $\{1, 2, ..., mn\}$. Ifølge det lige viste findes der da præcist to hele tal k og l så (12.14) er opfyldt. Når $j \in \{1, 2, ..., mn\}$ må endvidere $1 \leq k \leq n$, thi hvis $k \leq 0$ er $j = (k - 1) \cdot m + l \leq 0$ når $1 \leq l \leq m$ og hvis $n + 1 \leq k$ er $mn + 1 \leq (k - 1) \cdot m + l$ når $1 \leq l \leq m$. Til et $j \in \{1, 2, ..., mn\}$ findes altså entydigt bestemte hele tal k, l så

$$j = (k - 1) \cdot m + l \quad \text{hvor} \quad 1 \leq k \leq n \quad \text{og} \quad 1 \leq l \leq m. \tag{12.15}$$

Da nu $f : A \longrightarrow \{1, 2, ..., m\}$ og $g : B \longrightarrow \{1, 2, ..., n\}$ er bijektive, findes entydigt bestemte elementer $a \in A$ og $b \in B$ så $f(a) = l$ og $g(b) = k$. Men ifølge definitionen af h betyder det netop at der findes et entydigt bestemt element (a, b) i $A \times B$ så $h((a, b)) = j$. Det vil sige at $h : A \times B \longrightarrow \{1, 2, ..., mn\}$ er bijektiv. ■

Bemærkning 478 *Det ovenstående formelle bevis benytter den formelle definition af antal elementer i en mængde. Men det skjuler nok sætningens intuitive indhold. Det kommer frem, hvis vi skriver A på formen $A = \{a_1, a_2, ..., a_m\}$ og B på formen $B = \{b_1, b_2, ..., b_n\}$. Så kan vi nemlig angive elementerne i $A \times B$ i et rektangulært skema:*

$$\begin{array}{llll} (a_1, b_1) & (a_2, b_1) & \cdots & (a_m, b_1) \\ (a_1, b_2) & (a_2, b_2) & \cdots & (a_m, b_2) \\ \vdots & \vdots & \ddots & \vdots \\ (a_1, b_n) & (a_2, b_n) & & (a_m, b_n) \end{array} \tag{12.16}$$

Skemaet har størrelsen $m \times n$ så det ses klart at der er mn elementer i $A \times B$.

Bemærkning 479 *Fra nu af vil vi ikke give strengt formelle beviser for de kombinatoriske sætninger.*

Hvis vi tænker på mængderne A og B som en mængde af valgmuligheder eller hverv, der skal udføres kan vi opfatte elementerne i $A \times B$ som sammensatte valgmuligheder eller hverv, som består af at vi først skal foretage et valg (eller udføre et hverv) fra A og derefter et foretage et valg (eller udføre et hverv) fra B. Vi kan derfor omformulere sætning til følgende:

Sætning 480 ***Den multiplikative tællemetode*** *Hvis to hverv skal udføres, det ene efter det andet, og det første kan udføres på m måder, og for hver af disse kan det andet udføres på n måder, da kan det samlede hverv udføres på mn måder.*

Hvis to valg foretages efter hinanden, og det første valg står mellem m muligheder, og for hver af disse er der n muligheder i det andet valg, da vil det samlede valg have mn muligheder.

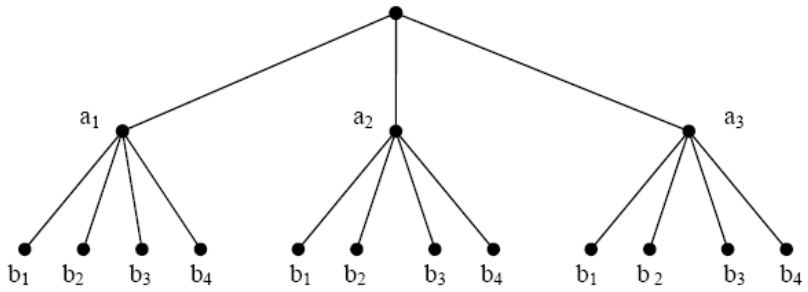
Her er det nødvendigt at hvert muligt samlet valg kun kan opnås på én måde (altså ved et bestemt første valg og et bestemt andet valg)

Tælletræer

Man kan illustrere den multiplikative tællemetode ved et tælletræ. Antag for eksempel, at første valg står mellem tre muligheder a_1, a_2, a_3 og andet valg står mellem fire muligheder b_1, b_2, b_3, b_4. Så kan vi illustrere situationen med tælletræet i figur 12.1

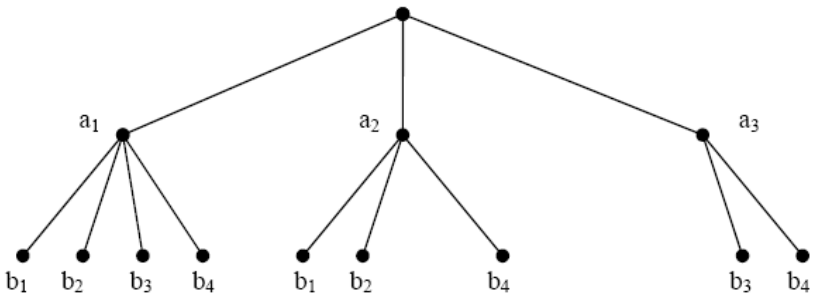
Dette tælletræ kunne illustrere de mulige valg af en menu på en restaurant, der serverer tre forretter og fire hovedretter. Hvis ingen af forretterne går igen som hovedretter, er menuen entydigt bestemt ved de to valg, og der er således $3 \cdot 4$ mulige menuer. Dette ses af tælletræet og fremgår også af den multiplikative tællemetode.

Det kunne dog tænkes at tjeneren ikke vil acceptere at visse forretter kombineres med visse hovedretter. Det betyder ikke noget for tællemetoden, så længe der er præcist det samme antal mulige valg af hovedret, uanset hvilken forret man vælger. Valgene b behøver altså ikke være ens i de tre tilfælde, så længe deres antal er det samme.



Figur 12.1: Tælletræ for to successive valg.

Men hvis nogle forretter indskrænker valg af hovedret til et mindre antal end andre forretter, kan den multiplikative tællemetode ikke længere bruges. Tælletræet kan dog stadig bruges til at systematisere optællingen af de mulige menuer. Antag for eksempel, at forret a_1 passer til alle fire hovedretter, medens forret a_2 kun passer sammen med tre af hovedretterne, og forret a_3 kun passer sammen med to af hovedretterne. I så fald ser tælletræet ud som i figur 12.2:



Figur 12.2: Tælletræ med forskelligt antal valgmuligheder i andet valg.

Det ses at der nu kun er 9 menuer tilbage.

Brugen af tælletræet svarer naturligvis til den additive tællemetode. Vi deler de mulige menuer op i tre disjunkte mængder: Dem med forret a_1, dem med forret a_2 og dem med forret a_3. Der er henholdsvist $4, 3$ og 2 menuer af de tre slags, og da vi skal vælge præcist en blandt disse, skal vi addere disse antal for at få det totale antal menuer. Den multiplikative tællemetode er et behændigt specialtilfælde, som virker, når der i andet valg er samme antal muligheder i alle tilfælde. I ovenstående tilfælde med 4 hovedretter for hver forret, er der jo $4 + 4 + 4$, som jo netop er $3 \cdot 4$, hovedretter.

Man kan naturligvis generalisere ovenstående sætning om produktmængder til flere end to mængder, svarende til valgsituationer, hvor vi skal foretage flere end to valg efter hinanden:

Sætning 481 *Lad $A_1, A_2, ..., A_k$ være endelige mængder. Da gælder*

$$|A_1 \times A_2 \times \cdots \times A_k| = |A_1|\,|A_2| \cdots |A_k|\,. \tag{12.17}$$

Bevis. Vises ved induktion ud fra sætning 477. ■

Sætning 482 *Antag vi skal foretage k valg efter hinanden. Antag endvidere, at det første valg kan foretages på n_1 måder, og at valg nummer i (for $i = 2, 3, ..., k$) kan foretages på n_i måder, uanset hvordan de første $i-1$ valg er foretaget, da kan det samlede valg foretages på $n_1 n_2 \cdots n_k$ måder*

Øvelse 483 *Hvis den ovennævnte restaurant serverer 5 forskellige desserter, hvor mange menuer kan man da vælge imellem 1. hvis tjeneren tillader alle kombinationer af forretter, hovedretter og desserter, og 2. hvis tjeneren laver de ovennævnte indskrænkninger i kombinationen af forret og hovedret? (lav tælletræer).*

12.3 Permutationer og kombinationer

Vi skal nu bruge de to tællemetoder fra forrige afsnit (især den multiplikative) til at tælle en række ting.

Definition 484 *En ordnet liste på r forskellige elementer udtaget blandt elementerne i en endelig mængde A kaldes en **permutation** på r elementer udtaget af A. Hvis A har n elementer (hvor $n \geq r$), betegnes antallet af forskellige permutationer på r elementer udtaget af A med ${}_nP_r$. Hvis $r = n$ taler man blot om en permutation af A.*

Definition 485 *Når n er et naturligt tal defineres $n!$ (siges: n **fakultet** eller n udråbstegn) som produktet af de naturlige tal mindre eller lig med n :*

$$n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n \tag{12.18}$$

Af praktiske grunde defineres endvidere $0! = 1$

Sætning 486 *Antallet af forskellige permutationer på r elementer udtaget af en mængde med n elementer er*

$${}_nP_r = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}. \tag{12.19}$$

Bevis. En ordnet liste på r elementer fra A kan bestemmes gennem r valg. Først vælges, hvilket element, som skal stå først på listen. Det kan gøres på n måder. Dernæst bestemmes, hvilket element der skal stå på andenpladsen på listen. Her kan vi vælge blandt alle A's elementer, på nær det element, vi valgte på førstepladsen. Der er altså $n-1$ elementer at vælge imellem. På tredjepladsen er der $n-2$ elementer at vælge imellem, osv. Det $r$te og sidste element kan vælges på $n-r+1$ måder.

Ifølge den multiplikative tællemetode er der altså $n(n-1)\cdots(n-r+1)$ måder at udvælge den ønskede liste af længde r ud af elementerne i A. Dette tal kan også skrives $\frac{n!}{(n-r)!}$ (overvej). ■

Korollar 487 *Lad A være en mængde med n elementer. Da er der $n!$ mulige permutationer af alle elementerne fra A.*

Øvelse 488 *I et 200-meter-løb deltager 6 løbere. På hvor mange mulige måder kan de fordele sig på første- til sjettepladsen? På hvor mange måder kan de fordele sig på guld-, sølv- og bronze-pladsen?*

Eksempel 489 *Fem personer skal sidde omkring et rundt bord. Det betyder ikke noget hvilken stol de sidder på; det eneste der betyder noget er, hvem der sidder til højre og hvem der sidder til venstre for hver person. På hvor mange måder kan de sidde?*

Da det kun er den relative placering som betyder noget, kan den første person anbringes på en bestemt stol. Derefter kan de resterende 4 sætte sig på $4! = 24$ forskellige måder. Disse svarer til 24 forskellige bordplaner.

Når man taler om permutationer, tages der hensyn til ordningen på den udvalgte liste. I mange tilfælde er man snarere interesseret i at udvælge en delmængde, hvor ordnen ikke betyder noget. I så fald taler man om kombinationer:

Definition 490 *I kombinatorik kaldes en delmængde på r elementer af en mængde A også for en **kombination** på r elementer udtaget af A. Hvis A har n elementer, kaldes antallet af kombinationer på r elementer udtaget af A for ${}_nK_r$ eller $\binom{n}{r}$ (siges: n over r).*

Bemærkning 491 *Forskellen på en permutation og en kombination er altså, at ordningen har betydning, når det drejer sig om permutationer, medens ordningen ikke har betydning, når det drejer sig om kombinationer. Permutationerne $(1,2,3)$ og $(3,1,2)$ udtaget af mængden $\{1,2,3,4,5\}$ er forskellige, hvorimod de er ens opfattet som kombinationer, da $\{1,2,3\} = \{3,1,2\}$.*

Lemma 492 *For ikke negative hele tal $n \geq r$ gælder*

$$ {}_nP_r = r!{}_nK_r. \tag{12.20}$$

Bevis. Betragt en vilkårlig kombination (en delmængde) med r elementer udtaget af en mængde A med n elementer. Da en mængde med r elementer kan ordnes på $r!$ måder (korollar 487), svarer der $r!$ permutationer til enhver sådan kombination. Deraf følger resultatet. ■

Sætning 493 *Antallet af kombinationer på r elementer udtaget af en mængde med n elementer er*

$$ {}_nK_r = \binom{n}{r} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r!} = \frac{n!}{r!(n-r)!}. \tag{12.21}$$

Bevis. Kombiner sætning 486 med 492. ■

Øvelse 494 *En fodboldtræner har 15 all-round spillere at vælge imellem. På hvor mange måder kan han udtage et hold på 11 spillere? Hvis to af de 15 er målmænd, hvor mange mulige hold kan han da udtage?*

12.4 Permutationer og kombinationer med gentagelser

I foregående afsnit så vi på permutationer og kombinationer af r *forskellige* elementer fra en forelagte mængde A. Nu skal vi se hvad der sker, når vi tillader gentagelser altså tillader at samme element i A optræder flere gange i permutationen eller kombinationen. Når vi i det følgende skriver "med gentagelser" menes: "hvor gentagelser er tilladt". Det betyder ikke, at der nødvendigvis skal være gentagelser.

Sætning 495 ***Permutationer med gentagelser****: Der er n^r permutationer (ordnede lister) på r elementer fra en mængde på n elementer, når man tillader gentagelser.*

Bevis. Hvert af listens r elementer kan vælges på n måder, så ifølge den multiplikative tællemåde er der n^r permutationer, når man tillader gentagelser. ■

Øvelse 496 *Hvor mange "ord" på 4 bogstaver kan man danne fra et alfabet på 6 bogstaver?*

Sætning 497 *1. Antallet af afbildninger af en endelig mængde A ind i en endelig mængde B er $|B|^{|A|}$.*

2. Antallet af injektive afbildninger af en endelig mængde A ind i en endelig mængde B er ${}_{|B|}P_{|A|} = \frac{|B|!}{(|B|-|A|)!}$. Her kræves at $|B| \geq |A|$, da der ellers ikke findes injektive afbildninger $A \longrightarrow B$.

Bevis. 1. Lad n betegne antallet af elementer i A og m antallet af elementer i B, og opskriv A som en liste: $A = \{a_1, a_2, ..., a_n\}$. En afbildning af A ind i B er bestemt, når vi for hvert element i A har gjort rede for hvilket element i B det afbildes over i. Vi udvælger altså en bestemt afbildning ved at foretage n valg: 1. Først vælges, hvilket element i B elementet a_1 skal afbildes i. 2. Dernæst vælges, hvilket element i B elementet a_2 skal afbildes i. ... Til slut vælges, hvilket element i B elementet a_n skal afbildes i. I hver valgsituation er der m muligheder (da det samme element i B jo kan være billede af flere elementer i A). Ifølge den multiplikative tællemetode er der altså $m \cdot m \cdot \cdots \cdot m$ (n faktorer)$= m^n = |B|^{|A|}$ mulige valg, svarende til $|B|^{|A|}$ afbildninger $A \longrightarrow B$.

Alternativt bevis: Man kan også føre sætningen tilbage til forrige sætning. Betragt nemlig en permutation med gentagelser på n elementer udtaget af elementerne i B. En sådan permutation repræsenterer en afbildning $A \longrightarrow B$ nemlig den, der sender a_i i permutationens $i$te element. Omvendt kan enhver afbildning repræsenteres på denne måde ved en permutation. Der er altså lige så mange afbildninger som der er permutationer med gentagelser på n elementer udtaget af elementerne i B, og ifølge forrige sætning er der m^n af dem.

2. Som i 1. kan fastlæggelsen af afbildningen opfattes som en følge af valg. Første valg kan foretages på m måder, men andet valg kan nu kun foretages på $(m-1)$ måder, da billedet af a_2 skal være forskelligt fra billedet af a_1. osv.

Dermed bliver der i alt $m(m-1)\cdots(m-n+1) =_m P_n =_{|B|} P_{|A|}$ injektive afbildninger $A \longrightarrow B$.

Alternativt bevis: Hvis vi, som i det alternative bevis for 1., repræsenterer en afbildning ved en permutation, vil afbildningen være injektiv, netop hvis der ikke er gentagelser i permutationen. Antallet af injektive afbildninger $f : A \longrightarrow B$ er altså lig med antal permutationer (uden gentagelser) på n elementer udtaget af B. Dette antal bestemte vi i sætning 486 til ${}_{|B|}P_{|A|} = \frac{|B|!}{(|B|-|A)!|}$. ■

Bemærkning 498 *: Ovenfor definerede vi en kombination som en mængde. Med den definition giver det strengt taget ingen mening at tale om kombinationer med gentagelser. For eksempel er mængden* $\{1,2,1\}$ *jo den samme mængde som* $\{1,2\}$*. Derfor vil vi herefter omdefinere en kombination, så den tillader gentagelser. Vi vil derfor nu definere en kombination som en "liste" hvor vi tillader gentagelser i listen, men hvor rækkefølgen på listen ikke har betydning. To kombinationer er altså ens, hvis de indeholder de samme elementer det samme antal gange.*

Sætning 499 *Antallet af kombinationer med gentagelser på* r *elementer udtaget af en mængde på* n *elementer er*

$$\binom{n+r-1}{r} \tag{12.22}$$

Bevis. Vi kan opfatte en kombination med gentagelser som en kommode med skuffer $s_1,\ s_2, ..., s_n$. Antallet af skuffer er lig med antallet n af elementer i mængden $A = \{a_1, a_2, ..., a_n\}$ som vi udtager kombinationen fra. I skufferne lægger vi r kugler. Når skuffe s_i indeholder k_i kugler, betyder det, at kombinationen indeholder k_i eksemplarer af elementet a_i. Når kombinationen skal indeholde r elementer, betyder det at vi skal anbringe r kugler i de n skuffer. Det kan illustreres ved følgende figur hvor x'erne symboliserer kuglerne (her $r = 8$), og skufferne (her $n = 5$) er repræsenteret ved mellemrummene mellem stregerne (og pladsen til venstre for første streg og til højre for sidste streg):

$$xx \mid x \mid\mid xxx \mid xx \tag{12.23}$$

Figuren betyder altså at der er to kugler i første skuffe, altså at der er to eksemplarer af elementet a_1 i kombinationen. Der er én kugle i anden skuffe, altså ét eksemplar af elementet a_2 i kombinationen. Der er ingen kugle i tredie skuffe, altså ingen eksemplar af elementet a_3 i kombinationen. Der er 3 kugler i fjerde skuffe, altså 3 eksemplar af elementet a_4 i kombinationen, og endeligt to kugler i femte skuffe svarende til to eksemplar af elementet a_5 i kombinationen. Kombinationen ser altså sådan ud:

$$\{a_1, a_1, a_2, a_4, a_4, a_4, a_5, a_5\}. \tag{12.24}$$

Læg mærke til, at konfigurationen benytter r krydser og $n-1$ steger.

For at angive en kombination med gentagelse på r elementer ud af en mængde på n, skal man altså fordele r krydser og $n-1$ steger på $r+n-1$ pladser. Når

først krydserne er placeret, er placeringen af stregerne bestemt. Krydserne kan placeres på $\binom{n+r-1}{r}$ måder. Herved er sætningen bevist. ■

Bemærkning 500 *Som i flere af de ovenstående argumenter har vi her løst et tælleproblem ved at føre det tilbage til et andet tælleproblem, som vi kendte løsningen på. Dette er en udbredt strategi. Vi kan altså ofte opfatte tælleproblemer som svar på andre tælleproblemer.*

Eksempel 501 *En bolsjefabrik fremstiller* 5 *slags bolsjer. De sælger dem som blandede bolsjer med 10 i hver pose. Hvor mange forskellige bolsjeposer kan der fremstilles?*

I en bolsjepose udtages altså 10 *bolsjer fra mængden af de* 5 *slags bolsjer. Hver slags bolsje kan optræde flere gange i posen. Vi kan derfor bruge resultatet i foregående sætning, så der er* $\binom{5+10-1}{10} = \binom{14}{10} = 1.001$ *forskellige bolsjeposer.*

Eksempel 502 *Hvor mange løsninger* (x_1, x_2, x_3, x_4) *er der til ligningen*

$$x_1 + x_2 + x_3 + x_4 = 10, \tag{12.25}$$

når x_1, x_2, x_3, x_4 *er ikke-negative hele tal?*

Som i beviset for sætning 499 kan vi opfatte dette problem som om vi skal lægge 10 *kugler (svarende til ligningens højreside) i* 4 *skuffer (svarende til de fire ubekendte). Hvis kugleantallet i de fire skuffer er* x_1, x_2, x_3, x_4*, svarer det til en løsning til ligningen. Ifølge argumentet i sætning 499 er der* $\binom{10+4-1}{10} = \binom{13}{10} =$ 286 *løsninger. Her skelner man mellem xernes orden: løsningen* $1+2+3+4$ *og* $4+1+2+3$ *regnes altså som værende forskellige.*

I Sætning 486, 493, 495, 499 er der behandlet forskellige tællesituationer. Resultaterne kan anføres på tabelform:

r udtaget af n	permutationer	kombinationer
uden gentagelser	${}_nP_r = \frac{n!}{(n-r)!}$	$\binom{n}{r} = \frac{n!}{r!(n-r)!}$
gentagelser tilladt	n^r	$\binom{n+r-1}{r}$

(12.26)

12.5 Permutationer, hvor nogle elementer ikke kan skelnes fra hinanden

Problem 503 *Hvor mange forskellige ord kan man danne ved at omordne bogstaverne i ordet RARERE?*

Løsning 504 *Hvis vi indicerer R-erne og E-erne så vi kan skelne dem fra hinanden:* $R_1AR_2E_1R_3E_2$ *så er der nu* $6! = 720$ *permutationer af bogstaverne, svarende til* 720 *ord. Men disse ord kommer i par som kun adskiller sig ved at de to E-er er byttet om. Når vi så fjerner indexerne på E-erne bliver ordene altså parvist ens, så der nu kun er* $\frac{720}{2}$ *forskellige ord. Ord, som kun adskiller sig ved at de tre R-er er permuteret, bliver endvidere ens når vi fjerner indiceringen på R-erne. Da der er* $3! = 6$ *permutationer af de tre R-er ender der altså med kun at være* $\frac{720}{2 \cdot 6} = 60$ *forskellige ord dannet af alle bogstaverne i RARERE.*

Løsningen på problemet illustrerer en udbredt tællemetode, hvor man først tæller ting med flere gange og derefter justerer det for store antal. Vi brugte en lignende (multiplikativ) strategi i 493 og en additiv variant i 470.

Løsningen på ovenstående problem kan let generaliseres til følgende sætning, som læseren selv kan vise:

Sætning 505 *Der kan dannes*

$$\frac{n!}{k_1!k_2!\cdots k_l!} \tag{12.27}$$

forskellige permutationer af n objekter, som falder i l klasser med $k_1, k_2, ..., k_l$ elementer ($n = k_1+k_2+\cdots+k_l$), hvor elementerne i hver klasse ikke kan skelnes fra hinanden, men elementer fra forskellige klasser kan skelnes fra hinanden.

Øvelse 506 *Hvor mange forskellige ord kan man danne ved omordning af bogstaverne i ordet Mississippi?*

Sætning 507 *En mængde A med n elementer kan opdeles i disjunkte delmængder $A_1, A_2, ..., A_l$ med henholdsvist $k_1, k_2, ..., k_l$ elementer ($n = k_1 + k_2 + \cdots + k_l$) på*

$$\frac{n!}{k_1!k_2!\cdots k_l!} \tag{12.28}$$

måder.

Bevis. Overlades til læseren. ■

Til slut kommer en sætning, som ikke rigtig hører hjemme her eller i nogle af de foregående afsnit.

Sætning 508 *Antallet af delmængder i en endelig mængde A er $2^{|A|}$. Altså:*

$$|P(A)| = 2^{|A|} \tag{12.29}$$

Bevis. Lad n betegne antallet af elementer i A, og opskriv A som en liste: $A = \{a_1, a_2, ..., a_n\}$. En delmængde af A er bestemt, når vi har gjort rede for hvilke af A's elementer, der ligger i den. Vi udvælger derfor en bestemt delmængde ved at foretage n valg efter hinanden: 1. Skal a_1 med i delmængden? 2. Skal a_2 med i delmængden? .... Skal a_n med i delmængden? I hver valgsituation er der netop to muligheder: ja eller nej. I følge den multiplikative tællemetode er der altså $2 \cdot 2 \cdot \cdots \cdot 2$ (n faktorer)$= 2^n$ mulige valg svarende til 2^n delmængder. Bemærk at formlen også passer når A er tom. ■

12.6 Binomialkoefficienterne

Definition 509 *Størrelserne $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ kaldes **binomialkoefficienter.***

Denne sprogbrug skyldes, at størrelserne optræder som koefficienter, når man udregner den n'te potens af en toleddet størrelse (et binomium):

Sætning 510 ***Binomialformlen****. Lad x og y være reelle eller komplekse tal og n et ikke-negativt helt tal. Da gælder*

$$(x+y)^n \tag{12.30}$$

$$= x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + y^n \tag{12.31}$$

$$= \sum_{r=0}^{n}\binom{n}{r}x^{n-r}y^r. \tag{12.32}$$

Bevis. Formlen indses let når $n = 0$. Antag derfor at $n \geq 1$.

For at udregne $(x + y)^n$ skal man gange $(x + y)$ med sig selv n gange: $(x+y)(x+y)\cdots(x+y)$ (n faktorer). Når disse parenteser ganges ud, fås 2^n led af formen $x^{n-r}y^r$. Samles nu alle led med samme værdi af r, fås n led af formen $kx^{n-r}y^r$, et for hvert r. Koefficienten k foran $x^{n-r}y^r$ i denne sum angiver, hvor mange led ud af de oprindelige 2^n led, som havde formen $x^{n-r}y^r$ for denne værdi af r. Hvor mange er det? Ja, hvert led af formen $x^{n-r}y^r$ fremkommer ved at multiplicere y'er fra r af parenteserne og x'er fra resten af parenteserne. Men vi kan vælge de r parenteser på $\binom{n}{r}$ måder, så koefficienten må være $\binom{n}{r}$. ■

Sætning 511 *For alle hele tal n, r hvor $n \geq r \geq 0$ gælder*

$$\binom{n}{r} = \binom{n}{n-r} \tag{12.33}$$

Bevis. Identiteten følger direkte af formlen $\binom{n}{r} = \frac{n!}{r!(n-r)!}$.

Et mere intuitivt argument forløber således: Når vi udtager r elementer af en mængde med n elementer, har vi også implicit udtaget en delmængde på $n - r$ elementer, nemlig komplementærmængden, altså de ikke udtagne elementer. Antallet af måder, vi kan udtage r elementer af en mængde på n elementer, er derfor lig med antallet af måder, vi kan udtage $n - r$ elementer. ■

Bemærkning 512 *Det sidste bevis forløber ved at tælle den samme mængde på to forskellige måder. Et sådant argument kaldes et* ***kombinatorisk argument****.*

Sætning 513 *For alle hele tal n, r hvor $n > r > 0$ gælder rekursionsformlen*

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1} \tag{12.34}$$

Bevis. Beviset kan naturligvis føres ved at bruge formlen $\binom{n}{r} = \frac{n!}{r!(n-r)!}$. (gør dette!).

Men igen giver et kombinatorisk argument nok mere indsigt i sagen: $\binom{n}{r}$ angiver antal delmængder på r elementer udtaget af en mængde A på n elementer. Dette antal kan vi også finde på en anden måde. Lad nemlig a_1 være et bestemt element i A (dette findes da $n > 2$). Nu kan vi inddele delmængderne (med r elementer) af A i to disjunkte klasser: Klasse 1 bestående af de delmængder, som indeholder a_1, og klasse 2 bestående af de delmængder, som ikke indeholder a_1. I klasse 1 er der $\binom{n-1}{r-1}$ mængder, thi for at fastlægge en sådan mængde skal vi udvælge delmængdens resterende $r-1$ elementer blandt A's resterende $n-1$ elementer. I klasse 2 er der $\binom{n-1}{r}$ mængder, thi for at fastlægge en sådan mængde skal vi udvælge delmængdens r elementer blandt A's resterende elementer. Ifølge den additive tællemetode er der altså $\binom{n-1}{r} + \binom{n-1}{r-1}$ delmængder på r elementer udtaget af A's n elementer. ■

Pascals trekant: For at få overblik over binomialkoefficienterne er det nyttigt at opstille dem i et trekantet skema kaldet Pascals trekant[1]. De første 7 rækker i trekanten ser således ud:

$$\begin{array}{ccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6}
\end{array} \tag{12.35}$$

Sætning 513 siger så at en binomialkofficient er lig med summen af de to binomialkoefficienter, som står skråt over den (til højre og til venstre) i Pascals trekant. Denne observation tillader en at udregne binomialkoefficienterne i Pascals trekant rekursivt række for række ud fra de 1'taller, som står i de yderste diagonaler ($\binom{n}{0}$ og $\binom{n}{n}$). De første 7 rækker i trekanten bliver:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array} \tag{12.36}$$

Øvelse 514 *Fortsæt selv Pascals trekant nogle rækker længere ned.*

[1] Efter Blaise Pascal (1623-1662), som studerede den grundigt i et værk udgivet 1665. Trekanten havde dog været opstillet tidligere.

Sætning 515 *For et vilkårligt naturligt tal n gælder*

$$\sum_{r=0}^{n}\binom{n}{r} = 2^n \tag{12.37}$$

Bevis. Der er flere mulige beviser for denne identitet:

1. Man kan regne venstresiden ud ved at bruge $\binom{n}{r} = \frac{n!}{r!(n-r)!}$. Denne metode kan ikke anbefales.

2. Man kan bruge binomialformlen

$$(x+y)^n = \sum_{r=0}^{n}\binom{n}{r}x^{n-r}y^r. \tag{12.38}$$

For hvis man heri sætter $x = 1$ og $y = 1$, så fås

$$2^n = \sum_{r=0}^{n}\binom{n}{r}1^{n-r}1^r, \tag{12.39}$$

hvilket giver det ønskede.

3. Man kan også give et kombinatorisk bevis: $\binom{n}{r}$ angiver antal delmængder på r elementer udtaget af en mængde A med n elementer. Hvis man lægger alle disse tal sammen fra $r = 0$ til $r = n$, får man antal delmængder med enten 0 eller 1 eller ...eller n elementer, altså antallet af samtlige delmængder af A. Men ifølge sætning 508 er dette antal netop 2^n.

4. Man kan også lave et induktionsbevis efter n, idet man bruger rekursionsformlen 12.34.[2] ■

Sætning 516 *For alle hele tal n, r hvor $n \geq r \geq 0$ gælder*

$$\binom{n+1}{r+1} = \sum_{k=r}^{n}\binom{k}{r}. \tag{12.40}$$

Bevis. For $r = 0$ er venstresiden af formlen lig med $\binom{n+1}{1} = n+1$, og højresiden er $\sum_{k=0}^{n}\binom{k}{0} = \sum_{k=0}^{n}1 = n+1$. Identiteten gælder altså i dette tilfælde.

Lad r være et naturligt tal. Vi vil bevise identiteten ved induktion efter n.

1. Induktionsstart: For $n = r$ er venstresiden af (12.40) lig med $\binom{n+1}{n+1} = 1$. Højresiden er lig med $\sum_{k=n}^{n}\binom{k}{r} = \binom{n}{n} = 1$. Identiteten er altså sand for $n = r$.

[2] Det var faktisk i forbindelse med dette og lignende beviser at Pascal for første gang formulerede princippet om matematisk induktion i sin afhandling om Pascals trekant.

2. Induktionsskridtet: Antag at identiteten (12.40) er sand for $n-1 \geq r$, altså at

$$\binom{n}{r+1} = \sum_{k=r}^{n-1} \binom{k}{r}. \tag{12.41}$$

Ifølge rekursionsformlen (12.34) fås da:

$$\binom{n+1}{r+1} = \binom{n}{r+1} + \binom{n}{r} = \sum_{k=r}^{n-1} \binom{k}{r} + \binom{n}{r} = \sum_{k=r}^{n} \binom{k}{r}. \tag{12.42}$$

Altså ses at identiteten er sand for n.

Fra princippet om matematisk induktion slutter vi derfor, at identiteten er sand for alle $n \geq r$. ■

Øvelse 517 *Forklar indholdet i ovenstående sætning ved at pege i Pascals trekant, og antyd beviset ved at bruge rekursionsformlen rekursivt i trekanten.*

Sætning 518 ***Vandermondes identitet***[3]*: Lad m, n, r være ikke-negative hele tal så $r \leq m, n$. Så gælder*

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \binom{n}{k} \tag{12.43}$$

Bevis. Betragt to disjunkte mængder med henholdsvist m og n elementer. Man kan da udtage r elementer fra foreningsmængden på $\binom{m+n}{r}$ måder. En anden måde at udtage r elementer fra foreningsmængden er at udtage k elementer fra mængden med n elementer og $r-k$ elementer fra mængden med m elementer (hvor $0 \leq k \leq r$). Det kan ifølge den multiplikative tællemåde gøres på $\binom{m}{r-k}\binom{n}{k}$ måder. Når vi summerer antallet af alle disse valg, for $0 \leq k \leq r$ fås antallet af samtlige måder at udtage r elementer fra foreningsmængden. ■

12.7 Skuffeprincippet

Sætning 519 ***Skuffeprincippet:*** *1. Hvis m objekter fordeles i s skuffer, og hvis $m > s$, er der mindst én skuffe med 2 objekter eller flere.*

2. Mere generelt: Hvis m objekter fordeles i s skuffer, og hvis $m > ks$, er der mindst én skuffe med $k+1$ objekter eller flere.

3. Og omvendt: Hvis m objekter fordeles i s skuffer, og hvis $m < ks$, er der mindst én skuffe med $k-1$ eller færre objekter.

Bevis. for 2. Føres ved kontraposition. Antag at alle s skuffer indeholder k objekter eller færre. Så er der højst ks objekter, altså $m \leq ks$. ■

Øvelse 520 *Bevis selv 1. og 3. i skuffeprincippet.*

[3] Efter Alexandre-Théophile Vandermonde (1735-1796)

Bemærkning 521 *Man kan naturligvis formulere skuffeprincippet matematisk mere stringent, men det vil vi ikke gøre.*

Selv om skuffeprincippet er så oplagt, har det mange overraskende konsekvenser. Man skal bare vælge skufferne og objekterne snedigt.

Eksempel 522 *1. I en serie af syv kast med en sædvanlig terning vil mindst to af kastene vise det samme antal øjne. Det kan ses af skuffeprincippet, hvis vi indretter en skuffe for hvert af de mulige antal øjne* $1, 2, 3, 4, 5, 6$ *og prøver at fordele de* 7 *kast i disse* 6 *skuffer.*

2. I en bridge hånd på 13 spillekort er der mindst 4 *kort i en af de* 4 *farver. Bevis dette ud fra skuffeprincippet ved et passende valg af skuffer og objekter.*

3. Blandt vilkårligt 101 *af tallene* $\{1, 2, 3, ..., 200\}$ *er der to, som er indbyrdes primiske. Lav nemlig* 100 *"skuffer" bestående af de ulige tal og deres efterfølger:* $\{1, 2\}, \{3, 4\}, ..., \{199, 200\}$. *Hvis vi lægger de* 101 *givne tal på deres rette plads i disse skuffer, er der altså mindst én skuffe med mere end ét tal. Der er altså mindst to tal* m, n *i følgen, som følger efter hinanden. Men så er* $1 = n - m$ *hvoraf det følger at* m *og* n *er indbyrdes primiske (sætning 140).*

Eksempel 523 *Hvis* 5 *punkter afsættes i et rektangel på* $6cm \times 8cm$, *så er der to punkter med en afstand på* 5 *cm eller mindre.*

Thi, hvis rektanglet deles i fire rektangler på $3cm \times 4cm$, *så må der ifølge skuffeprincippet være et af rektanglerne, som indeholder to punkter. Og ifølge Pythagoras er der maximalt* 5 *cm mellem to punkter i et af de små rektangler.*

Eksempel 524 *Hvis* A *er en delmængde af* $\{1, 2, 3, ..., 2n\}$ *med* $n+1$ *elementer, så indeholder* A *to tal, så det ene er en divisor i det andet.*

Thi ethvert naturligt tal kan skrives på formen $2^k m_k$ *hvor* m_k *er ulige. Men der er kun* n *ulige tal mindre eller lig med* $2n$. *Altså er der i følge skuffeprincippet to tal i* A, *som har samme* m_k: $2^i m_i$ *og* $2^j m_i$. *Hvis* $i < j$, *vil* $2^i m_i$ *være en divisor i* $2^j m_i$, *og hvis* $j < i$ *vil* $2^j m_i$ *være en divisor i* $2^i m_i$.

12.8 Opgaver

1. På en hylde står 8 matematikbøger, 7 datalogibøger og 5 historiebøger. På hvor mange måder kan man vælge to bøger herfra om to forskellige emner?

2. Hvor mange fircifrede tal indeholder mindst et 5-tal?

3. Find antallet af naturlige tal mindre eller lig med 1001, som er multipla af enten 3 eller 5.

Find antallet af naturlige tal mindre eller lig med 200, som er multipla af $2, 3$ eller 5.

4.Et firma opgiver oplysninger om sine medarbejdere til et statistisk bureau. De opgiver, at ud af firmaets 1.200 medarbejdere er 675 gift, 682 er over 30 år, 684 er mænd, 195 er gift og over 30 år, 467 er gifte mænd, 318 er mænd over 30 år, og 165 er gifte mænd over 30 år. Har firmaet været omhyggeligt med sin indberetning?

5. Hvor mange naturlige tal under 100.000 indeholder et ciffer som er $2, 4$ eller 6?

6. Tegn et tælletræ, som illustrerer de mulige forløb af en turnering mellem to spillere a og b. Den, der først vinder 3 spil, har vundet. Hvor mange mulige forløb er der af turneringen? Hvor mange af disse har a mulighed for at vinde hvis b vinder første spil?

7. Et password skal bestå af fem bogstaver (a,b,c eller d) efterfulgt af fire tal $(0, 1, 2, 3, 4, 5, 6, 7, 8$ eller $9)$. Hvor mange passwords kan der dannes?

8. På hvor mange måder kan man vælge et password på 5 bogstaver ud fra et alfabet på 10 bogstaver?

Hvor mange af disse indeholder gentagelser?

9. Hvor mange naturlige tal mindre eller lig med 999 har to eller tre ens cifre?

10. Bevis at ${}_nP_1 +_n P_2 = n^2$.

11. Syv personer skal i teatret og har fået 7 sæder ved siden af hinanden.

(a) På hvor mange måder kan de sætte sig, hvis der er to som insisterer på at ville sidde ved siden af hinanden

(b) På hvor mange måder kan de sætte sig, hvis der er to som nægter at sidde ved siden af hinanden?

12. En ekspeditionsleder skal udvælge et ekspeditionshold på 5 andre, som skal ledsage hende på en ekspedition. Hun har 11 personer at vælge imellem, men blandt dem er der et ægtepar, som kun vil med, hvis ægtefælden også er med. Hvor mange mulige ekspeditionshold kan lederen danne?

To år senere er ekspeditionslederen klar til en ny ekspedition med 5 af de samme 11 personer. Men denne gang er ægteparret blevet skilt, og de hader nu hinanden, så de kun vil med, hvis deres ex ikke skal med. Hvor mange hold kan der nu dannes?

13. Fire drenge og fem piger skal stilles op i række, så to drenge ikke står ved siden af hinanden, og to piger ikke står ved siden af hinanden. På hvor mange måder kan det gøres?

Hvor mange mulige opstillinger er der hvis der er 5 drenge og 5 piger?

14. Du skal anbringe 5 matematikbøger, 6 fysikbøger og 3 historiebøger på en hylde. Hvor mange måder kan det gøres, hvis

(a) der ikke er nogen indskrænkninger i bøgernes placering?

(b) bøgerne om de enkelte emner skal stå sammen?

(c) hvis bøgerne om de enkelte emner skal stå sammen, og matematikbøgerne skal stå i midten?

15. Hvor mange binære tal kan skrives med 5 ettaller og 7 nuller?

16. Betragt et hold på 12 personer bestående af 5 mænd og 7 kvinder.

(a) Hvor mange 5-personers grupper kan der udvælges med 2 mænd og 3 kvinder?

(b) Hvor mange 5-personers grupper har mindst en mandlig deltager?
(c) Hvor mange 5-personers grupper har højst en mandlig deltager?

17. Hvor mange afbildninger er der fra en mængde med 5 elementer ind i en mængde med 7 elementer? Hvor mange af disse afbildninger er injektive? Hvor mange er surjektive?

18. Hvor mange bijektive afbildninger er der fra en mængde med 5 elementer på en mængde med n elementer for forskellige værdier af n?

19. Hvor mange forskellige bridge hænder på 13 kort kan der dannes fra et almindeligt spil kort, hvis man ikke skelner mellem de forskellige kort i hver kulør (der er fire kulører)?

20. En blomsterforretning sælger 6 forskellige slags blomster. Hvor mange buketter på 10 blomster kan der sammensættes?

21. Hvor mange forskellige ord kan dannes ved omordning af bogstaverne i ordet "matematik"

Hvor mange af disse ord både begynder og slutter på t?

Hvor mange af ordene indeholder tegnstrengen "mat" et sted i ordet?

22. På hvor mange måder kan man fordele 5 kort til 4 spillere fra et almindeligt spil kort på 52 spillekort?

23. En bager har 6 slags morgenbrød (han har mere end 10 af hver). Hvor mange forskellige poser med 10 morgenbrød kan man sammensætte?

Hvor mange af disse indeholder alle de 6 slags morgenbrød?

24. Angiv antallet af ikke negative heltallige løsninger (x, y, z) til ligningen

$$x + y + z = 9 \tag{12.44}$$

25. Madsen vinder i bogklubbens lotteri. Som gevinst får han lov til at vælge tre af bogklubbens 10 bøger. Han må gerne vælge flere eksemplarer af den samme bog. Hvor mange mulige valg har Madsen?

26. Bevis at $\sum_{r=0}^{n}(-1)^r\binom{n}{r} = 0$

27. Bevis at $\binom{2n}{n} = \sum_{r=0}^{n}\binom{n}{r}^2$

28. Bevis at når n, r, k er ikke negative hele tal med $k \leq r \leq n$ så gælder

$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k} \tag{12.45}$$

Bevis identiteten dels ved et kombinatorisk argument og ved at bruge formel (12.21)

29. Bevis at når $1 \leq k \leq n$ så gælder

$$k\binom{n}{k} = n\binom{n-1}{k-1}. \tag{12.46}$$

Giv et bevis, som bruger formel (12.21), og et kombinatorisk bevis, idet du fortolker de to sider i identiteten som antallet af måder, man kan udvælge en delmængde på k elementer af en mængde på n elementer og derefter udvælge et af elementerne i denne delmængde.

30. Bevis at i en mængde af $m + 1$ naturlige tal er der to som har samme rest ved division med m.

31. Hvor mange mennesker skal være samlet for at man kan være sikker på, at der er to, der har fødselsdag i samme måned?

32. Hvis en gruppe af mennesker kommer fra 3 forskellige lande, hvor stor skal gruppen da være for at sikre, at der kommer 4 fra samme land.

33. Hvor mange tal skal man vælge fra mængden $\{1, 2, ..., 20\}$ for at være sikker på, at to af dem har sum 21?

34. Vis at kardinaliteten af mængden af de lige tal er lig med kardinaliteten af mængden af de ulige tal.

Kapitel 13

Permutationer

I forrige kapitel betragtede vi permutationer opfattet som måder at udtage en ordnet liste på r elementer af en mængde A på n elementer. I dette kapitel vil vi kun se på de permutationer, hvor $r = n$ altså på omordninger af alle elementerne i A. Og hvor vi i forrige kapitel studerede antallet af permutationer, vil vi i dette kapitel studere strukturen af mængden af permutationer. Vi vil undersøge, hvordan de kan sammensættes og hvordan en given permutation kan sammensættes af simplere permutationer. Det giver til slut anledning til indførelsen af fortegnet for en permutation.

13.1 Notation og produkt

Vi starter med en ny definition af en permutation:

Definition 525 *En bijektion $\sigma : A \longrightarrow A$ kaldes en permutation af mængden A.*

Bemærkning 526 *I dette afsnit ser vi på permutationer på endelige mængder. Når man skal checke om en afbildning af en endelig mængde ind i sig selv er bijektiv, er det nok at checke, om den er enten surjektiv eller injektiv. Der gælder nemlig:*

Sætning 527 *Lad A være en endelig mængde og σ en afbildning $\sigma : A \longrightarrow A$. Da gælder*

$$\sigma \text{ er surjektiv } \Leftrightarrow \sigma \text{ er injektiv.} \tag{13.1}$$

Bevis. Antag at A har n elementer, så den kan skrives på formen $A = \{a_1, a_2, ..., a_n\}$. Da gælder

$$\sigma \text{ er injektiv} \tag{13.2}$$
$$\Leftrightarrow \sigma(a_1), \sigma(a_2), ..., \sigma(a_n) \text{ er forskellige} \tag{13.3}$$
$$\Leftrightarrow \sigma(a_1), \sigma(a_2), ..., \sigma(a_n) \text{ er alle } A\text{'s elementer} \tag{13.4}$$
$$\Leftrightarrow \sigma \text{ er surjektiv.} \tag{13.5}$$

■

Notation 528 ***Tabelnotation****: Lad $A = \{a_1, a_2, ..., a_n\}$ være en endelig mængde og σ en permutation $\sigma : A \longrightarrow A$. Da repræsenteres σ ofte ved tabellen*

$$\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ \sigma(a_1) & \sigma(a_2) & \sigma(a_3) & \dots & \sigma(a_n) \end{pmatrix} \tag{13.6}$$

Bemærkning 529 *Da σ er en bijektion $A \longrightarrow A$, er nederste linje i tabellen en omordning af elementerne i A. Omvendt giver enhver omordning anledning til en permutation. Vores nye definition af en permutation af en mængde stemmer derfor overens med definitionen 484 af en permutation på n elementer udtaget af en mængde A med n elementer. Ifølge korollar 487 er der $n!$ sådanne permutationer.*

Eksempel 530 *Betragt mængden $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ og permutationen σ på X defineret ved*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 3 & 6 & 8 & 2 & 4 & 1 \end{pmatrix}. \tag{13.7}$$

Permutationen σ afbilder altså 1 i 5, 2 i 7 osv. Man kan altså direkte aflæse hvad hvert tal i X afbildes i:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 7 & 3 & 6 & 8 & 2 & 4 & 1 \end{pmatrix} \tag{13.8}$$

Bemærkning 531 *Når en permutation opskrives på tabelform, kan man naturligvis flytte rundt på søjlerne, så længe det bare er de samme elementer, som står under hinanden. For eksempel kan permutationen σ i Eksempel 530 også repræsenteres ved tabellen*

$$\sigma = \begin{pmatrix} 4 & 7 & 8 & 1 & 3 & 2 & 6 & 5 \\ 6 & 4 & 1 & 5 & 3 & 7 & 2 & 8 \end{pmatrix}. \tag{13.9}$$

Notation 532 ***Direkte notation****: Når permutationen er defineret på en mængde af formen $\{1, 2, 3, ..., n\}$, så er det naturligt at stille øverste række i tabelnotationen op i voksende orden: $1, 2, 3, ..., n$ Men hvis vi vedtager at gøre det, er det jo nok at angive den nederste række $(\sigma(1), \sigma(2), \sigma(3), ..., \sigma(n))$. Dette er den direkte notation.*

Eksempel 533 *Permutationen σ i Eksempel 530 skrives i direkte notation som*

$$\sigma = (5, 7, 3, 6, 8, 2, 4, 1). \tag{13.10}$$

Sammensætning af permutationer. Hvis σ og τ er to permutationer af A, så kan de sammensættes som afbildninger:

$$\tau \circ \sigma : A \xrightarrow{\sigma} A \xrightarrow{\tau} A. \tag{13.11}$$

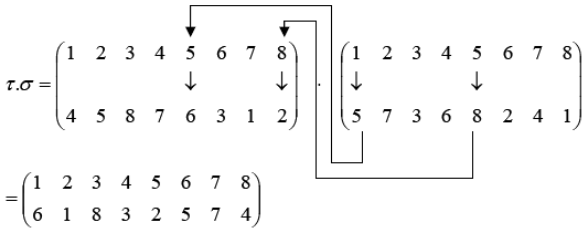
Her skal man være opmærksom på rækkefølgen: $\tau\circ\sigma$ betyder den afbildning som fremkommer, når man *først* anvender σ og *dernæst* τ. altså $\tau\circ\sigma(a)=\tau(\sigma(a))$

Ofte bruger man multiplikativ skrivemåde, så man i stedet for $\tau\circ\sigma$ skriver $\tau\cdot\sigma$ eller blot $\tau\sigma$.

Eksempel 534 *Lad σ være den permutation af $X=\{1,2,3,4,5,6,7,8\}$, som blev defineret i eksempel 530. Lad endvidere τ være den permutation af X, som i tabelnotation kan skrives*

$$\tau=\begin{pmatrix}1&2&3&4&5&6&7&8\\4&5&8&7&6&3&1&2\end{pmatrix} \tag{13.12}$$

Vi ønsker at bestemme $\tau\cdot\sigma$. Først bestemmes hvad 1 afbildes i: Ved σ afbildes det i 5, som afbildes videre i 6 ved τ. Ligeså ses at $2\to 7\to 1$, osv. På figur 13.1 ses, hvordan man kan bestemme produktet. Det er vigtigt at man husker at starte fra permutationen til højre.



Figur 13.1: Multiplikation af permutationer.

Da permutationer er bijektive afbildninger, kan man tale om identitetspermutationen 1_A og om den inverse permutation σ^{-1} til en permutation σ. Den inverse til en permutation skrives i tabelnotation ved at bytte om på de to rækker (overvej)

Eksempel 535 *På $X=\{1,2,3,4,5,6,7,8\}$ kan identitetspermutationen skrives*

$$1_X=\begin{pmatrix}1&2&3&4&5&6&7&8\\1&2&3&4&5&6&7&8\end{pmatrix}, \tag{13.13}$$

og den inverse til permutationen σ i Eksempel 530 kan skrives

$$\sigma^{-1}=\begin{pmatrix}5&7&3&6&8&2&4&1\\1&2&3&4&5&6&7&8\end{pmatrix}, \tag{13.14}$$

som ved ombytning af søjlerne kan skrives

$$\sigma^{-1}=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&6&3&7&1&4&2&5\end{pmatrix} \tag{13.15}$$

eller i direkte notation: $(8,6,3,7,1,4,2,5)$.

Permutationer kommuterer normalt ikke. For eksempel hvis σ og τ er de to permutationer defineret i (13.7) og (13.12), så er

$$\begin{aligned}&\sigma \cdot \tau \\ &= \begin{pmatrix} 4 & 7 & 8 & 1 & 3 & 2 & 6 & 5 \\ 6 & 4 & 1 & 5 & 3 & 7 & 2 & 8 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 8 & 7 & 6 & 3 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 8 & 1 & 4 & 2 & 3 & 5 & 7 \end{pmatrix},\end{aligned}$$

som er forskellig fra $\tau \cdot \sigma$, som vi udregnede i eksempel 534.

Definition 536 *Et element a i en endelig mængde A kaldes et **fixpunkt** for en permutation σ af A hvis $\sigma(a) = a$.*

*Hvis $\sigma(a) \neq a$ siges σ at **flytte** a.*

Eksempel 537 *Permutationen σ defineret i (13.7) har fixpunktet 3 og flytter alle andre elementer i X.*

Definition 538 *To permutationer σ og τ på samme mængde kaldes **disjunkte,** hvis mængden af elementer, der flyttes af σ, er disjunkt fra mængden af elementer, der flyttes af τ.*

Eksempel 539 *For eksempel er permutationen*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}, \tag{13.16}$$

som kun flytter 3 og 4, disjunkt fra permutationen

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}, \tag{13.17}$$

som flytter 1 og 2, men ikke disjunkt fra

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}, \tag{13.18}$$

som flytter $1, 2, 3$ og 4.

Lemma 540 *Lad σ være en permutation af mængden A. Hvis a flyttes af σ, så flyttes $\sigma(a)$ også af σ.*

Bevis. Da σ er bijektiv og dermed injektiv, fås

$$a \neq \sigma(a) \Rightarrow \sigma(a) \neq \sigma(\sigma(a)). \tag{13.19}$$

Heraf følger det ønskede. ■

Sætning 541 *Disjunkte permutationer af samme mængde kommuterer.*

Bevis. Lad σ og τ være disjunkte permutationer af A og lad $a \in A$. Vi skal da vise at

$$\tau \cdot \sigma(a) = \sigma \cdot \tau(a). \tag{13.20}$$

Enten er a et fixpunkt for begge permutationer, eller også flyttes a af en af dem.

1. Hvis a er et fixpunkt for både σ og τ så gælder

$$\tau \cdot \sigma(a) = \tau(a) = a = \sigma(a) = \sigma \cdot \tau(a) \tag{13.21}$$

2. Antag at a flyttes af en af permutationerne, for eksempel af σ. Da σ og τ er disjunkte, må a derfor være et fixpunkt for τ. Altså gælder

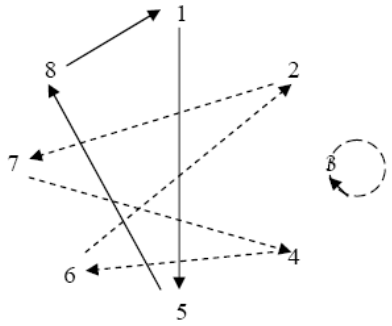
$$\sigma \cdot \tau(a) = \sigma(a) \tag{13.22}$$

Ifølge lemma 540 ved vi, at da a flyttes af σ, så flyttes $\sigma(a)$ også af σ. Men da σ og τ er disjunkte, må $\sigma(a)$ derfor også være et fixpunkt for τ. Derfor gælder

$$\tau \cdot \sigma(a) = \sigma(a). \tag{13.23}$$

Af (13.22) og (13.23) ses, at det også i dette tilfælde gælder at $\tau \cdot \sigma(a) = \sigma \cdot \tau(a)$. ■

Bemærkning 542 *Man kan illustrere en permutation σ ved en figur, hvor mængdens elementer $a_1, a_2, ..., a_n$ er placeret på en vilkårlig måde, og hvor der anbringes en pil fra et element a_i til et andet a_j hvis $\sigma(a_i) = a_j$. For eksempel kan permutationen σ defineret i (13.7) illustreres ved diagrammet i figur 13.2*



Figur 13.2: Permutation delt op i cykler.

Det ses af figuren at σ kan deles op i tre cykler, hvori elementerne successivt afbildes over i hinanden. Denne observation vil vi nu forfølge.

13.2 Cykler

Definition 543 *Lad $a_1, a_2, ..., a_p$ være p forskellige elementer i en mængde A. Vi kan da definere en permutation σ ved:*

$$\sigma(a_1) = a_2 \tag{13.24}$$
$$\sigma(a_2) = a_3 \tag{13.25}$$
$$\sigma(a_3) = a_4 \tag{13.26}$$
$$\vdots \tag{13.27}$$
$$\sigma(a_p) = a_1 \tag{13.28}$$
$$\sigma(a) = a \quad \text{når} \quad a \notin \{a_1, a_2, ..., a_p\} \tag{13.29}$$

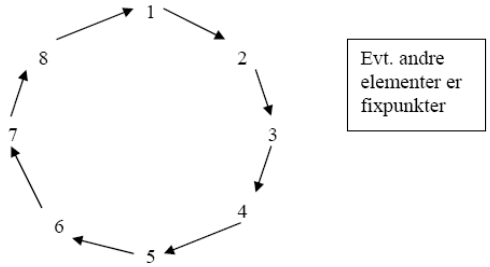
En permutation af denne form kaldes en ***p-cykel*** *eller en cykel af længde p. Cykler angives normalt i den såkaldte cykelnotation. I denne notation angives ovenstående cykel som:*

$$(a_1\ a_2\ ...\ a_p)\,. \tag{13.30}$$

Bemærkning 544 *Bemærk at der ikke sættes kommaer mellem elementerne i cykelnotationen. Derved kan den skelnes fra den direkte notation*[1]*.*

Bemærk også at når man angiver en cykel i cykelnotationen, er det vigtigt at angive hvilken mængde det er en permutation af. I cykelnotationen angives fixpunkterne for cyklen jo ikke. For eksempel kan (1 2 3) *være en cykel på en hvilken som helst af mængderne $\{1, 2, 3, ..., n\}$ når bare $n \geq 3$. Herved adskiller cykelnotationen sig fra tabelnotationen, hvor man i øverste linje kan aflæse, hvilken mængde permutationen virker på.*

Cyklen (1 2 3 4 5 6 7 8) *på en mængde $\{1, 2, 3, ..., n\}$ $(n \geq 8)$ kan illustreres ved diagrammet i figur 13.3*



Figur 13.3: Illustration af en cykel.

[1] I andre bøger angives cykler i cykelnotationen dog ofte med kommaer mellem elementerne.

Bemærkning 545 *Det er klart at første elementet i cykelnotationen kan vælges vilkårligt blandt de elementer cyklen flytter, blot rækkefølgen bibeholdes. Cyklen* (1 3 2) *er således den samme cykel som* (3 2 1).

Endelig bemærkes at definition 543 også giver mening når $p = 1$*, hvor den blot er en definition af identitetspermutationen. Vi kan altså opfatte identititspermutationen som en cykel og kan i cykelnotation skrive den som*

$$1_A = (a)\,, \tag{13.31}$$

hvor a *er et vilkårligt at* A*'s elementer.*

Sætning 546 *Lad* $a_1, a_2, ..., a_p$ *være* p *forskellige elementer i en endelig mængde* A*. Da gælder*

$$(a_1\ a_2\ \ ...\ a_p)^{-1} = (a_p\ a_{p-1}\ ...\ a_1)\,. \tag{13.32}$$

Altså er den inverse til en cykel igen en cykel, og den angives i cykelnotationen ved at opskrive elementerne i cykelnotationen bagfra.

Bevis. Lad $\sigma = (a_1\ a_2\ \ ...\ a_p)$ være en cykel på A, og lad τ beregne cyklen $\tau = (a_p\ a_{p-1}\ ...\ a_1)$. Vi skal da vise, at for et vilkårligt element $a \in A$ gælder

$$\tau \cdot \sigma(a) = \sigma \cdot \tau(a) = a. \tag{13.33}$$

Hvis $a \notin \{a_1, a_2, ..., a_p\}$ er a et fixpunkt for både σ og τ, og så er $\tau \cdot \sigma(a) = a = \sigma \cdot \tau(a)$.

Hvis $a = a_i$ for $i = 2, 3, ..., p-1$, er $\tau \cdot \sigma(a_i) = \tau(a_{i+1}) = a_i$ og $\sigma \cdot \tau(a_i) = \sigma(a_{i-1}) = a_i$.

Endvidere er $\tau \cdot \sigma(a_1) = \tau(a_2) = a_1$ og $\sigma \cdot \tau(a_1) = \sigma(a_p) = a_1$.

Og endelig er $\tau \cdot \sigma(a_p) = \tau(a_1) = a_p$ og $\sigma \cdot \tau(a_p) = \sigma(a_{p-1}) = a_p$. ■

Definition 547 *En* 2*-cykel* $(a_i\ a_j)$ *kaldes en* ***transposition***

Sætning 548 *En transposition er sin egen inverse.*

Bevis. Overlades til læseren. Husk også at redegøre for de elementer, som ikke indgår i cykelnotationen. ■

Sætning 549 *Enhver* p*-cykel er et produkt af* $p-1$ *transpositioner.*

Der gælder nemlig, at hvis $a_1, a_2, ..., a_p$ *er* p *forskellige elementer i en endelig mængde* A*, så er*

$$(a_1\ a_2\ \ ...\ a_p) = (a_1\ a_p)\,(a_1\ a_{p-1}) \cdots (a_1\ a_3)\,(a_1\ a_2)\,. \tag{13.34}$$

Bevis. Vi skal altså vise at de to sider af lighedstegnet er samme afbildning, altså at de afbilder alle elementer i A ens.

Hvis $a \notin \{a_1, a_2, ..., a_p\}$, er a et fixpunkt for begge sider af (13.34).

Elementet a_1 afbildes ved venstresiden i a_2. På højresiden afbilder den første transposition (læst fra højre!) a_1 i a_2, og det fixes af resten af transpositionerne.

Hvis $i = 2, ..., p-1$, afbildes a_i af venstresiden i a_{i+1}. På højresiden fixes a_i af de første $i-2$ transpositioner, afbildes så i a_1 af den $i-1$ te transposition, sendes så videre til a_{i+1} af den $i$te transposition og fixes endelig af resten.

Endelig afbilder venstresiden a_p i a_1. På højresiden fixes a_p af alle transpositionerne på nær den sidste, som sender a_p over i a_1. ■

Eksempel 550 *Figur 13.2 antyder at permutationen σ defineret i (13.7) kan skrives som et produkt af tre disjunkte cykler nemlig*

$$\sigma = (1\ 5\ 8) \cdot (2\ 7\ 4\ 6) \cdot (3)\,. \tag{13.35}$$

Den sidste cykel er faktisk overflødig da det er identitetspermutationen. Vi kan altså skrive

$$\sigma = (1\ 5\ 8) \cdot (2\ 7\ 4\ 6)\,. \tag{13.36}$$

Du kan selv checke at σ faktisk er lig med det angivne produkt.

Er det nu en tilfældighed, at denne permutation kan skrives som produkt af disjunkte cykler? Nej, det kan alle permutationer:

Sætning 551 *Enhver permutation af en endelig mængde kan på entydig måde skrives som produkt af disjunkte cykler af længde større end* 1.

Algoritme 552 *Inden vi giver et egentligt bevis for sætningen, angiver vi en algoritme til at bestemme de disjunkte cykler, som en permutation er bygget op af:*

Lad σ være en permutation af mængden A

1. Udvælg et tilfældigt element for eksempel a_1 i A og dan dets successive billeder ved σ:

$$a_1, a_2 = \sigma(a_1), a_3 = \sigma(a_2), ..., a_k = \sigma(a_{k-1}), ... \tag{13.37}$$

Da A er endelig, må der før eller siden opstå gentagelser i denne følge. Antag, at det sker første gang når vi danner $\sigma(a_p)$, således at $a_1, a_2, ..., a_p$ er forskellige, men at $a_{p+1} = \sigma(a_p)$ er lig med a_q for et $q = 1, 2, ..., p$. Nu er det let at indse, at q må være lig med 1*, altså at den første gentagelse må være a_1. Thi hvis $2 \leq q \leq p$, har vi at $a_{p+1} = \sigma(a_p) = \sigma(a_{q-1})$ og $a_p \neq a_{q-1}$ men det er umuligt, da σ er injektiv.*

Vi har dermed fået beskrevet en cykel $\gamma_1 = (a_1\ a_2\ \ ...\ a_p)$ således at σ virker ligesom cyklen på cyklens elementer.

2. Hvis alle A's elementer optræder i den fundne cykel, er $\sigma = (a_1\ a_2\ \ ...\ a_p)$ og vi er færdige. Hvis ikke, vælges et element a_1' i A forskelligt fra $a_1, a_2, ..., a_p$. Som ovenfor ses på de successive billeder af a_1' under σ:

$$a_1', a_2' = \sigma(a_1'), a_3' = \sigma(a_4'), ..., a_k' = \sigma(a_{k-1}'), .. \tag{13.38}$$

Disse må være forskellige fra $a_1, a_2, ..., a_p$, thi hvis $\sigma(a_k')$ var det første element i følgen, som også optrådte i følgen $a_1, a_2, ..., a_p$, ville $\sigma(a_k')$ være et billede af et element i $\{a_1\ a_2\ \ ...\ a_p\}$ og et billede af et element, som ikke ligger i denne

mængde. Det er umuligt, da σ er injektiv. Som ovenfor danner de successive billeder derfor en cykel $\gamma_2 = \left(a'_1\ a'_2\ \ ...\ a'_{p'}\right)$, som er disjunkt fra den forrige cykel.

3. Ved at fortsætte på denne måde findes disjunkte cykler γ_i. Processen må slutte efter et endeligt antal trin, da der kun er endeligt mange elementer i A. Produktet af de fundne cykler er da lig med σ. Hvis σ har fixpunkter, er nogle af de fundne cykler 1-cykler. Disse kan udelades fra produktet, hvorved opnås at alle cykler har længde større end 1.

Øvelse 553 *Prøv ovenstående algoritme på σ defineret i (13.7)og τ defineret i (13.12).*

I forbindelse med ovenstående algoritme er det nyttigt at indføre noget notation:

Definition 554 *Lad σ være en permutation af en endelig mængde A, og lad $a \in A$. Mængden af successive billeder af a under σ kaldes* ***banen*** *bestemt ved a og betegnes B_a:*

$$B_a = \left\{a, \sigma(a), \sigma^2(a), \sigma^3(a), ...\right\}. \tag{13.39}$$

Bemærkning 555 *Som vi argumenterede for i fremstillingen af algoritmen, består banen bestemt ved a af en følge af p elementer: $a = a_1, a_2, ..., a_p$ så*

$$a_2 = \sigma(a_1) \tag{13.40}$$
$$a_3 = \sigma(a_2) \tag{13.41}$$
$$\vdots \tag{13.42}$$
$$a_p = \sigma(a_{p-1}) \tag{13.43}$$
$$a_1 = \sigma(a_p). \tag{13.44}$$

Antallet af elementer i banen (altså p) kaldes ***banens længde****.*

Til en bane B svarer en cykel γ nemlig $(a_1\ a_2\ \ ...\ a_p)$. Den er entydigt bestemt ved at

$$\gamma(a) = \sigma(a) \text{ hvis } a \in B \tag{13.45}$$
$$\gamma(b) = b \text{ hvis } b \notin B \tag{13.46}$$

Det er klart at

$$a \in B_b \Leftrightarrow B_a = B_b. \tag{13.47}$$

Fixpunkter bestemmer baner af længde 1 som også kaldes et-punkts-baner.

Sætning 556 *Lad σ være en permutation af en endelig mængde A. Da udgør banerne for σ en klassedeling af A. Med andre ord:*

1. *Banerne er ikke tomme.*
2. *Hvis to baner har et element tilfælles er de ens.*

3. Foreningsmængden af alle banerne er hele A.

Bevis. 1. og 3. følger af, at $a \in B_a$.

2: Hvis $c \in B_a$ og $c \in B_b$, så findes naturlige tal m og n, så $c = \sigma^n(a)$ og $c = \sigma^m(b)$. Hvis $m = n$, er $a = b$ (fordi σ^n er injektiv). Hvis $m > n$, er $\sigma^n(a) = \sigma^n(\sigma^{m-n}(b))$, og da σ^n er injektiv, følger det at $a = \sigma^{m-n}(b)$. Det vil sige at $a \in B_b$, så ifølge (13.47) er $B_a = B_b$. ■

Nu kan vi præcisere og bevise sætning 551.

Sætning 557 ***Cykelsætningen****: Lad σ være en permutation på en endelig mængde A, og lad $B_1, B_2, ..., B_n$ betegne banerne for σ og $\gamma_1, \gamma_2, ..., \gamma_n$ de tilhørende cykler.*

1. *Da gælder*
$$\sigma = \gamma_1 \cdot \gamma_2 \cdots \gamma_n. \tag{13.48}$$
2. *Hvis et-punkts-banerne fjernes fra denne fremstilling fås en fremstilling af σ som produkt af disjunkte cykler af længde større end 1. Denne fremstilling er entydig på nær rækkefølgen af de indgående cykler.*

Bevis. 1. Vi skal vise, at for ethvert $a \in A$ gælder
$$\sigma(a) = \gamma_1 \cdot \gamma_2 \cdots \gamma_n(a). \tag{13.49}$$
Lad $a \in A$. Da ligger a ifølge foregående sætning i netop én bane B_i. Ifølge (13.45) og (13.46) gælder $\sigma(a) = \gamma_i(a)$, hvorimod a og $\sigma(a)$ er et fixpunkt for de andre cykler. Derfor gælder:
$$\gamma_1 \cdot \gamma_2 \cdots \gamma_n(a) = \gamma_i(a) = \sigma(a). \tag{13.50}$$

2. Da cyklerne svarende til et-punkts-banerne er identitetspermutationen, kan de fjernes fra $\gamma_1 \cdot \gamma_2 \cdots \gamma_n$ uden at ændre permutationen. Dermed er det bevist, at enhver permutation kan skrives som produkt af cykler med længde større end 1.

Entydigheden: Antag at σ er skrevet som et produkt af disjunkte cykler af længde større end 1:
$$\sigma = \gamma_1 \cdot \gamma_2 \cdots \gamma_k \tag{13.51}$$
Hvis a er et fixpunkt for σ så optræder a ikke i noget γ. Hvis derimod a ikke er fixpunkt for σ, da optræder a i præcist en af cyklerne γ_j. Men så må hele banen hørende til a også optræde i samme cykel, og cyklen må være cyklen hørende til banen hørende til a. Altså er cyklerne i fremstillingen netop de entydigt bestemte cykler hørende til de baner, som ikke er et-punkts-baner. ■

Bemærkning 558 *Hvis alle baner er et-punkts-baner, er permutationen identitetspermutationen. I det tilfælde vedtager vi at sige, at et produkt med nul faktorer fremstiller identitetspermutationen.*

Sætning 559 *1. Enhver permutation σ af $A = \{a_1, a_2, ..., a_n\}$ kan skrives som et produkt af transpositioner.*

2. Er $b \in A$ kan transpositionerne i produktet vælges på formen $(b\ a)$ for $a \in A$.

*3. Transpositionerne i produktet også vælges på formen $(a_i\ a_{i+1})$ (**nabo-transpositioner**).*

Bevis. 1. Følger af cykelsætningen, ifølge hvilken enhver permutation kan skrives som et produkt at cykler, og sætning 549, ifølge hvilken enhver cykel kan skrives som at produkt af transpositioner.

2. Skriv σ som et produkt af transpositioner iflg. 1. Enhver af disse transpositioner er af formen $(a_i\ a_j)$. Hvis $a_i = b$ eller $a_j = b$ er transpositionen allerede på formen $(b\ a)$ så vi lader den stå. Hvis $a_i, a_j \neq b$ så er

$$(a_i\ a_j) = (b\ a_i)\,(b\ a_j)\,(b\ a_i)\,. \tag{13.52}$$

(Bevis selv dette. Husk at du skal checke alle $a \in A$). Hvis højresiden indsættes i produktet i stedet for venstresiden, fås et produkt af den ønskede form.

3. ifølge 2. kan enhver permutation på $A = \{a_1, a_2, ..., a_n\}$ skrives som et produkt af transpositioner af formen $(a_1\ a_i)$ $i \neq 1$. Vi har altså vist pkt. 3, hvis vi kan vise, at en permutation af formen $(a_1\ a_j)$ kan skrives som et produkt af nabotranspositioner. Det vil vi gøre ved induktion efter i.

Induktionsstart: $i = 2$: $(a_1\ a_2)$ er allerede på den ønskede form.

Induktionsskridtet: Antag at $(a_1\ a_i)$ er et produkt af nabotranspositioner. Da

$$(a_1\ a_{i+1}) = (a_i\ a_{i+1})\,(a_1\ a_i)\,(a_i\ a_{i+1}) \tag{13.53}$$

(overvej), kan $(a_1\ a_{i+1})$ skrives som produkt af nabotranspositioner.

Ifølge princippet om matematisk induktion kan enhver transposition af formen $(a_1\ a_j)$ derfor skrives som et produkt af nabotranspositioner. Deraf følger 3. ■

Bemærkning 560 *Opskrivningen af en permutation som produkt af transpositioner er ikke entydig.*

13.3 Cykeltype og fortegn

Definition 561 *Lad σ være en permutation af $A = \{a_1, a_2, ..., a_n\}$. Da indføres følgende betegnelser om banerne og deres længder:*

$m(\sigma) =$ antal baner for σ.

$m_p(\sigma) =$antal baner for σ af længde p.

Den endelige følge $m_1(\sigma), m_2(\sigma), ..., m_n(\sigma)$ kaldes σ's cykeltype. Den skrives ofte som et formelt produkt:

$$1^{m_1} 2^{m_2} \cdots n^{m_n} \tag{13.54}$$

Eksempel 562 *Permutationen σ i eksempel 13.35 har cykeltypen $1^1 3^1 4^1$.*
En permutation af form

$$(*)\,(*)\,(**)\,(****)\,(****)\,(****)\,(*****)\,, \tag{13.55}$$

hvor cyklerne er disjunkte, har cykeltypen $1^2 2^1 4^3 5^1$.

Bemærkning 563 *Da et-punkts-baner svarer til fixpunkter ses at*

$$m_1(\sigma) = \text{ antal fixpunkter for } \sigma \tag{13.56}$$

Det er vigtigt at huske at medtage et-punkts-banerne når man skal finde cykeltypen for en permutation.

Sætning 564 *Lad σ være en permutation af A. Da gælder*

$$m(\sigma) = \sum_p m_p(\sigma) \tag{13.57}$$

$$|A| = \sum_p p \cdot m_p(\sigma) \tag{13.58}$$

Bevis. Den første identitet overlades til læseren.

Den anden udsiger, at man kan tælle antallet af elementer i A ved at tælle antallet af elementer i hver af σ's disjunkte cykler og lægge antallene sammen. ■

Ud fra σ's cykeltype kan vi nu definere dens **fortegn** (skrives $\text{sign}(\sigma)$). Det er enten $+1$ eller -1, og defineres mere præcist sådan:

Definition 565 *Lad σ være en permutation på en endelig mængde A. Fortegnet for σ defineres som*

$$sign(\sigma) = (-1)^k \text{ , hvor } k = |A| - m(\sigma). \tag{13.59}$$

*Hvis fortegnet er $+1$ (altså hvis k er lige), siges σ at være **lige**.*
*Hvis fortegnet er -1 (altså hvis k er ulige), siges σ at være **ulige**.*

Eksempel 566 *Betragt permutationen σ defineret i (13.7) som vi skrev som produkt af disjunkte cykler i (13.35). Her er $k = |A| - m(\sigma) = 8 - 3 = 5$ så $sign(\sigma) = (-1)^k = (-1)^5 = -1$. Permutationen er altså ulige. Bemærk at det er nødvendigt at medtage et-punkts-banen $\{3\}$.*

Eksempel 567 *Identiteten: Antag at $|A| = n$. Identiteten har alle punkter som fixpunkter, så den har n et-punkts-baner. Altså er $m(\sigma) = n$ og $k = n - n = 0$, så $sign(1_A) = (-1)^0 = 1$. Identitetspermutationen er altså en lige permutation på enhver mængde.*

Eksempel 568 *p-cykel: Antag at $|A| = n$. En p-cykel σ vil da se ud som følger*

$$(*)\,(*)\,(*)\,(*)\,(*\,*\,*\,*\,*)\,, \tag{13.60}$$

hvor der er $n-p$ 1-cykler og én p-cykel. Altså er $m(\sigma) = n-p+1$ hvorfor $k = n-(n-p+1) = p-1$. Fortegnet er altså $sign\,(\sigma) = (-1)^{p-1}$. Vi har altså flg. huskeregel:

Huskeregel: For en p-cykel gælder:

$$\sigma \text{ er ulige, hvis } p \text{ er lige} \tag{13.61}$$

$$\sigma \text{ er lige, hvis } p \text{ er ulige} \tag{13.62}$$

Specielt har en transposition fortegn $sign(\tau) = -1$ og er altså ulige.

Vi vil nu vise at $\text{sign}(\mu \cdot \sigma) = \text{sign}(\mu) \cdot \text{sign}(\sigma)$. Først vises et lemma:

Lemma 569 *Lad τ være en transposition på A og σ en vilkårlig permutation på A. Da gælder*

$$m(\tau\sigma) = m(\sigma) \pm 1. \tag{13.63}$$

Bevis. Lad $A = \{a_1, a_2, ..., a_n\}$, og $\tau = (a\ b)$. Opskriv banerne $B_a(\sigma)$ og $B_b(\sigma)$ på følgende måde:

$$B_a(\sigma) = \{a = a_1, a_2, ..., a_p\} \tag{13.64}$$

$$\text{hvor } \sigma(a_i) = a_{i+1} \text{ når } 1 \le i \le p-1, \text{ og } \sigma(a_p) = a_1 \tag{13.65}$$

$$B_b(\sigma) = \{b = b_1, b_2, ..., b_q\} \tag{13.66}$$

$$\text{hvor } \sigma(b_i) = b_{i+1} \text{ når } 1 \le i \le q-1, \text{ og } \sigma(b_q) = b_1 \tag{13.67}$$

Der er nu to tilfælde: enten er $B_a(\sigma)$ og $B_b(\sigma)$ disjunkte, eller også er $B_a(\sigma) = B_b(\sigma)$ (iflg. sætning 556).

1. Antag at $B_a(\sigma) \cap B_b(\sigma) = \emptyset$. Da er

$$B_a(\tau\sigma) = \{a = a_1, a_2, ..., a_p, b = b_1, b_2, ..., b_q\}\,. \tag{13.68}$$

For at indse det betragtes elementerne $(\tau\sigma)^i(a)$ for $i = 1, 2, ..., p+q$:

$$\tau\sigma(a) = \tau(\sigma(a)) = \tau(a_2) = a_2 \tag{13.69}$$

$$(\tau\sigma)^2(a) = \tau\sigma(\tau\sigma(a)) = \tau\sigma(a_2) = \tau(a_3) = a_3 \tag{13.70}$$

$$\vdots \tag{13.71}$$

$$(\tau\sigma)^p(a) = \tau\sigma((\tau\sigma)^{p-1}(a) = \tau\sigma(a_p) = \tau(a_1) = \tau(a) = b \tag{13.72}$$

$$(\tau\sigma)^{p+1}(a) = \tau\sigma(b) = b_2 \tag{13.73}$$

$$\vdots \tag{13.74}$$

$$(\tau\sigma)^{p+q}(a) = \tau\sigma(b_q) = \tau(b_1) = \tau(b) = a \tag{13.75}$$

Altså bliver de to σ-baner $B_a(\sigma)$ og $B_b(\sigma)$ slået sammen til én $\tau\sigma$-bane. De andre σ-baner forbliver baner for $\tau\sigma$ (overvej). Altså fås i dette tilfælde at $m(\tau\sigma) = m(\sigma) - 1$.

2. Antag dernæst at $B_a(\sigma) = B_b(\sigma)$. Da $b \in B_b$, er $b = a_{k+1}$ for $1 \leq k \leq p$. Altså kan $B_a(\sigma)$ skrives:

$$B_a(\sigma) = \{a = a_1, a_2, ..., a_k, b = b_1, b_2, ..., b_{p-k}\} \tag{13.76}$$

$$\text{hvor } \sigma(a_i) = a_{i+1} \text{ når } 1 \leq i \leq k-1, \tag{13.77}$$

$$\sigma(b_i) = b_{i+1} \text{ når } 1 \leq i \leq p-k-1 \tag{13.78}$$

$$\sigma(a_k) = b = b_1, \tag{13.79}$$

$$\sigma(b_{p-k}) = a = a_1. \tag{13.80}$$

Men så er $B_a(\tau\sigma) = \{a = a_1, a_2, ..., a_k\}$ og $B_b(\tau\sigma) = \{b = b_1, b_2, ..., b_{p-k}\}$ (overvej), medens de øvrige σ-baner forbliver $\tau\sigma$-baner. I dette tilfælde gælder altså $m(\tau\sigma) = m(\sigma) + 1$.

I begge tilfælde har vi altså vist at $m(\tau\sigma) = m(\sigma) \pm 1$. ■

Sætning 570 *Hvis μ og σ er permutationer på en endelig mængde A, gælder at*

$$sign(\mu\sigma) = sign(\mu) \cdot sign(\sigma). \tag{13.81}$$

Bevis. Antag først at μ er en transposition. Da gælder iflg. den foregående sætning:

$$|A| - m(\mu\sigma) = |A| - m(\sigma) \pm 1, \tag{13.82}$$

hvorfor

$$\text{sign}(\mu\sigma) = (-1)^{|A|-m(\mu\sigma)} = (-1)^{|A|-m(\sigma)\pm 1} \tag{13.83}$$

$$= (-1) \cdot (-1)^{|A|-m(\sigma)} = (-1)\text{sign}(\sigma). \tag{13.84}$$

Antag dernæst at σ er et produkt af k transpositioner : $\sigma = \tau_1\tau_2\cdots\tau_k$. Da gælder ved successiv brug af (13.84) og eksempel 567 at

$$\text{sign}(\sigma) = (-1)^k \text{sign}(1_A) = (-1)^k. \tag{13.85}$$

Ifølge sætning 559 kan enhver permutation skrives som et produkt af transpositioner.

Antag at μ kan skrives som et produkt af l transpositioner og σ kan skrives som et produkt af k transpositioner. Da kan $\mu\sigma$ skrives som et produkt af $k + l$ transpositioner. Derfor gælder at

$$\text{sign}(\mu\sigma) = (-1)^{k+l} = (-1)^l \cdot (-1)^k = \text{sign}(\mu) \cdot \text{sign}(\sigma). \tag{13.86}$$

■

I ovenstående bevis fik vi vist følgende sætning, som også er et let korollar af sætningen:

Korollar 571 *Hvis σ er et produkt af k transpositioner, da er*

$$sign(\sigma) = (-1)^k. \tag{13.87}$$

Bemærkning 572 *Det betyder altså at en lige permutation er et produkt af et lige antal transpositioner, medens en ulige permutation er et produkt af et ulige antal transpositioner. Dette anføres ofte som en definition af fortegnet for en permutation. Men denne definition har den ulempe, at det ikke a priori er klart at den er veldefineret. Vi bemærkede jo ovenfor, at når en permutation fremstilles som et produkt af transpositioner, er deres antal ikke entydigt bestemt.*

Den definition vi har givet har den fordel, at den klart er veldefineret. Og derfra og fra korollar 571 kan vi nu slutte, at en permutation ikke på en gang kan skrives som et produkt af et lige og et ulige antal transpositioner. Så selv om antallet af transpositioner i en produktfremstilling af en permutation ikke er entydigt bestemt, er det altså fastlagt om antallet er lige eller ulige.

Bemærkning 573 ***Metoder til fortegnsbestemmelse****. Når man skal bestemme fortegnet for en permutation, kan man altså prøve at skrive permutationen som et produkt af transpositioner. Det er dog ofte for besværligt.*

Den letteste metode er normalt, at skrive permutationen som et produkt af disjunkte cykler. Deres fortegn kan findes ved huskereglerne (13.61) og(13.62), og fortegnet for produktet kan så bestemmes ved at gange cyklernes fortegn sammen. Her gør det ikke noget om man glemmer 1-cyklerne, for de har jo fortegn $+1$.

Eksempel 574 *Betragt permutationen σ defineret i (13.7) som vi skrev som produkt af disjunkte cykler i (13.35): $\sigma = (1\ 5\ 8) \cdot (2\ 7\ 4\ 6) \cdot (3)$. Der er to cykler af ulige længde, som derfor har fortegn 1 og én cykel af lige længde, som derfor har fortegn -1. fortegnet for σ er derfor $1 \cdot 1 \cdot (-1) = -1$ så permutationen er ulige. Vi ville have fået det samme hvis vi havde udeladt et-punkts-banen og skrevet: $\sigma = (1\ 5\ 8) \cdot (2\ 7\ 4\ 6)$.*

Sætning 575 *Lad $A = \{a_1, a_2, ..., a_n\}$ være en mængde med n elementer ($n \geq 2$). Da er der $n!/2$ lige permutationer og $n!/2$ ulige permutationer af A.*

Bevis. Lad A_n betegne mængden af lige permutationer og B_n betegne mængden af ulige permutationer. Lad endvidere τ være en transposition f.eks. (a_1, a_2) Vi kan da definere en afbildning $f : A_n \longrightarrow B_n$ ved følgende regel.

$$f(\sigma) = \tau \cdot \sigma. \tag{13.88}$$

Da en transposition er ulige følger af sætning 570, at f afbilder en lige permutation i en ulige permutation, altså at f faktisk er en afbildning $A_n \longrightarrow B_n$. Vi vil nu vise at f er bijektiv.

1. Injektivitet: Antag at $f(\sigma) = f(\mu)$ altså at

$$\tau \cdot \sigma = \tau\mu. \tag{13.89}$$

Men så er

$$\tau(\tau\sigma) = \tau(\tau\mu), \tag{13.90}$$

og da $\tau = \tau^{-1}$, følger at

$$(\tau^{-1}\tau)\sigma = (\tau^{-1}\tau)\mu, \tag{13.91}$$

så

$$1_A \cdot \sigma = 1_A \cdot \mu, \tag{13.92}$$

hvoraf vi slutter, at $\sigma = \mu$. Altså er f injektiv.

2. Surjektivitet: Lad $\mu \in B_n$, altså μ ulige. Da er $\tau\mu$ lige, altså $\tau\mu \in A_n$, og

$$f(\tau\mu) = \tau(\tau\mu) = (\tau\tau)\mu = \mu. \tag{13.93}$$

Altså er ethvert element i A_n et billede af et element i B_n så f er surjektiv.

Afbildningen f er altså en bijektion mellem A_n og B_n. Ifølge Sætning 458 har A_n og B_n derfor samme antal elementer. Endvidere ved vi fra Sætning 487 at mængden S_n af alle permutationer af A har $n!$ elementer. Da A_n og B_n er disjunkte, følger derfor af sætning 465 at

$$2\,|A_n| = 2\,|B_n| = |A_n| + |B_n| = |S_n| = n! \tag{13.94}$$

hvoraf vi kan se, at $|A_n| = |B_n| = n!/2$. ■

13.4 Opgaver

1. Betragt de to permutationer

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 7 & 3 & 6 & 5 & 2 \end{pmatrix} \tag{13.95}$$

og

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 4 & 7 & 1 & 6 & 3 \end{pmatrix}. \tag{13.96}$$

(a) Bestem $\mu\sigma$ og $\sigma\mu$.

(b) Bestem permutationernes fixpunkter.

(c) Bestem permutationernes inverser.

(d) Opskriv de to permutationer og deres inverser som produkt af disjunkte cykler.

e. Bestem fortegnet for μ, σ, μ^{-1}, σ^{-1}, $\mu\sigma$ og $\sigma\mu$.

2. Betragt følgende to permutationer opskrevet i direkte notation:

$\sigma = (2, 9, 8, 5, 3, 1, 4, 6, 7)$ og $\mu = (3, 2, 1, 9, 8, 5, 7, 6, 4)$.

(a) Bestem $\mu\sigma$ og $\sigma\mu$.

(b) Bestem permutationernes fixpunkter.

(c) Bestem permutationernes inverser.

(d) Opskriv de to permutationer og deres inverser som produkt af disjunkte cykler.

(e) Bestem fortegnet for μ, σ, μ^{-1}, σ^{-1}, $\mu\sigma$ og $\sigma\mu$.

3. På mængden $\{1,2,3,4,5,6,7,8\}$ er givet følgende produkt af cykler: $\sigma = (1\ 5\ 6\ 7\ 3)\,(8\ 2\ 4\ 6)\,(3\ 5\ 7)$.

(a) Opskriv σ som produkt af disjunkte cykler.

(b) Bestem σ's fortegn.

(c) Angiv den inverse til σ.

4. Lad $A = \{1,2,3,4,5,6,7\}$. Betragt følgende produkt af cykler på A :

$$(4\ 1\ 3\ 5)\,(5\ 6\ 3)\,. \tag{13.97}$$

Opskriv produktet med tabelnotation.

5. Opskriv cyklen (1 3 5 4 2) som produkt af transpositioner.

6. Opskriv permutationen

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 5 & 2 & 1 & 8 & 7 \end{pmatrix} \tag{13.98}$$

som et produkt af transpositioner

7. Opskriv μ og σ fra opgave 1 som produkter af transpositioner. Brug resultatet til at opskrive μ^{-1} og σ^{-1} som produkter af transpositioner og til at bestemme permutationernes fortegn.

8. Lad σ være en p-cykel. Vis at σ^2 er en p-cykel, når p er ulige, og at σ^2 ikke er en cykel, når p er et lige tal forskellig fra 2.

9. Lad $|A| = 3$. Angiv samtlige mulige cykeltyper for permutationer på A.

10. Lad $|A| = 4$. Angiv samtlige mulige cykeltyper for permutationer på A.

11. Lad $A = \{1,2,3,4,5,6\}$, og lad

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix} \tag{13.99}$$

være en permutation af A.

(a) Skriv σ som produkt af disjunkte cykler.

(b) Beregn σ^{-1} og σ^2.

(c) Find σ's periode (orden), dvs. det mindste naturlige tal n så at $\sigma^n = 1_A$.

12. Lad A være en endelig mængde og σ en permutation af A.

(a) Vis at der eksisterer et naturligt tal n, så at $\sigma^n = 1_A$, Det mindste sådanne tal kaldes σ's periode (orden).

(b) Lad n være perioden af permutationen σ. Lad $k \in \mathbb{N}$. Vis ved at bruge division med rest, at følgende udsagn er ækvivalente

(i) $\sigma^k = 1_A$

(ii) $n \mid k$.

13. Antag at permutationerne σ og τ af mængden A er disjunkte. (Definition 538).
(a) Benyt Sætning 541 til at vise at for $k \in \mathbb{N}$ er

$$(\sigma\tau)^k = \sigma^k\tau^k.$$

(b) Vis at for $k \in \mathbb{N}$ er følgende udsagn ækvivalente:
(i) $(\sigma\tau)^k = 1_A$
(ii) $\sigma^k = \tau^k = 1_A$.
(c) Gør rede for, at perioden for $\sigma\tau$ er lig mindste fælles multiplum af perioden for σ og perioden for τ.

14. Antag at permutationen σ af mængden A er skrevet som et produkt af disjunkte cykler

$$\sigma = \gamma_1 \cdot \gamma_2 \cdots \gamma_m,$$

hvor γ_i er en p_i-cykel for $1 \leq i \leq m$. Vis at perioden af σ er lig mindste fælles multiplum af tallene $p_1, p_2, ..., p_m$. (Her kan den forrige opgave benyttes).

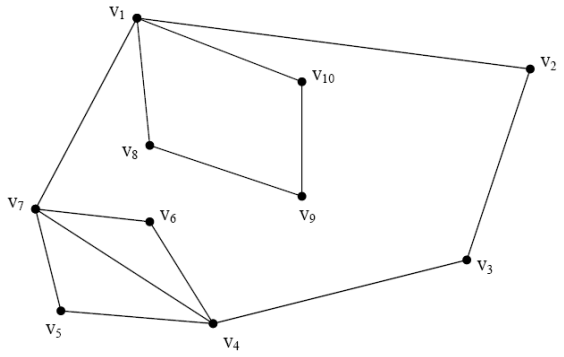
15. Antag at permutatationen σ af mængden A, $|A| = n$, har cykeltype $1^{m_1}2^{m_2}...n^{m_n}$. (Definition 561).
(a) Gør rede for, at permutationen σ^{-1} har samme cykeltype som σ.
(b) Gør rede for at $\sigma = \sigma^{-1}$ præcis når $m_3 = m_4 = ... = m_n = 0$.
(c) Opskriv alle permutationer af mængden $\{1, 2, 3, 4\}$ som er lig deres egen inverse.

16. Lad A og B være endelige mængder. Antag at $|A| < |B|$. Vis at B har mindst så mange cykeltyper som A og at deres antal af mulige cykeltyper er forskellige.

Kapitel 14

Grafer

I matematisk analyse tegner man grafer af funktioner. I dette kapitel skal vi studere en anden slags grafer, nemlig grafer som består af et endeligt antal knuder med et endeligt antal kanter mellem (se figur 14.1)



Figur 14.1: Graf

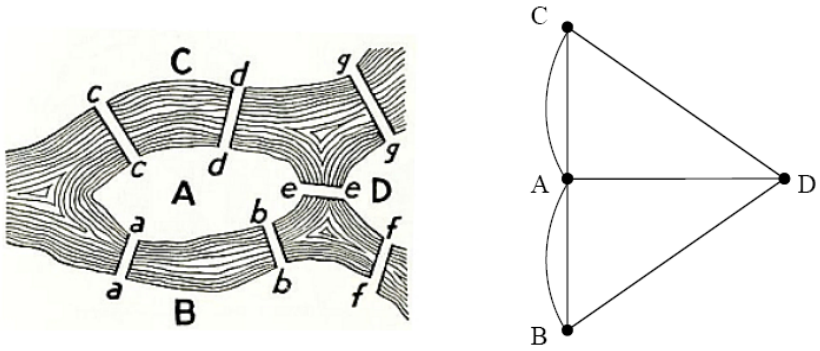
14.1 Definitioner og simple egenskaber

Definition 576 *En **graf** består af en endelig ikke-tom mængde V af **knuder** (eller punkter) (engelsk: vertices) og en endelig mængde E af **kanter** (engelsk: edges) og en funktion f, som til hver kant i E knytter et par af knuder i V. Disse knuder kaldes kantens **endeknuder** eller **endepunkter,** og man siger at kanten forbinder sine endeknuder eller ligger mellem sine endeknuder. Man skriver $G = (V, E, f)$*

Bemærkning 577 *I definitionen siges der ikke noget om, hvad slags objekter knuderne og kanterne er. Når vi tegner grafer, repræsenterer vi knuderne ved*

punkter og kanterne ved streger, men det er kun en illustration. Knuderne og kanterne kan være alt muligt, og det gør grafer til et fleksibelt redskab til at analysere situationer, hvor nogle objekter er relateret til hinanden på en eller anden måde. For eksempel kan knuderne være byer og kanterne flyforbindelser mellem disse byer, eller knuderne kan være mennesker og kanterne kan være telefonsamtaler mellem dem på en bestemt dag, eller knuderne kan være lande og kanterne være landegrænser, således at to lande er forbundet af en kant, hvis de grænser op til hinanden.

Eksempel 578 *I 1737 udgav Leonhard Euler (1707-1783) en artikel, hvori han analyserede, om det ville være muligt at lave en procession i Königsberg, hvor man gik over hver af byens 7 broer præcist én gang. Denne artikel regnes for det første bidrag til grafteorien. Königsberg og dens broer kan ses på figur 14.2. Situationen kan repræsenteres ved grafen ved siden af, hvor knuderne er de fire landområder og kanterne er broerne, som forbinder landområderne.*



Figur 14.2: Broerne i Königsberg.

Definition 579 *Her følger en række definitioner:*

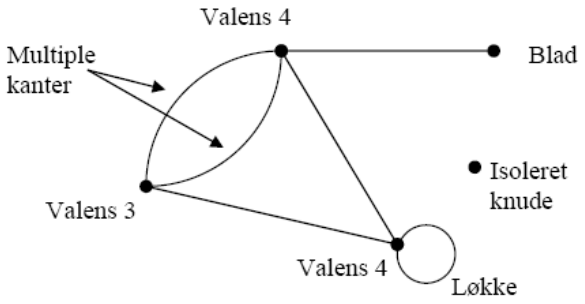
1. ***Løkke**: En kant, som har to ens endepunkter, kaldes en løkke.*
2. ***Multiple kanter**: Hvis to knuder forbindes af mere end en kant, siges disse kanter at være multiple kanter.*
3. ***Naboknuder**: To knuder kaldes naboknuder, hvis de er forbundet af en kant.*
4. ***Valens**: En knudes valens er lig med antallet af kanter, som har endepunkt i knuden (hvor løkker tæller dobbelt). Summen af valenserne af alle grafens knuder kaldes **grafens totale valens**.*
5. ***Isoleret knude**: En knude med valens 0, dvs. en knude, som ikke er endepunkt for nogen kanter, kaldes en isoleret knude.*

6. ***Blad**: En knude med valens* 1 *kaldes et blad.*

7. ***Tom graf**: En graf uden kanter ($E = \emptyset$) kaldes tom.*

8. ***Trivielle graf**: Den tomme graf med én knude kaldes den trivielle graf.*

9. ***Simpel graf**: En graf uden multiple kanter og løkker kaldes en simpel graf.*



Figur 14.3: Grafer: simple begreber.

Bemærkning 580 *I en graf uden multiple kanter kan en kant entydigt angives ved sine endepunkter: $v_i v_j$.*

Sætning 581 *I enhver graf er den totale valens det dobbelte af antallet af kanter. Specielt er den totale valens et lige tal.*

Bevis. Summen af alle knudernes valens er netop lig antallet af gange, en af grafens knuder optræder som endepunkt for en kant. Men det er netop to gange antallet af kanter. ■

Sætning 582 *I enhver graf er der et lige antal knuder med ulige valens.*

Bevis. Hvis der var et ulige antal knuder med ulige valens, ville summen S_u af disse knuders valens være ulige. Summen S_l af valenserne af knuderne med lige valens er lige. Derfor ville summen af alle knudernes valenser $S_u + S_l$ et ulige tal, i modstrid med sætning 581. Derfor må der være et lige antal knuder med ulige valens ■

Nu følger en række definitioner af forskellige måder, man kan vandre rundt i en graf fra knude til knude ved at følge grafens kanter:

Definition 583 *Lad G være en graf, og lad v og w være knuder i G.*

1. ***Rute**: En **rute** fra v til w er en endelig alternerende følge af knuder og kanter i G:*

$$v_0 e_1 v_1 e_2 v_2 ... v_{n-1} e_n v_n, \tag{14.1}$$

*hvor v'erne repræsenterer knuder, og e'erne repræsenterer kanter, og hvor $v_0 = v$ og $v_n = w$, og hvor v_{i-1} og v_i er endepunkter for e_i for alle $i = 1, 2, ..., n$. Antallet n af kanter kaldes rutens **længde**. Den trivielle rute fra v til v består af den ene knude v.*

2. ***Tur**: En tur fra v til w er en rute fra v til w, hvis kanter er indbyrdes forskellige (knuder må gerne gå igen).*

3. ***Vej**: En vej fra v til w er en tur fra v til w, hvis knuder er indbyrdes forskellige.*

4. ***Lukket rute**: En lukket rute er en rute, hvor første og sidste knude er ens. Hvis en rute ikke er lukket kaldes den **åben***

5. ***Lukket tur:** En lukket tur er en tur, hvor første og sidste knude er ens.*

6. ***Kreds**: En lukket tur kaldes en kreds, hvis alle dens knuder er forskellige på nær første og sidste knude, som er ens.*

7. ***Euler-tur**: En tur, som indeholder alle grafens kanter kaldes en Euler-tur i grafen.*

8. ***Lukket Euler-tur**: En lukket tur som indeholder alle kanter i grafen, kaldes en lukket Euler-tur i grafen.*

9. ***Hamilton-vej**: En vej kaldes en Hamilton-vej, hvis den indeholder alle grafens knuder.*

10. ***Hamilton-kreds**: En kreds kaldes en Hamilton-kreds, hvis den indeholder alle grafens knuder.*

Følgende skema indeholder nogle af disse definitioner på mere overskuelig form:

	Gentagne kanter	Gentagne knuder	Begynder og ender i samme knude
rute	tilladt	tilladt	tilladt
tur	nej	tilladt	tilladt
vej	nej	nej	nej
lukket rute	tilladt	tilladt	ja
lukket tur	nej	tilladt	ja
kreds	nej	kun første og sidste	ja

"Euler-" betyder at alle grafens kanter er med.
"Hamilton-" betyder at alle grafens knuder er med.

Bemærkning 584 *Eulers problem om broerne i Königsberg (se eksempel 578) kan formuleres: Eksisterer der en Euler-tur eller en lukket Euler-tur i grafen på figur 14.2.*

Bemærkning 585 *Betragt en graf, hvis knuder er gadekryds og hvis kanter er gader i en by.*

Et gadeløb følger en rute. Hvis det skal være et afvekslende løb skal det følge en tur, og hvis man skal undgå kaos på gadehjørnerne, bør man planlægge løbet langs en vej.

Hvis start og mål skal være samme sted, vælges en lukket rute, hvis den skal være afvekslende vælges en lukket tur, og hvis kaos ved gadehjørner skal undgås, vælges en kreds.

En kontrollant, som skal kontrollere om afstribningen på byens gader er i orden skal (helst) følge en Euler-tur, og hvis han skal ende samme sted som han begynder skal han vælge en lukket Euler-tur.

En kontrollant, som skal kontrollere lyskurvene i alle byens gadekryds, skal helst følge en Hamilton-vej, og hvis han skal ende samme sted som han begyndte, skal han vælge en Hamilton-kreds.

Bemærkning 586 *I mange tilfælde er en rute (tur, vej, kreds) entydigt bestemt ved sin kantfølge. I så tilfælde kan man skrive $e_1e_2...e_n$ i stedet for*

$$v_0e_1v_1e_2v_2...v_{n-1}e_nv_n. \tag{14.2}$$

I mange tilfælde er en rute (tur, vej, kreds) entydigt bestemt ved sin knudefølge. I så tilfælde kan man skrive $v_0v_1v_2...v_{n-1}v_n$ i stedet for

$$v_0e_1v_1e_2v_2...v_{n-1}e_nv_n. \tag{14.3}$$

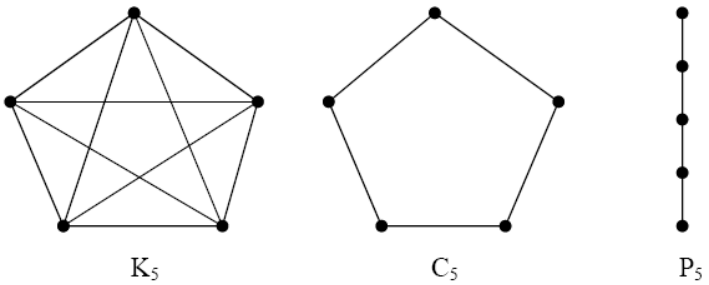
Øvelse 587 *Giv eksempler hvor en rute (tur, vej, kreds) er entydigt bestemt ved sin kant- eller knude-følge, og eksempler hvor dette ikke er tilfældet. Hvilken af de to følger karakteriserer en rute (tur, vej, kreds) i en simpel graf?*

Eksempel 588 *For et givet antal knuder er der tre standard-grafer det er godt at kende:*

1. ***Komplette grafer**: En simpel graf, hvori to vilkårlige forskellige knuder er forbundet med en kant, kaldes en komplet graf. Den komplette graf med n knuder betegnes K_n.*

2. ***Kredsgrafer**: En simpel graf kaldes en kredsgraf hvis dens knuder kan opstilles i en bestemt rækkefølge $v_1, v_2, v_3, ..., v_n$ så at kantmængden netop består af kanterne i kredsen $v_1, v_2, v_3, ..., v_n, v_1$. Kredsgrafen med n knuder ($n \geq 3$) betegnes C_n.*

3. ***Vejgrafer**: En simpel graf kaldes en vejgraf (eller en lineær graf), hvis dens knuder kan opstilles i en bestemt rækkefølge $v_1, v_2, v_3, ..., v_n$, så at kantmængden består af kanterne i vejen $v_1, v_2, v_3, ..., v_n$. Vejgrafen med n knuder betegnes P_n.*



Figur 14.4: De tre standardgrafer med 5 knuder.

Sætning 589 *Lad G være en graf og v, w to forskellige knuder i G. Da er følgende udsagn ækvivalente:*

1. Der findes en rute i G fra v til w.
2. Der findes en tur i G fra v til w.
3. Der findes en vej i G fra v til w.

Bevis. Vi vil vise sætningen ved at vise følgen af implikationer: $3 \Rightarrow 2 \Rightarrow 1 \Rightarrow 3$. De to første implikationer er trivielle.

$1 \Rightarrow 3$: Vi vil vise, at en rute fra v til w enten er en vej, eller den kan udtyndes til en vej fra v til w ved at udelade en række knuder og de mellemliggende kanter. Det vil vi vise ved fuldstændig induktion efter længden af ruten.

Induktionsstart: Hvis der findes en rute af længde 1 fra v til w, er det en en vej fra v til w.

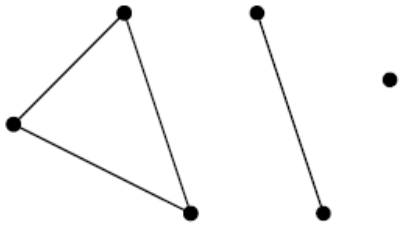
Induktionsskridtet: Antag, at enhver rute af længde $n-1$ eller mindre fra v til w enten er en vej eller kan udtyndes til en vej fra v til w. Antag endvidere, at $v_0e_1v_1e_2v_2...v_{n-1}e_nv_n$ er en rute i G fra v til w. Hvis alle knuderne i ruten er forskellige må alle kanterne også være forskellige, og ruten er en vej i G fra v til w. Hvis derimod der er gengangere i knudefølgen, f.eks. v_k og v_l med $k < l$, så kan man danne en kortere rute fra v til w ved at udelade v_k og alle knuder og kanter mellem v_k og v_l. Denne kan ifølge induktionsantagelsen videre udtyndes til en vej fra v til w.

Altså følger påstanden fra princippet om fuldstændig induktion. ■

Definition 590 *To knuder v, w i en graf G siges at være **vejforbundne,** hvis $v = w$, eller der findes en vej fra v til w.*

*En graf kaldes **sammenhængende,** hvis vilkårlige to knuder er vejforbundne.*

Eksempel 591 *Alle standardgraferne i eksempel 588 er sammenhængende. Derimod er grafen i figur 14.5 ikke sammenhængende*



Figur 14.5: En ikke-sammenhængende graf.

Sætning 592 *Relationen "er vejforbundet med" er en ækvivalensrelation på mængden af knuder i en graf.*

Bevis. Refleksiviet: trivielt

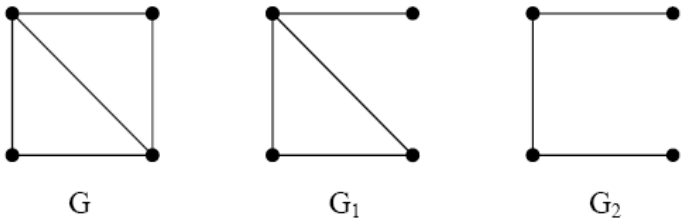
Symmetri: Hvis $v_0e_1v_1e_2v_2...v_{n-1}e_nv_n$ er en vej fra v til w, så er vejen, som fås ved at skrive kanter og knuder i omvendt rækkefølge en vej fra w til v.

Transitivitet: Lad $v'_0e'_1v'_1e'_2v'_2...v'_{n-1}e'_nv'_n$ være en vej fra u til v og $v_0e_1v_1e_2v_2...v_{n-1}e_nv_n$ en vej fra v til w.

Da er $v'_0e'_1v'_1e'_2v'_2...v'_{n-1}e'_nv_0e_1v_1e_2v_2...v_{n-1}e_nv_n$ en rute fra u til w. Ifølge sætning 589 kan denne rute udtyndes til en vej fra u til v. ■

Definition 593 *Lad G være en graf med knudemængde V og kantmængde E. Udvælg en delmængde E' af E og en delmængde V' af V, så at alle endepunkter for kanterne i E' ligger i V'. Så er V' og E' knude- og kantmængde for en graf G', som kaldes en **delgraf** i G.*

Eksempel 594 *Graferne G_1 og G_2 i figur 14.6 er delgrafer af G.*



Figur 14.6: Delgrafer.

Eksempel 595 *En specielt vigtig måde at danne delgrafer fra en graf G er at fjerne en af grafens kanter. Delgrafen G_1 i eksempel 594 er dannet fra G på denne måde.*

Definition 596 *Lad G være en graf. En ækvivalensklasse for relationen "er vejforbundet med" er en mængde V' af knuder. Hvis E' er mængden af de kanter i G som har begge endepunkter i V', så er V' og E' knudemængde og kantmængde for en delgraf af G (overvej). Den kaldes en* ***sammenhængskomponent*** *af G.*

Eksempel 597 *Grafen på figur 14.5 har tre sammenhængskomponenter.*

Bemærkning 598 *En graf G's sammenhængskomponenter er sammenhængende delgrafer af G. Der er ingen kanter fra G som forbinder knuder i forskellige sammenhængskomponenter. Sammenhængskomponenterne er dermed en opdeling af grafen i uforbundne sammenhængende dele.*

Bemærkning 599 *Hvis R er en ækvivalensrelation er sammenhængskomponenterne i dens graf netop ækvivalensklasserne.*

14.2 Euler-ture og Hamilton-kredse

Nu kan vi vende os mod spørgsmålene: Hvilke grafer har en Euler-tur? Hvilke grafer har en lukket Euler-tur? Hvilke grafer har en Hamilton-vej? Hvilke grafer har en Hamilton-kreds? Man overbeviser sig let om, at nogle grafer har sådanne ture, veje og kredse og andre har det ikke. Vi skal vise, at de let kan afgøres om en graf har en lukket eller en åben Euler-tur. Problemerne om Hamilton-veje og -kredse er endnu ikke løst så tilfredsstillende.

Sætning 600 *Lad G være en graf uden isolerede knuder. Da har grafen en lukket Euler-tur, hvis og kun hvis den er sammenhængende og alle knuderne har lige valens.*

Bevis. 1. Antag først, at G har en lukket Euler-tur. Da er G sammenhængende. Thi lad v og w være to vilkårlige knuder i G. Vi har forudsat at ingen knuder er isolerede, så både v og w er endepunkt for en kant. Da alle G's kanter indgår i Euler-turen, forbinder en del af turen v med w. Men ifølge sætning 589 er v og w så vejforbundne. Altså er G sammenhængende.

Endvidere er ethvert punkts valens lige. Lad nemlig v være en vilkårlig knude. Enhver kant der ender i v indgår i den lukkede Euler-tur. Hvis vi gennemløber den lukkede Euler-tur én gang, vil vi altså passere kanterne, der ender i v netop en gang hver. Men hver gang vi ankommer til v langs en kant, forlader vi straks knuden langs en anden kant. Kanterne med endepunkt i v må altså komme i par: en ankomst-kant og en afgangs-kant. Det gælder også den første knude i den lukkede tur, idet den første afgangskant parres sammen med den sidste ankomst-kant. Der er altså et lige antal kanter med endepunkt i v, så v's valens er lige.

Det var den simple implikation i sætningen. Den anden vej er mere overraskende og lidt sværere at vise:

2. Antag nu at G er sammenhængende og at alle knuderne har lige valens. Vi skal da vise, at der findes en lukket Euler-tur i grafen. Det gør vi ved fuldstændig induktion efter antallet af grafens kanter.

Induktionsstart: Hvis der er 1 kant i grafen, må det være en løkke, og så er der klart en lukket Euler-tur. Hvis der er 2 kanter i grafen er det enten to løkker fra samme knude eller to (multiple) kanter, der forbinder de to samme knuder. Igen er eksistensen af en lukket Euler-tur oplagt.

Induktionsskridtet. Antag nu, at $n \geq 3$, og at sætningen er sand for alle grafer med $n-1$ eller færre kanter. Vælg en knude v i grafen, og bestem en lukket tur T af længde ≥ 1, som starter og slutter i v.

At sådan en lukket tur findes, ses på følgende måde: Da v ikke er isoleret er den endepunkt af en kant. Start langs en af disse kanter. Hvis det er en løkke er vi færdige. Ellers har kanten sit andet endepunkt i en anden knude, og da denne knude har lige valens, kan vi fortsætte turen langs en af de andre kanter, som har endepunkt i denne anden knude. Sådan fortsættes indtil vi ikke kan fortsætte turen længere. Da der kun er et endeligt antal kanter i grafen, må turen stoppe. Men den kan ikke stoppe i en anden knude end v, thi hver gang den kommer til en anden knude end v, er der mindst én ubrugt kant, som leder videre. Turen må altså ende i v og er derfor lukket.

Nu fjernes alle de kanter fra G som indgår i den konstruerede lukkede tur T, samt alle de knuder, som derved bliver isolerede. Dermed er det muligt at grafen bliver usammenhængende. Men hver sammenhængskomponent har et kantantal mindre eller lig med $n-1$ og enhver knude har lige valens (overvej). Så ifølge induktionsantagelsen har sammenhængskomponenterne hver en lukket Euler-tur. Endvidere har hver af sammenhængskomponenterne en knude fælles med T (overvej).

Nu kan vi så konstruere en lukket Euler-tur i G: Vi starter i v og går ad turen T, indtil vi kommer til en knude i en af sammenhængskomponenterne. Der tager vi så en omvej ad dens lukkede Euler-tur. Når den er slut er vi tilbage på T og fortsætter ad T indtil næste sammenhængskomponent, hvor vi atter tager en omvej ad dens lukkede Euler-tur. således fortsættes, og når T er slut har vi gennemløbet en lukket Euler-tur i G. ■

Øvelse 601 *Kan man finde en lukket Euler-tur over broerne i Königsberg?*

Sætning 602 *Lad G være en graf uden isolerede knuder. Da har grafen en åben Euler-tur, hvis og kun hvis den er sammenhængende og har præcist to knuder med ulige valens.*

Bevis. 1. Antag, at G har en åben Euler-tur. Da viser et argument helt magen til beviset for 1. i foregående sætning at G er sammenhængende, og at enhver knude på nær begyndelsesknuden og slutknuden har lige valens. Begyndelsesknuden har derimod ulige valens, thi den første afgangs-kant har ingen tilsvarende ankomst-kant, medens de resterende kanter med endepunkt i begyndelsesknuden kommer i par. Ligeså må slutknuden have ulige valens.

2. Antag, at G er sammenhængende og præcist to af dens knuder har ulige valens. Konstruer en ny graf G' ved at tilføje en ny kant e mellem de to knuder med ulige valens. Da er G' en sammenhængende graf uden isolerede knuder, hvori alle knuder har lige valens. Ifølge forige sætning har G' altså en lukket Euler-tur T. Fjernes den ekstra kant e fra T, fås en åben Euler-tur i G. ■

Øvelse 603 *Kan man finde en åben Euler-tur over broerne i Königsberg?*

Øvelse 604 *Hvilke af standard-graferne K_n, C_n, P_n i eksempel 588 har en lukket Euler-tur, og hvilke har en åben Euler-tur ?*

Beviset for sætning 600 giver en algoritme til at bestemme en lukket Euler-tur i en sammenhængende graf G, hvori enhver knude har lige valens. Man kan dog forbedre algoritmen:

Definition 605 *En kant i en graf kaldes en **bro**, hvis grafen bliver usammenhængende når kanten fjernes.*

Algoritme 606 ***Fleurys algoritme*** *Uformel forklaring: Start med at vælge en vilkårlig knude v_0 i G. Vi bygger da successivt en tur op ved at starte langs en kant e_1 til en ny knude v_1. Fjern kanten e_1 fra G. Hvis der kun er én kant e_2 videre fra knuden v_1, går vi videre ad den til en ny knude v_2, og fjerner både e_2 og v_1 fra grafen. Hvis der derimod er flere kanter videre fra v_1 vælger vi én e_2, som ikke er en bro. Vi går da videre ad e_2 til en knude v_2 og fjerner kun e_2 fra grafen. Således fortsættes til vi når tilbage til v_0.*

Algoritmen afviger fra den vi brugte i beviset for sætning 600 ved at vi hele tiden sørger for at gå ad en kant, som ikke er en bro (hvis det overhovedet er muligt). Den har den fordel, at når den slutter, har den frembragt en lukket Euler-tur. Der bliver altså ikke nogle mindre delgrafer til overs, som man så skal tilføje til turen, for at den bliver en Euler-tur. Algoritmen har dog den ulempe, at det ikke er klart at den virker. Der er to spørgsmål som skal afklares:

1. Hvis der er flere kanter videre fra en knude, hvorfor er der da en af dem, som ikke er en bro?

2. Hvorfor har algoritmen frembragt en lukket Euler-tur når den slutter?

Før vi beviser at Fleurys algoritme virker, skal vi lige vise et lemma, som vi også får brug for i behandlingen af træer:

Lemma 607 *Lad e være en kant i en sammenhængende graf G. Da er følgende tre udsagn ækvivalente:*

1. *Den graf der fremkommer ved at fjerne e er sammenhængende.*
2. *e er kant i en kreds i G.*
3. *e er kant i en lukket tur i G.*

Bevis. Hvis e er en løkke, er udsagnene 1, 2 og 3 alle sande, hvorfor de implicerer hinanden.

Hvis e forbinder to forskellige knuder, og der er en anden kant, der forbinder de to knuder, er alle tre udsagn også sande (overvej).

Vi kan derfor antage, at e forbinder to forskellige knuder v og w, og at e er den eneste kant som forbinder v og w.

Vi vil vise $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.

$1 \Rightarrow 2$: Lad G' være den graf, der fremkommer ved at fjerne e. Vi antager altså at G' er sammenhængende. Der findes derfor en vej i G' mellem v og w. Tilføjes nu e til denne vej fås en kreds i G.

$2 \Rightarrow 3$: Klart da en kreds specielt er en lukket tur.

$3 \Rightarrow 1$: Antag at e er en kant i en lukket tur T i G. Vi skal vise at G' er sammenhængende. Først bemærker vi, at når vi fjerner e fra T, fås en tur T' i G' fra v til w. Lad nu u_1 og u_2 være to knuder i G'. Vi skal da vise, at der går en vej i G' mellem dem. Da G er sammenhængende, går der en vej $W : u_1 = v_0e_1v_1e_2v_2...v_{n-1}e_nv_n = u_2$ i G mellem u_1 og u_2. Hvis kanten e ikke indgår i vejen, er det en vej i G', og vi er færdige. Hvis derimod e indgår i denne vej i kombinationen vew, så erstatter vi e med T', som jo er en tur fra v til w. Hvis derimod v og w kommer i omvendt rækkefølge i W (altså wev), så erstatter vi e med T' gennemløbet i omvendt rækkefølge. I begge tilfælde fremkommer der en rute mellem v og w. Men ifølge sætning 589 findes der så en vej mellem v og w. Altså er G' sammenhængende. ■

Algoritme 608 ***Fleurys algoritme.*** *Mere formel forklaring: Lad G være en sammenhængende graf hvori enhver knude har lige valens. Da vil følgende algoritme frembringe en lukket Euler-tur i G.*

1. *Vælg en vilkårlig knude v i G. Sæt $T = v$.*
2. *Hvis der ikke er flere kanter fra v stoppes.*
3. *Hvis der er præcist én resterende kant e fra v for eksempel til w, så slet knuden v og kanten e fra grafen G. Gå til trin 5.*
4. *Hvis der er mere end én resterende kant fra v vælges én, som ikke er en bro, for eksempel e fra v til w. Slet e fra G.*
5. *Tilføj ew til enden af T, erstat w med v og gå til trin 2.*

Bevis. Vi skal vise at algoritmen ikke bryder sammen og at den frembringer det den skal.

1. Algoritmen bryder ikke sammen: Det eneste sted det kan gå galt er i punkt 4. Vi skal vise at hvis vi er nået til punkt 4 i algoritmen, til en knude vi kan kalde v', så er der i den del af grafen, som ikke er blevet slettet, mindst én kant til v', som ikke er en bro. Lad G' betegne den del af grafen, som er tilbage, når vi er nået til dette trin. G' er sammenhængende, thi G er sammenhængende og i hvert af de foregående trin har vi enten (trin 3) fjernet en kant og en derved isoleret knude, eller (trin 4) en kant, som ikke er en bro. Ved begge disse processer forbliver grafen sammenhængende. Der er så to muligheder: Enten er $v' = v_0$, hvor v_0 er den knude vi begyndte algoritmen i, eller også er $v' \neq v_0$.

Hvis $v' \neq v_0$, er der netop to knuder i G', som har ulige valens, nemlig v' og v_0 (overvej), så ifølge sætning 602 er der en åben Euler-tur i G'fra v' til v_0. Da vi er i punkt 4 i algoritmen, og altså er kommet forbi punkt 2 i algoritmen, er der mere end én kant i G' fra v'. Alle kanterne indgår i den åbne Euler-tur. Derfor må denne indeholde knuden v' mere end én gang. Den del af Euler-turen,

som ligger imellem to forekomster af v,' er en lukket tur i G'. Hvis vi nu vælger kanten e, som den første kant i en af disse lukkede ture, følger det af lemma 607, at G' forbliver sammenhængende, når e fjernes.

Hvis $v' = v_0$, har alle knuder i G lige valens. Ifølge sætning 600 har G' derfor en lukket Euler-tur. Da vi er kommet forbi trin 2 ved vi, at der er en kant fra v', og den indgår derfor i den lukkede Euler-tur. Ifølge lemma 607 forbliver G' derfor sammenhængende, hvis denne kant fjernes.

2. Algoritmen frembringer en lukket Euler-tur: Det er klart at algoritmen stopper, thi i hvert gennemløb fjernes en kant, og dem er der kun endelig mange af.

Når algoritmen stopper, er vi kommet til en knude v', hvorfra der ikke udgår nogen kant. Men da den resterende del G' af grafen er sammenhængende, må den bestå af denne ene knude. Knuden v' må altså være lig v_0 (som jo ligger i G'). Altså er turen T en lukket tur, og da der ikke er flere kanter tilbage i G', må de alle være med i T, som altså er en lukket Euler-tur. ■

Bemærkning 609 *Hvis G er en sammenhængende graf med præcist to knuder med ulige valens, er det let at se at hvis Fleurys algoritme startes i en af knuderne med ulige valens, så ender den i den anden knude med ulige valens, og frembringer en åben Euler-tur mellem disse to knuder.*

Der kendes ingen pæne nødvendige og tilstrækkelige betingelser for om en graf har en Hamilton-vej eller -kreds. Det er klart at jo flere kanter, der er i en graf, jo lettere har den ved at have en Hamilton-vej eller -kreds. Her skal uden bevis nævnes en betingelse, der sikrer, at der er nok kanter i grafen til at den har en Hamilton-kreds:

Sætning 610 *Lad G være en sammenhængende simpel graf med n knuder, $n > 2$. G har en Hamilton-kreds, hvis summen af valenserne af to vilkårlige knuder v og w, som ikke er naboer, er større eller lig med n.*

Korollar 611 *Lad G være en sammenhængende simpel graf. med n knuder, $n > 2$. G har en Hamilton-kreds, hvis enhver knude har valens $\geq n/2$.*

Bemærkning 612 *Disse betingelser er dog ikke nødvendige. For eksempel har standardgraferne C_n i 588 en Hamilton-kreds, men for $n \geq 5$ er betingelsen i sætning 610 ikke opfyldt.*

Øvelse 613 *Hvilke af standardgraferne i 588 har en Hamilton-vej, og hvilke har en Hamilton-kreds?*

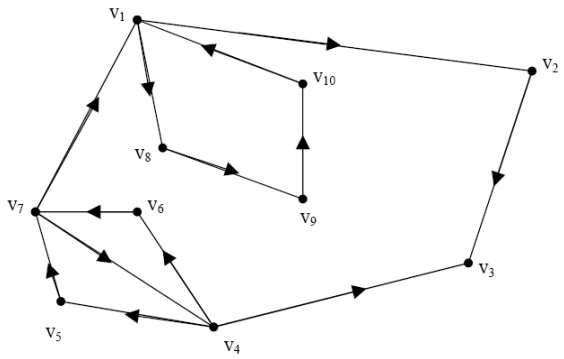
14.3 Orienterede grafer og relationer

Bemærkning 614 *Der er mange varianter af grafer. For eksempel kan en graf være forsynet med et tal på hver kant. Dette tal kan symbolisere en omkostning ved at bevæge sig langs kanten eller et tidsforbrug. I så fald er det en oplagt*

opgave at finde den vej fra en knude til en anden, som minimerer summen af de tilhørende tal. Eller tallet kan betyde en kapacitet for hvor meget der kan transporteres langs kanten. Grafer kommer også med farvede kanter eller knuder. For eksempel kan det berømte firfarveproblem formuleres som et problem om farvning af knuderne i en graf.

Den eneste variant af grafbegrebet vi skal nævne her er orienterede grafer, fordi vi allerede har brugt dem, og kommer til at bruge dem igen. En orienteret graf er simpelthen en graf, hvor hver kant er forsynet med en retning. Den angives ved en pil på kanten. Orienteringen kan angives ved at endeknuderne for kanterne ordnes. Derfor er den formelle definition af en orienteret graf følgende lille variant af definitionen af en graf:

Definition 615 *En **Orienteret graf** (eller digraf (engelsk: directed graph)) består af en endelig ikke-tom mængde V af **knuder** og en endelig mængde E af **kanter** og en funktion f som til hver kant i E knytter et ordnet par (v, w) af knuder i V. Disse knuder kaldes henholdsvist kantens **begyndelsesknude** og **endeknude** og vi siger at kanten går fra v til w.*



Figur 14.7: Orienteret graf.

Bemærkning 616 *Mange af de ovennævnte begreber og resultater kan generaliseres til orienterede grafer. For eksempel defineres orienterede ruter, ture og veje på oplagt måde.*

Hvis en orienteret graf har to orienterede kanter fra v til w siger vi at der er en multipel kant. Vi kalder det altså ikke en multipel kant, bare fordi både (v, w) og (w, v) er orienterede kanter i den orienterede graf.

Definition 617 *En orienteret graf G definerer en relation R_G på mængden V af knuder i G. Relationen R_G er defineret ved at for $v, w \in V$ gælder at*

$$vR_Gw \Leftrightarrow \textit{Der eksisterer en kant i } G \textit{ fra } v \textit{ til } w. \tag{14.4}$$

Bemærkning 618 *Betragt orienterede grafer med en fast knudemængde V. Hvis der tillades multiple kanter, er der flere af disse grafer, som svarer til samme relation på V. Hvis vi derimod kun betragter grafer uden multiple kanter, bestemmer forskellige grafer forskellige relationer (overvej).*

Definition 619 *Omvendt, hvis R er en relation på mængden V, definer vi en orienteret graf G_R uden multiple kanter på følgende måde: G_R har knudemængde V og for $v, w \in V$ er (v, w) en orienteret kant i G_R, hvis vRw.*

Bemærkning 620 *Derved er der etableret en bijektiv korrespondance mellem mængden af relationer på V og orienterede grafer uden multiple kanter med V som knudemængde. Af denne grund ser man ofte en orienteret graf defineret som en relation på en mængde, men denne definition kan ikke indfange grafer med multiple kanter.*

Bemærkning 621 *Vi har allerede brugt den bijektive korrespondance mellem relationer og orienterede grafer uden multiple kanter i kapitel 10. Der observerede vi også følgende sætninger:*

Sætning 622 *En relation R på V er irrefleksiv (altså $\neg vRv$ for alle $v \in V$), hvis og kun hvis dens tilhørende orienterede graf ikke har nogen løkker.*

Sætning 623 *En relation R på V er symmetrisk, hvis og kun hvis alle kanter i dens tilhørende orienterede graf kommer i modsat orienterede par, dvs. når $v, w \in V$ gælder det, at (v, w) er en orienteret kant i G_R, hvis og kun hvis (w, v) er en orienteret kant i G_R.*

Bemærkning 624 *Hvis R er en symmetrisk relation, kan man derfor slå hvert par af modsat orienterede kanter sammen til én uorienteret kant. På den måde fremkommer en (uorienteret) graf uden multiple kanter. Omvendt er det klart, at en (uorienteret) graf uden multiple kanter på denne måde er en graf hørende til en symmetrisk relation.*

Bemærkning 625 *Hvis en relation er refleksiv vil dens tilhørende orienterede graf indeholde en løkke ved hver knude. Ofte vælger man helt at udelade disse løkker, når det på anden vis fremgår at relationen er refleksiv.*

Bemærkning 626 *En refleksiv og symmetrisk relation svarer på denne måde til en simpel graf. Omvendt definerer en simpel graf en refleksiv og symmetrisk relation. Vær dog opmærksom på at man her skal fastlægge at relationen er refleksiv og at vi har valgt at udelade løkkerne.*

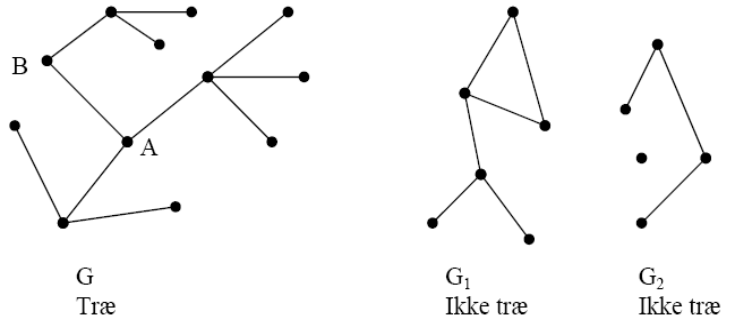
14.4 Træer

I afsnittet om kombinatorik har vi allerede brugt tælletræer til at ordne tælleprocesser. Vi skal nu karakterisere træer som en særlig slags grafer.

Definition 627 *En graf siges at være* ***kredsløs,*** *hvis den ikke indeholder en ikke-triviel kreds.*

En kredsløs graf kaldes også en ***skov****.*

En sammenhængende kredsløs graf kaldes et ***træ.***



Figur 14.8: Træer og ikke-træer.

Bemærkning 628 *Når en sammenhængende graf ikke indeholder nogen kreds betyder det intuitivt, at den ikke indeholder flere kanter end der lige skal til for at få den til at hænge sammen. Hvis grafen har n knuder skal der mindst* $n-1$ *kanter til at gøre den sammenhængende. Faktisk har et træ netop dette minimale antal kanter. Mere præcist gælder følgende sætning:*

Sætning 629 *Lad G være en graf med n knuder. Da er følgende udsagn ækvivalente:*

1. *G er et træ, altså G er sammenhængende og kredsløs.*
2. *G er sammenhængende og har* $n-1$ *kanter.*
3. *G er kredsløs og har* $n-1$ *kanter*

Til brug i beviset for denne sætning bevises først et par lemmaer:

Lemma 630 *Et træ med mere end én knude har en knude med valens* 1 *(det vi har kaldt et blad).*

Bevis. Lad T være et træ med mere end én knude. Vælg en vilkårlig knude v_1. Da T er sammenhængende, er der en kant e_1, som forbinder v_1 med en anden knude v_2. Hvis v_2 har valens 1 er vi færdige. Hvis ikke, er der en anden kant $e_2 \neq e_1$, som forbinder v_2 med en tredie knude v_3. Da der ikke findes en kreds i G, må v_3 være forskellig fra v_1 og v_2. Hvis v_3 har valens 1 er vi færdige. Ellers fortsættes på denne måde. Da G ikke indeholder nogen kreds, leder algoritmen hele tiden til nye knuder. Men da der kun er endeligt mange knuder må processen stoppe ved en knude med valens 1. ■

Korollar 631 *Et træ med mere end én knude har to knuder med valens* 1.

Bevis. I lemmaet ovenfor viste vi, at der findes en knude med valens 1. Hvis vi vælger at begynde algoritmen i beviset for lemmaet med denne knude (v_1), så føres vi til endnu en knude med valens 1. Der er altså to sådanne knuder. ■

Lemma 632 *Hvis T er et træ, og v er en knude heri med valens* 1*, så er den graf, der fremkommer ved at fjerne v og den ene kant, der ender i v, også et træ.*

Lad T være et træ og v en knude i T. Lad endvidere w være et element, der ikke er en knude i T. Hvis vi danner en ny graf T_1 ved at tilføje w til T's knudemængde, og tilføje kanten e med endepunkter v og w til T's kantmængde, så er T_1 et træ

Bevis. Bevis overlades til læseren. ■

Nu er vi klar til

Bevis. af sætning 629. Vi vil vise $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$. Vi antager altså at G er en graf med n knuder

$1 \Rightarrow 2$: Antag at G er sammenhængende og kredsløs. Vi skal bevise at G har $n-1$ kanter. Beviset føres ved induktion efter antallet n af knuder.

Induktionsstart: Hvis grafen har 1 knude, er enhver kant en løkke; men løkker er kredse, og dem er der ingen af. Der må altså være $0 = 1 - 1$ kanter. Altså er påstanden korrekt når $n = 1$.

Induktionsskridtet: Antag at ethvert træ med n knuder har $n-1$ kanter. Lad så G være et træ med $n+1$ knuder og m kanter. Vi skal vise at $(n+1)-1 = m$ altså at $n = m$ Ifølge lemma 630 findes der i G en knude med valens 1. Fjernes denne knude og den kant, der forbinder den med resten af G fra G, vil den resterende graf ifølge lemma 632 være et træ. Og det har n knuder og $m-1$ kanter. ifølge induktionsantagelsen er derfor $m - 1 = (n-1)$, hvoraf $m = n$.

Ifølge princittet om simpel induktion gælder sætningen altså for alle $n \in \mathbb{N}$.

$2 \Rightarrow 3$. Antag at G er sammenhængende og har $n-1$ kanter. Vi skal bevise at G er kredsløs. Det indses ved modstrid. Antag altså, at der er en ikke-triviel kreds i G. Fjernes en af kredsens kanter fra G, er den resterende graf sammenhængende ifølge lemma 607. Hvis der stadig er en ikke triviel kreds i denne graf, fjernes en af dens kanter, osv. indtil vi når til en sammenhængende graf uden kredse. Det er et træ med samme knuder som G, og ifølge det netop viste har det $n-1$ kanter. Men det er umuligt, for vi antog at der var $n-1$ kanter i G, og træet er fremkommet ved at fjerne nogle kanter fra G.

$3 \Rightarrow 1$. Antag endelig at G er kredsløs og har $n-1$ kanter. Vi skal vise at G er sammenhængende. Antag at G har k sammenhængskomponenter. Vi skal da vise at $k = 1$. Hver sammenhængskomponent er sammenhængende og kredsløs, altså et træ. Hvis antallet af knuder i den $i$te sammenhængskomponent kaldes n_i, så har den altså iflg. det allerede viste $n_i - 1$ kanter. Men så er antallet af kanter i hele G altså lig med

$$\sum_{i=1}^{k}(n_i - 1) = \sum_{i=1}^{k} n_i - k = n - k. \tag{14.5}$$

Men vi havde antaget, at antallet af kanter var $n-1$. Altså kan vi slutte at $k=1$. ■

Definition 633 *Lad G være en sammenhængende graf. Da siges et træ med samme knuder og med en kantmængde, som er en delmængde af G's kantmængde, at være et* ***udspændende træ*** *for grafen. Den fremkommer af grafen ved successivt at fjerne kanter i kredse.*

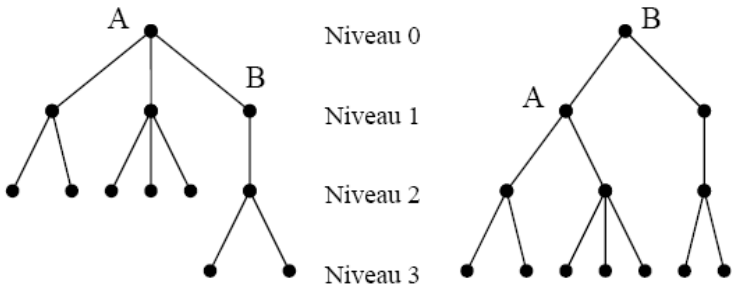
Bemærkning 634 *Hvis R er en ækvivalensrelation kan vi som bemærket i 375 repræsentere R ved en simpel graf. Hvis man heri successivt fjerner alle kanter i kredse ender man med en skov hvis sammenhængskomponenter er udspændende træer for hver af relationens ækvivalensklasser.*

Definition 635 *Et træ, hvori der er udvalgt en bestemt knude, kaldes et* ***træ med rod****, og den udvalgte knude kaldes* ***roden****.*

Træer med rod tegnes normalt med roden øverst! Derunder tegnes på samme vandrette linje de knuder i træet, som er forbundet med roden. Disse knuder siges at være på niveau 1. Derunder tegnes de knuder (forskellig fra de foregående) som er forbundet med knuderne på niveau 1. De er på niveau 2. osv. Generelt siges en knude at være på niveau n, hvis den er forbundet med roden ved en vej af længde n.

Øvelse 636 *Overvej, at denne definition af niveau er veldefineret.*

Eksempel 637 *På figur 14.9 er tegnet to træer med rod. De svarer til træet i figur 14.8. Det venstre har A som rod, og det højre har B som rod.*



Figur 14.9: Træer med rod.

På denne måde udstyres et træ med rod med en naturlig ordning, nemlig den hvor kanterne er orienteret nedad. Et træ med rod kan derfor opfattes som et ordnet træ.

Eksempel 638 *De tælletræer, vi tegnede i kapitel 3, er træer med rod.*

Et stamtræ, der illustrerer en stamfaders eller stammoders slægt, er et træ med stamfaderen eller stammoderen som rod, hvis der da ikke er sket indgiftning i slægten.

Sætning 639 *En orienteret graf G er et træ med rod, hvis og kun hvis der findes en knude v_0 i G, hvorfra der er en entydig orienteret rute til enhver anden knude i grafen, men ingen ikke-triviel vej fra v_0 til v_0.*

Bevis. Lad G være en orienteret graf.

1. Antag, at G er et træ med roden v_0. Da G er sammenhængende findes der en vej fra v_o til enhver anden knude i G og vi har konstrueret orienteringen så at alle kanterne i vejen er orienteret fra v_0 til den anden knude. Denne orienterede rute er entydig, thi hvis der var to forskellige orienterede ruter til en knude ville det give anledning til en kreds. Der er ingen ikke-triviel vej fra v_0 til v_0 fordi G er kredsløs.

2. Antag omvendt, at der findes en knude v_0 i G, hvorfra der er en entydig orienteret rute til enhver anden knude i grafen, men ingen ikke-triviel vej fra v_0 til v_0. Da er grafen sammenhængende. Vi skal altså blot vise at grafen, vi får ved at se bort fra orienteringen i G, er kredsløs. Det gøres ved kontraposition.

Antag, et der findes en ikke-orienteret ikke-triviel kreds $v_0'v_1'...v_0'$ i G. Lad T være den entydigt bestemte orienterede rute $v_0v_1...v_nv_0'$ fra v_0 til v_0'. Kredsen kan ikke være en løkke eller et modsat orienteret kantpar, thi det ville føre til at der ville være mere end en rute fra v_0 til v_0'. Kredsen indeholder derfor mindst to kanter fra v_0 til to forskellige knuder. Det er derfor muligt at vælge en kant i kredsen, (antag det er $v_0'v_1'$) som ikke ender i v_n. Der er nu to muligheder: Denne kant $v_0'v_1'$ er rettet fra v_1' mod v_0' eller den er rettet fra v_0' mod v_1'.

a. Hvis $v_0'v_1'$ er rettet fra v_1' mod v_0' er der to forskellige orienterede veje fra v_0 til v_0' nemlig T og vejen fra v_0 til v_1' efterfulgt af $v_1'v_0'$. Disse to veje er forskellige da $v_1' \neq v_n$.

b. Hvis $v_0'v_1'$ er rettet v_0' mod v_1', gås ud ad denne kant og videre rundt i kredsen, så langt man kan komme med orienteringen. Derved fremkommer en ikke tom orienteret vej $T' = v_0'v_1'v_1'v_2'...v_{k-1}'v_k'$ som er orienteret i den angivne retning, og således at $v_k'v_{k+1}'$ er orienteret modsat og så $v_1' \neq v_n$.

Ingen af knuderne v_i' $(i = 1, 2, ..., k)$ kan være lig en af knuderne $v_0, v_1, ..., v_n$ på vejen fra v_0 til v_0'. Antag nemlig at i er det mindste tal så v_i' er lig en af knuderne $v_0, v_1, ..., v_n$. Hvis $v_i' = v_0$ ville der være en orienteret ikke-triviel vej $v_0v_1...v_nv_0'v_1'v_1'v_2'...v_{i-1}'v_i'$ fra v_0 til v_0 i modstrid med forudsætningerne, og hvis $v_i' = v_j$ $(1 \leq j \leq n)$ ville der være to forskellige veje fra v_0 til v_j nemlig $v_0v_1...v_j$ og $v_0v_1...v_nv_0'v_1'v_1'v_2'...v_{i-1}'v_i'$ i modsætning til forudsætningerne.

Altså er $v_0v_1...v_nv_0'v_1'v_1'v_2'...v_{k-1}'v_k'$ en orienteret vej fra v_0 til v_k'. Men hvis T'' er den orienterede vej fra v_0 til v_{k+1}, så vil T'' efterfulgt af $v_{k+1}v_k$ også være en orienteret vej fra v_0 til v_k. Og den er forskellig fra $v_0v_1...v_nv_0'v_1'v_1'v_2'...v_{k-1}'v_k'$ thi $v_{k+1} \neq v_{k-1}$ (overvej). Men det er i modstrid med den forudsatte entydighed. ■

Bemærkning 640 *Den foregående sætning gør det muligt at definere et træ med rod som en orienteret graf G, hvori der findes en knude v_0, hvorfra der er en entydig orienteret rute til enhver anden knude i grafen, men ingen ikke-triviel orienteret vej fra v_0 til v_0.*

Definition 641 *Et træ med rod, hvor hver knude er forbundet med højst to knuder på det underliggende niveau, kaldes et* ***binært træ****.*

Eksempel 642 *Binære træer er særligt vigtige i datalogi.*

Øvelse 643 *Tegn et eksempel på et binært træ med 4 niveauer og 13 knuder.*

14.5 Opgaver

1. Tegn en graf med følgende specifikationer, eller vis at den ikke eksisterer:
(a) En graf med fire knuder med valens $1, 1, 2$ og 3.
(b) En graf med fire knuder med valens $1, 1, 3$ og 3.
(c) En simpel graf med fire knuder med valens $1, 1, 3$ og 3.

2. (a) Er det muligt i en gruppe af 9 personer, at hver person er ven med præcist 5 andre? Vi antager her at vennerelationen er symmetrisk, så at x er ven med y, hvis y er ven med x. Tegn en passende graf til at afgøre spørgsmålet.
(b) Er det muligt i en gruppe af 15 personer, at hver person er ven med præcist 3 andre?
(c) Er det muligt i en gruppe af 4 personer, at hver person er ven med præcist 3 andre?

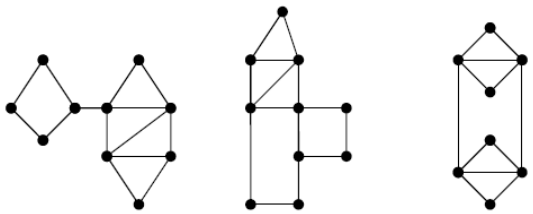
3. Eksisterer der en simpel graf, hvori alle knuder har lige valens?

4. (a) Tegn K_6.
(b) Vis at K_n har $\frac{n(n-1)}{2}$ kanter.
(c) Vis at en simpel graf med n knuder højst har $\frac{n(n-1)}{2}$ kanter.
(d) Findes der en simpel graf som har dobbelt så mange kanter som den har knuder?
(e) Findes der en graf der har dobbelt så mange kanter som den har knuder?

5. (a) Find en øvre grænse for valensen af en knude i en simpel graf med n knuder.
(b) Findes der en simpel graf med fire knuder med forskellig valens?
(c) Findes der en simpel graf hvor alle knuderne har forskellig valens?

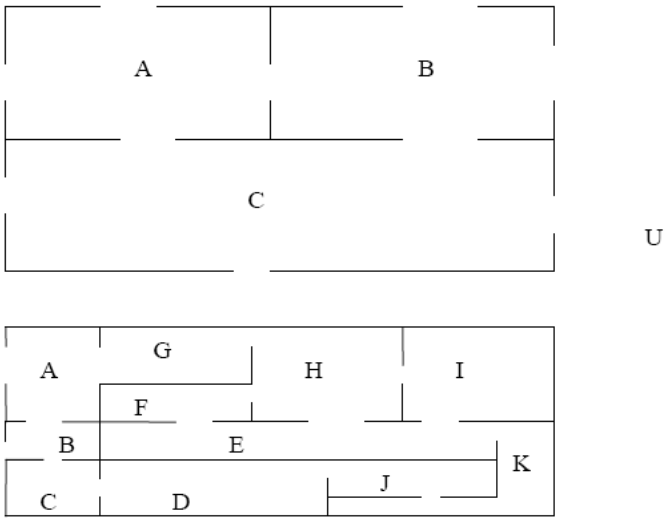
6. (a) Argumenter for at grafen i figur **14.1** har en lukket Euler-tur.
(b) Brug algoritmen i beviset for sætning 600 til at finde en lukket Euler-tur i grafen, idet du starter med vejen $v_1v_2v_3v_4v_7v_1$: .
(c) Brug Fleurys algoritme til at finde en lukket Euler-tur i grafen.

7. Afgør om graferne i figur 14.10 har en lukket eller en åben Euler-tur, og find om muligt en ved at bruge Fleurys algoritme.



Figur 14.10: Har graferne Euler-ture?

8. I figur 14.11 er tegnet en plan over to huse. Afgør for hver af dem, ved at tegne passende grafer, om det er muligt at gå en tur gennem huset, således at man går gennem hver dør præcist en gang. (Det er en god idé at opfatte haven som et rum). Kan man starte og slutte samme sted.? Brug Fleury's algoritme til at bestemme turen, hvis den er mulig.



Figur 14.11: Er der Euler-ture gennem dørene?

9. Find to eksempler på grafer, som har en lukket Euler-tur men ingen Hamilton-kreds.

10. 10. Bestem den totale valens i et træ med n knuder

11. 11. Tegn grafer med følgende specifikationer, eller vis at de ikke findes:

(a) træ, 9 kanter, 9 knuder.
(b) graf, sammenhængende, 9 knuder, 9 kanter.
(c) graf, kreds-løs, 9 knuder, 6 kanter.
(d) træ, 6 knuder, total valens 14.
(e) træ, 5 knuder, total valens 8.
(f) graf, sammenhængende, 6 knuder, 5 kanter, har ikke triviel kreds.
(g) graf, 2 knuder, en kant, ikke et træ.
(h) graf, kreds-løs, 7 knuder, 4 kanter.

12. Vis at en sammenhængende graf med n knuder har mindst $n-1$ kanter.

13. Find det maksimale antal knuder i et binært træ med n niveauer.

Kapitel 15

Ordningsrelationer

15.1 Partiel og total ordning

Det er normalt at bruge betegnelsen $\leq$ (læses "mindre eller lig (med)) for en ordningsrelation, også når der er tale om andre ordningsrelationer end den velkendte ordning på de reelle tal. Vi skal følge denne konvention i dette afsnit.

Definition 644 *En relation $\leq$ på en mængde M kaldes en (partiel) **ordningsrelation** (eller en (partiel) ordning), hvis den er refleksiv, antisymmetrisk og transitiv, d.v.s hvis den opfylder følgende tre betingelser:*

1. *Refleksivitet: For alle $a \in M$ gælder det at $a \leq a$*
2. *Antisymmetri: For alle $a, b \in M$ gælder det at $(a \leq b) \wedge (b \leq a) \Rightarrow a = b$.*
3. *Transitivitet: For alle $a, b, c \in M$ gælder at $(a \leq b) \wedge (b \leq c) \Rightarrow a \leq c$*

En mængde forsynet med en ordning kaldes en ordnet mængde. Den ordnede mængde M forsynet med ordningen $\leq$ betegnes $(M, \leq)$.

Øvelse 645 *Bevis følgende simple sætning: Lad $(M, \leq)$ være en partielt ordnet mængde og $A \subseteq M$. Da definerer $\leq$ også en partiel ordning på A.*

Eksempel 646

1. *Den almindelig kendte ordning $\leq$ af de reelle tal er en ordningsrelation.*
2. *Relationen $\subseteq$ er en ordningsrelation på potensmængden $P(M)$ af en given mængde M.*
3. *"Være efterkommer af" er en ordningsrelation på mængden af mennesker, hvis man siger at en person er efterkommer efter sig selv.*
4. *Relationen $=$ på en mængde M er en ordningsrelation. Den derved ordnede mængde $(M, =)$ kaldes den totalt uordnede mængde.*

Bemærkning 647 *I det første af disse eksempler kan to vilkårlige elementer a og b sammenlignes, i den forstand at enten er $a \leq b$ eller $b \leq a$. Noget tilsvarende gælder ikke i almindelighed i de sidste tre eksempler. Vi siger, at den første ordningsrelation er en total ordning.*

Definition 648 *En ordningsrelation $\leq$ på en mængde M kaldes en* ***total ordningsrelation*** *(eller en* ***total ordning****), hvis der for alle $a, b \in M$ gælder enten $a \leq b$ eller $b \leq a$. I så fald kaldes $(M, \leq)$ en totalt ordnet mængde.*

Bemærkning 649 *Man bruger også betegnelsen lineær ordningsrelation om en total ordningsrelation. Det antyder ideen om, at man kan tænke sig en totalt ordnet mængde $(M, \leq)$ anbragt langs en ret linje, således at $a \leq b$, hvis a ligger til venstre for b eller under b hvis linjen er lodret. Hvis en partielt ordnet mængde ikke er totalt ordnet, kan den ikke tænkes anbragt således.*

Eksempel 650 *De reelle tal med den sædvanlige ordning er en totalt ordnet mængde.*

Bemærkning 651 *Hvis A er en delmængde af en partielt ordnet mængde $(M, \leq)$, vil relationen $\leq$ anvendt på A også være en ordningsrelation. Derved bliver $(A, \leq)$ en ordnet mængde. Man siger at A arver ordensstrukturen fra $(M, \leq)$. Hvis $(M, \leq)$ er en totalt ordnet mængde, bliver enhver delmængde, udstyret med den nedarvede ordning, ligeledes totalt ordnet. For eksempel bliver alle delmængder af $\mathbb{R}$ totalt ordnede mængder, når de udstyres med den sædvanlige ordning. Talmængderne $\mathbb{N}$, $\mathbb{Z}$ og $\mathbb{Q}$ er altså totalt ordnede mængder, når de udstyres med den sædvanlige ordning.*

Øvelse 652

1. *Overvej om $(P(M), \subseteq)$ kan være totalt ordnet for passende valg af M.*
2. *Angiv en uendelig delmængde af $P(\mathbb{N})$, som er totalt ordnet ved relationen $\subseteq$.*

Definition 653 *Lad $(M, \leq)$ være en partielt ordnet mængde, og lad $a, b \in M$. Vi siger da at*

- *$a < b$ hvis $a \leq b$ og $a \neq b$*
- *$a \geq b$ hvis $b \leq a$*
- *$a > b$ hvis $b < a$*

Sætning 654 *Lad $(M, \leq)$ være en partielt ordnet mængde, og lad $a, b \in M$. Da gælder:*

1. *$a < b \wedge b \leq c \Rightarrow a < c$*
2. *$a \leq b \wedge b < c \Rightarrow a < c$*

Bevis. Overlades til læseren. ■

Definition 655 *En partielt ordnet mængde $(M, \leq)$ siges at opfylde* ***trikotomiloven*** *(eller tredelingsloven) hvis der for vilkårlige elementer $a, b \in M$ gælder, at præcist et af udsagnene*

$$a < b,\ a = b,\ b < a \tag{15.1}$$

er sandt.

Sætning 656 *En partielt ordnet mængde $(M, \leq)$ er totalt ordnet, hvis og kun hvis den opfylder trikotomiloven.*

Bevis. Antag først, at $(A, \leq)$ er totalt ordnet. Vi skal vise, at tredelingsloven gælder. Lad derfor $a, b \in A$ være vilkårlige. Vi skal vise, at mindst et af udsagnene $a < b$, $a = b$ og $b < a$ er sandt. Dette kan vises ved at vise, at såfremt de to første er falske, da må det tredie være sandt (overvej).

Vi antager derfor $\neg(a < b)$ og $\neg(a = b)$ og skal da vise $b < a$.

Da $a < b$ per definition betyder $(a \leq b \wedge a \neq b)$, har vi:

$$\neg(a < b) \equiv \neg(a \leq b) \vee a = b.$$

Da vi har antaget $\neg(a < b)$ og $a \neq b$, kan vi således slutte $\neg(a \leq b)$. Da A er totalt ordnet, slutter vi heraf, at $b \leq a$. Da også $b \neq a$, har vi da per definition $b < a$.

Antag nu omvendt, at $(A, \leq)$ tilfredstiller tredelingsloven. Vi skal da vise, at A er totalt ordnet. Lad da $a, b \in A$ være vilkårlige. Vi skal vise, at mindst et af udsagnene $a \leq b$ og $b \leq a$ er sandt. Dette kan vises ved at antage, at $a \leq b$ er falsk og på grundlag heraf slutte, at $b \leq a$ gælder.

Vi antager derfor $\neg(a \leq b)$. Nu, da $a < b$ betyder $(a \leq b \wedge a \neq b)$, er implikationen $a < b \Rightarrow a \leq b$ altid sand; da vi har antaget, at $a \leq b$ er falsk, kan derfor $a < b$ ikke være sand. Tilsvarende kan $a = b$ ikke være sand, da i så fald $a \leq b$ også ville være det.

Vi har nu indset, at udsagnene $a < b$ og $a = b$ begge er falske. Da $(A, \leq)$ tilfredsstiller tredelingsloven, slutter vi, at $b < a$. Men da er også $b \leq a$ sand som ønsket. ■

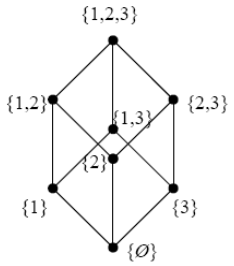
Vi vil nu se på den orienterede graf hørende til en ordningsrelation på en endelig mængde.

Sætning 657 *Lad $(M, \leq)$ være en partielt ordnet endelig mængde. Da har dens orienterede graf ingen andre orienterede kredse end løkkerne.*

Bevis. Antag at $a, a_1, a_2, ..., a_n, a$ er en kreds fra a til a. Antag at kredsen har længde større end 1. Da indeholder den et $a_i \neq a$ hvorom det gælder at $a \leq a_i$ og $a_i \leq a$. Fra antisymmetrien følger at $a = a_i$. Det fører altså til modstrid, hvorfor vi kan slutte at de eneste lukkede kredse i den orienterede graf er løkker. ■

Bemærkning 658 ***Hasse diagram****: Da en ordningsrelation på en endelig mængde A er refleksiv indeholder den løkker ved alle elementer i A. Når man illustrerer en ordningsrelation undlader man normalt at tegne løkkerne. Desuden undlader man at tegne de kanter, som er konsekvenser af den transitive egenskab. Altså hvis der er en pil mellem a og b og der er en pil mellem b og c så udelades pilen mellem a og c. Man udelader også normalt de små cirkler om kanternes navne og erstatter dem med punkter. Endelig tegnes den orienterede graf, så alle pilene peger opad. Når det er gjort er pilen overflødig og udelades. Det resulterende diagram kaldes et* ***Hasse diagram.***

Eksempel 659 *På figur 15.1 er tegnet et Hasse diagram for ordningsrelationen $\subseteq$ på $P\{1,2,3\}$. Prøv selv at tegne den tilhørende orienterede graf.*



Figur 15.1: Hasse diagram.

Bemærkning 660 *Vær opmærksom på at konventionen angående orienteringen er den modsatte af konventionen for træer. Træer er orienteret nedad, Hasse diagrammer er orienteret opad. Det betyder at når ordningsrelationen er $\leq$ så ligger større elementer højere oppe i Hasse diagrammet end mindre elementer.*

Bemærkning 661 *Hvis der i et Hasse diagram går en rute opad fra a til b så er $a \leq b$. Her betyder opad ikke bare at ruten slutter højere oppe end den begynder, men at hver kant i ruten går opad. Hvis a og b ikke forbindes med en rute som går opad eller nedad er a og b ikke relateret.*

Bemærkning 662 *Hvis en ordning på en endelig mængde er total er dens Hasse diagram en vejgraf (lineær graf) stillet på højkant.*

15.2 Maximalt og største element. Supremum

Definition 663 *Et element a i en partielt ordnet mængde $(M, \leq)$ kaldes et et* ***maximalt element,*** *hvis der ikke eksisterer et $b \in M$, så $a < b$.*

Et element a i en partielt ordnet mængde $(M, \leq)$ kaldes et et ***største element,*** *hvis $x \leq a$ for alle $x \in M$.*

Bemærkning 664 *Ved første øjekast kunne det se ud som om "maximalt element" og "største element" er en og samme ting. Hvis ordningen på M ikke er total, så dækker de to begreber dog ikke over det samme. Betragt for eksempel delmængden $M = \{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\}\}$ i $P\{1,2,3\}$ med ordningen $\subseteq$. Denne mængde har tre maximale elementer, nemlig $\{1,2\},\{1,3\}$, og $\{2,3\}$, men den har ingen største element.*

Eksempel 665 *Det højre endepunkt b er et maximalt element og det største element i det lukkede interval $[a,b]$ med den sædvanlige ordning.*

Eksempel 666 *Det åbne interval $]a,b[$ har intet maximalt element.*

Bevis. Antag at $c \in]a,b[$. Vi skal vise at c ikke er et maximalt element dvs. vi skal vise at der findes et $d \in]a,b[$ så $c < d$. Betragt tallet $d = \frac{b+c}{2}$ (midt mellem b og c). Da $c < b$ er

$$d = \frac{b+c}{2} < \frac{b+b}{2} = b, \tag{15.2}$$

og da $a < b$ og $a < c$, er

$$a = \frac{a+a}{2} < \frac{b+c}{2} = d. \tag{15.3}$$

Altså ligger d i intervallet $]a,b[$. Men da $c < b$ fås også

$$c = \frac{c+c}{2} < \frac{c+b}{2} = d. \tag{15.4}$$

Altså er c ikke et maximalt element i $]a,b[$. ■

Øvelse 667 *Bevis at intervallet $[a,\infty[$ ikke har noget maximalt element.*

Sætning 668 *Hvis en partielt ordnet mængde har et største element, så er det entydigt bestemt.*

Bevis. For at vise denne entydighedssætning benytter vi den strategi vi lagde i Bemærkning 65.

Antag at a og b begge er største elementer i en ordnet mængde $(M,\leq)$. Da $a \in M$, og b er et største element i M, gælder at

$$a \leq b. \tag{15.5}$$

Da $b \in M$, og a er et største element i M, gælder at

$$b \leq a. \tag{15.6}$$

Men da relationen $\leq$ er antisymmetrisk, betyder det at $a = b$. ■

Hvis en ordnet mængde har et største element, kan vi altså tale om *det* største element i mængden.

Sætning 669 *Hvis en partielt ordnet mængde har et største element, så er det også et maximalt element i mængden og det er det eneste maximale element i mængden.*

Bevis. Antag at a er det største element i den partielt ordnede mængde $(M, \leq)$. Lad $b \in M$. Så er $b \leq a$ og derfor er det udelukket at $a < b$. Altså er a et maximalt element.

Antag endvidere at c er et maximalt element i M. Da a er det største element i M gælder at $c \leq a$. Men da c er et maximalt element er det udelukket at $c < a$. altså må der gælde at $c = a$. Det vil sige at a er det eneste maximale element i M. ■

Sætning 670 *I en totalt ordnet mængde er et maximalt element også det største element.*

Bevis. Overlades til læseren. ■

Definition 671 *Et element a i en partielt ordnet mængde $(M, \leq)$ kaldes et **minimalt element**, hvis der ikke eksisterer et $b \in M$ så $b < a$*

*Et element a i en partielt ordnet mængde $(M, \leq)$ kaldes et **mindste element,** hvis $a \leq x$ for alle $x \in M$.*

Øvelse 672 *Betragt Hasse diagrammet på figur 15.1. Angiv en delmængde af $P\{1, 2, 3\}$ som har minimale elementer men intet mindste element.*

Sætning 673 *Hvis en partielt ordnet mængde har et mindste element, så er det entydigt bestemt.*

Sætning 674 *Hvis en partielt ordnet mængde har et mindste element, så er det også et minimalt element i mængden og det er det eneste minimale element i mængden.*

Øvelse 675 *Bevis de to foregående sætninger.*

Øvelse 676 *Bevis at det venstre endepunkt a er minimum af det lukkede interval $[a, b]$, og bevis at de åbne intervaller $]a, b[$ og $]-\infty, b[$ ikke har noget minimum.*

Definition 677 *Lad A være en delmængde af en partielt ordnet mængde $(M, \leq)$, og lad $x \in M$.*

1. *x kaldes en **majorant** for A hvis $a \leq x$ for alle $a \in A$.*
2. *x kaldes en **minorant** for A hvis $x \leq a$ for alle $a \in A$.*

*Hvis der findes en majorant for A siges A at være **opadtil begrænset**. Hvis der findes en minorant for A siges A at være **nedadtil begrænset**. Hvis A er både opadtil og nedadtil begrænset, kaldes A for **begrænset***

Eksempel 678 *Tallet* 1000 *er en majorant for* $[0,1]$. *Intervallet* $[0,1]$ *er altså opadtil begrænset.*

Øvelse 679 *Giv eksempler på intervaller, som er/ikke er opadtil og nedadtil begrænsede. I de tilfælde de er begrænsede, giv da flere majoranter/minoranter.*

Øvelse 680 *Bestem en majorant for delmængden* $M = \{\{1\},\{2\},\{3\},\{1,2\},\{1,3\}\}$ *i* $P\{1,2,3\}$ *med ordningen* $\subseteq$.

Bemærkning 681 *Betegnelserne majorant og minorant hedder "upper bound" og "lower bound" på engelsk. De er i flere bøger fejlagtigt blevet oversat til "øvre og nedre grænse" på dansk. Disse betegnelser kan imidlertid virke vildledende. Normalt tænker man sig jo en grænse som liggende lige der, hvor noget begynder eller ender. Den danske grænse ligger ved Kruså ikke ved Hamborg. Men i matematik kan en majorant altså ligge "langt fra mængden", bare den er større eller lig med alle elementerne i mængden. Det er derfor vi i disse noter har valgt betegnelserne majorant og minorant. Når der er tale om talmængder bruger man også betegnelserne* ***overtal*** *og* ***undertal*** *for majorant og minorant.*

Bemærkning 682 *Vi har bemærket, at en majorant eller minorant for en delmængde af en ordnet mængde ikke behøver at ligge i delmængden, men det kan ske.*

Sætning 683 *Lad* A *være en delmængde af en partielt ordnet mængde* $(M,\leq)$.

1. *Hvis* M *har et største element* x *så er* x *en majorant for* A.
2. *Hvis* A *har et største element* x, *så er* x *også en majorant for* A.
3. *Hvis* A *har en majorant* x, *som ligger i* A, *da vil* x *være det største element i* A.

Bevis. Overlades til læseren ■

Bemærkning 684 *Vi har set at der (for eksempel i de reelle tal og i* $P\{1,2,3\}$*) er mængder, som ikke har et største eller et mindste element. Hvis mængden er ubegrænset, er der ikke noget at gøre ved det. Men hvis mængden er begrænset, kan man somme tider (for eksempel i de reelle tal), finde en erstatning for maximum og minimum, det såkaldte supremum og infimum. Disse begreber vil vi nu indføre.*

Definition 685 *Lad* A *være en delmængde af en partielt ordnet mængde* $(M,\leq)$. *Et element* b *i* M *kaldes* ***supremum*** *for* A *hvis det er den mindste majorant for* A, *d.v.s opfylder følgende to kriterier:*

1. b *er en majorant for* A, *altså:* $\forall a \in A : a \leq b$.
2. b *er den mindste majorant for* A, *altså: Hvis* x *er en majorant for* A, *da er* $b \leq x$.

Hvis b er supremum for A skriver man: $b = \sup A$.

Øvelse 686 *Betragt $M = \{\{1\}, \{2\}, \{1,3\}\}$ i $P\{1,2,3\}$ med ordningen $\subseteq$. Afgør om M har et supremum, og bestem det hvis det eksisterer.*

Hvis mængden er totalt ordnet, kan det være praktisk at omformulere det andet krav i definitionen af supremum.

Sætning 687 *Lad A være en delmængde af en totalt ordnet mængde $(M, \leq)$. Da er $b = \sup A$, hvis og kun hvis*

1. *b er en majorant for A, altså: $\forall a \in A : a \leq b$.*
2. *$\forall x < b \exists a \in A : x < a$.*

Bevis. Da formuleringen af punkt 1 er det samme som i definitionen af supremum, skal vi bare vise at punkt 2 i definitionen og i sætningen er ækvivalente under forudsætning af at b er en majorant for A:

$$
\begin{aligned}
& b \text{ er den mindste majorant for } A && (15.7)\\
\Leftrightarrow\ & (x \text{ er en majorant for } A\ \Rightarrow b \leq x) && (15.8)\\
\Leftrightarrow\ & (x \text{ er en majorant for } A \Rightarrow \neg\,(x < b)) && (15.9)\\
\Leftrightarrow\ & ((x < b) \Rightarrow x \text{ ikke en majorant for } A) && (15.10)\\
\Leftrightarrow\ & \forall x < b \exists a \in A : x < a. && (15.11)
\end{aligned}
$$

Den anden omskrivning benytter at M er totalt ordnet.

Den tredie omskrivning er kontraposition.

For at indse den sidste omskrivning, bemærker vi at udsagnet: "x er en majorant for A" jo betyder: $\forall a \in A : a \leq x$, så ved negering ses at udsagnet "x er ikke majorant for A" betyder: $\exists a \in A : x < a$. ■

Eksempel 688 *Intervallet $]1,2[$ har supremum 2.*

Bevis. Vi vil bevise at 2 opfylder de to krav i sætning 687, altså *1.* at 2 er en majorant for $]1,2[$, og *2.* at hvis $x < 2$, da findes et $a \in]1,2[$ så $x < a$.

Bevis for *1.* Ifølge definitionen af $]1,2[$, gælder at et vilkårligt $a \in]1,2[$ opfylder $a < 2$ og desto mere $a \leq 2$. Altså er 2 en majorant for $]1,2[$.

Bevis for *2.* Antag at $x < 2$. Betragt tallet $y = \frac{x+2}{2}$ midt mellem x og 2. Da $x < 2$ gælder det at

$$y = \frac{x+2}{2} < \frac{2+2}{2} = 2. \tag{15.12}$$

Hvis $1 < y$, vælges $a = y$. Hvis $y \leq 1$, vælges $a = 3/2$. I begge tilfælde gælder at $a \in]1,2[$ (overvej dette), og

$$x = \frac{x+x}{2} < \frac{x+2}{2} = y \leq a. \tag{15.13}$$

Vi har altså fundet et element a i $]1,2[$, som opfylder $x < a$.

■

Øvelse 689 *Bevis, at hvis $k \in \mathbb{R}$, vil intervallet $]-\infty, k[$ have supremum k.*

Sætning 690 *Lad A være en delmængde af en partielt ordnet mængde $(M, \leq)$. Hvis A har et supremum, er det entydigt bestemt.*

Bevis. Antag at x og y begge er supremum for A. Da x er den mindste majorant, og y er en majorant, gælder $x \leq y$. Da y er en mindste majorant, og x er en majorant, gælder $y \leq x$. Da relationen $\leq$ er antisymmetrisk, kan vi fra $x \leq y$ og $y \leq x$ slutte, at $x = y$. ■

Sætning 691 *Lad A være en delmængde af en partielt ordnet mængde $(M, \leq)$. Hvis A har et største element a, da vil a også være supremum for A.*

Bevis. Antag at a er det største element i A. Ifølge sætning 683 er a en majorant for A. Vi skal altså bare vise, at det er den mindste. Antag altså at x er en majorant for A. Da $a \in A$ gælder da, at $a \leq x$. Altså er a den mindste majorant for A. ■

Bemærkning 692 *Et største element er altså også et supremum. Det omvendte gælder ikke altid. For eksempel har intervallet $]1, 2[$ supremum 2, men det har intet største element.*

Bemærkning 693 *Det er klart, at en opadtil ubegrænset mængde ikke har noget supremum. Den har jo ikke en gang nogen majorant. Men hvad med opadtil begrænsede mængder, Kan vi bevise at de har et supremum? Nej, det kan vi heller ikke generelt (se Eksempel 697). Men der er en klasse vigtige partielt ordnede mængder, bl.a. de reelle tal, hvor enhver ikke tom opadtil begrænset mængde har et supremum. Disse giver vi et særligt navn:*

Definition 694 *En partielt ordnet mængde siges at have* ***supremumsegenskaben****, hvis enhver ikke tom opadtil begrænset delmængde har et supremum.*

Øvelse 695 *Overvej om de hele tal $(\mathbb{Z}, \leq)$ med den sædvanlige ordning har supremumsegenskaben.*

Øvelse 696 *Overvej at hvis A er en mængde, så har $P(A)$ med ordningen $\subseteq$ supremumsegenskaben.*

Eksempel 697 *De rationale tal med den sædvanlige ordning har ikke supremumsegenskaben.*

Bevis. Analyse: For at bevise dette skal vi angive en ikke tom delmængde af $\mathbb{Q}$, som er opadtil begrænset, men som ikke har et supremum. Hvordan skal vi gætte en kandidat? Vi kommer senere til at vise (eller postulere), at de reelle tal har supremumsegenskaben. Enhver ikke tom opadtil begrænset delmængde i $\mathbb{Q}$, vil også være en ikke tom opadtil begrænset delmængde af $\mathbb{R}$. Mængden har altså et supremum i $\mathbb{R}$. Vi skal altså sørge for, at dette supremum ikke ligger i $\mathbb{Q}$, det skal altså være et irrationalt tal. Vi har vist at $\sqrt{2}$ er irrationalt (se Sætning

53), så hvis vi kan finde en mængde af rationale tal, som i $\mathbb{R}$ har supremum $\sqrt{2}$, har vi en god kandidat. En sådan mængde er $B = \left\{x \in \mathbb{Q} \mid x < \sqrt{2}\right\}$. Nu er det pænere at undlade at involvere de reelle tal i en diskussion af de rationale tals egenskaber. Derfor vil vi helst angive mængden uden at involvere $\sqrt{2}$. Det kan vi gøre ved i stedet at se på mængden $A = \left\{x \in \mathbb{Q} \mid x^2 < 2\right\}$. Denne mængde er ikke lig med B, idet den ikke indeholder tallene mindre end $-\sqrt{2}$, men dens supremumsegenskab er er naturligvis de samme. Efter denne analyse, kan vi gå over til det syntetiske bevis.

Beviset. Betragt mængden

$$A = \left\{x \in \mathbb{Q} \mid x^2 < 2\right\}. \tag{15.14}$$

Den er en delmængde af $\mathbb{Q}$, og da $0 \in A$ er den ikke tom. Da 2 er en majorant (overvej), er mængden endvidere opadtil begrænset. Vi vil bevise at A ikke har et supremum i $\mathbb{Q}$. Beviset føres ved modstrid.

Antag altså, at $b \in \mathbb{Q}$ er supremum for A. Da $1 \in A$ og 2 er en majorant for A, gælder det, at $1 \leq b \leq 2$. Da $\mathbb{Q}$ er totalt ordnet, gælder et af følgende udsagn: $b^2 < 2$, $2 < b^2$, $b^2 = 2$. Vi vil udelukke de to første muligheder.

1. Antag først at $b^2 < 2$. Vi vil vise, at dette er i modstrid med antagelsen om at b er en majorant for A. Det gør vi ved at finde et tal i A, som er større end b.[1] Da vi har antaget at $b^2 < 2$, vil $d = \frac{2-b^2}{5}$ være et positivt rationalt tal. Tallet $c = b + d$ er derfor et rationalt tal større end b. Men c ligger i A, thi, da $b > 1$ er $d < \frac{2-1}{5} = \frac{1}{5} < 1$, og da endvidere $1 \leq b \leq 2$, kan vi slutte som følger:

$$c^2 = (b+d)^2 = b^2 + 2bd + d^2 < b^2 + 2 \cdot 2d + 1d \tag{15.15}$$

$$= b^2 + 5d = b^2 + 5\left(\frac{2-b^2}{5}\right) = b^2 + 2 - b^2 = 2. \tag{15.16}$$

   Vi har altså fundet et element c af A, som er større end b. Dette strider mod at b er en majorant for A. Vi kan altså udelukke at $b^2 < 2$.

2. Antag dernæst at $2 < b^2$. Vi vil vise at det er i modstrid med, at b er den *mindste* majorant for A. Det gør vi ved at finde en majorant for A, som er mindre end b.[2] Da vi har antaget at $2 < b^2$, vil $d = \frac{b^2-2}{4}$ være et positivt rationalt tal. Tallet $c = b - d$ er derfor et rationalt tal mindre end b. Vi vil vise at c er en majorant for A. Da $b \leq 2$ gælder nemlig at

$$c^2 = (b-d)^2 = b^2 - 2bd + d^2 > b^2 - 2bd \tag{15.17}$$

$$\geq b^2 - 2 \cdot 2d = b^2 - 4\left(\frac{b^2-2}{4}\right) = 2. \tag{15.18}$$

[1] Her skal vi altså finde en kandidat. I det følgende trækkes denne op af hatten. Prøv selv at lave den analyse, som fører frem til kandidaten.

[2] Prøv selv at lave analysen.

Så hvis $x > c$ vil $x^2 > c^2 > 2$ (her bruges at $c \geq 0$). hvorfor $x \notin A$. Kontraposition af dette udsagn giver at $x \in A \Rightarrow x \leq c$, som netop betyder at c er en majorant for A. Vi har altså fundet en majorant c, som er mindre end b, i modstrid med at b var antaget at være et supremum for A. Vi har altså udelukket at $2 < b^2$.

Da vi hverken har $b^2 < 2$ eller $2 < b^2$ må det altså gælde at $b^2 = 2$. Men det strider mod Sætning 53.

Vi har dermed bevist at mængden A ikke har et supremum i $\mathbb{Q}$, hvorfor $\mathbb{Q}$ ikke har supremumsegenskaben.

Helt analogt til supremum, defineres infimum: ■

Definition 698 *Lad A være en delmængde af en partielt ordnet mængde $(M, \leq)$. Et element b i M kaldes **infimum** for A, hvis det er den største minorant for A, d.v.s opfylder følgende to kriterier:*

1. *b er en minorant for A, altså: $\forall a \in A : b \leq a$.*
2. *b er den største minorant for A, altså: Hvis x er en minorant for A, da er $x \leq b$.*

Hvis b er infimum for A, skriver man $b = \inf A$

Sætning 699 *Lad A være en delmængde af en totalt ordnet mængde $(M, \leq)$. Da er $b = \inf A$ hvis og kun hvis*

1. *b er en minorant for A, altså: $\forall a \in A : b \leq a$.*
2. *$\forall x > b \exists a \in A : a < x$.*

Bevis. Overlades til læseren. ■

Sætning 700 *Lad A være en delmængde af en partielt ordnet mængde $(M, \leq)$. Hvis A har et mindste element a, da vil a også være infimum for A.*

Bevis. Bevis overlades til læseren. ■

Øvelse 701 *Afgør om følgende mængder har et infimum i $\mathbb{R}$, og bestem infimum, hvis det findes:*

1. $]1, 2[$.
2. $[1, 2]$.
3. $]-\infty, 0[$.
4. $\left\{\frac{1}{n} \mid n \in \mathbb{N}\right\}$

Definition 702 *En partielt ordnet mængde siges at have **infimumsegenskaben**, hvis enhver ikke tom nedadtil begrænset delmængde har et infimum.*

Sætning 703 *En partielt ordnet mængde har supremumsegenskaben, hvis og kun hvis den har infimumsegenskaben.*

Bevis. Lad $(M, \leq)$ være en partielt ordnet mængde. Vi vil vise, at hvis den har supremumsegenskaben, da har den også infimumsegenskaben. Det bevises helt analogt, at hvis $(M, \leq)$ har infimumsegenskaben, da har den også supremumsegenskaben.

Antag altså at $(M, \leq)$ har supremumsegenskaben. Vi vil da vise, at den har infimumsegenskaben. Lad derfor A være en ikke tom nedadtil begrænset delmængde af M. Vi skal vise at A har et infimum. Lad N_A betegne mængden af minoranter for A altså:

$$N_A = \{x \in M \mid x \text{ er en minorant for } A\}. \tag{15.19}$$

Ideen i beviset er nu at vise, at N_A er ikke tom og opadtil begrænset, hvorfor den iflg supremumsegenskaben har et supremum. Dette supremum vil vi så vise er et infimum for A.

Da A er antaget at være nedadtil begrænset, har A en minorant, så N_A er ikke tom. Da endvidere A er antaget at være ikke tom, kan vi vælge et $a \in A$. Hvis $x \in N_A$ er x en minorant for A, hvorfor $x \leq a$. Det betyder at a er en majorant for N_A. Altså er N_A ikke tom og opadtil begrænset, og da vi har antaget at $(M, \leq)$ har supremumsegenskaben, har N_A et supremum. Sæt $s = \sup N_A$. Vi vil vise, at s er infimum af A.

Først vises, at s er en minorant for A: Lad derfor a være et vilkårligt element i A. Vi så ovenfor, at a er en majorant for N_A. Da nu s er den mindste majorant for N_A, må den være mindre eller lig med a: $s \leq a$. Da dette gælder for alle $a \in A$ er s en minorant for A.

Dernæst vises, at s er den største minorant for A: Antag nemlig at z er en anden minorant for A. Da er pr. definition $z \in N_A$. Da $s = \sup N_A$, og s således specielt er en majorant for N_A, vil $z \leq s$. Altså er s en største minorant for A, hvorfor $s = \inf A$.

Vi konkluderer derfor at $(M, \leq)$ har infimumsegenskaben. ■

Øvelse 704 *Gennemfør den udeladte halvdel af ovenstående bevis, altså beviset for at hvis $(M, \leq)$ har infimumsegenskaben, da har den også supremumsegenskaben. Prøv at lære det ovenstående bevis så godt, at du kan gennemføre den manglende del med lukket bog. Det lærer du mere af end hvis du "oversætter" ovenstående bevis ord for ord med åben bog.*

15.3 Opgaver

1. Bevis at relationen $n \mid m$ er en partiel ordning på $\mathbb{N}$. Er det en total ordning?

2. Nedenfor angives en række delmængder af $\mathbb{R}$ med den sædvanlige ordning. Afgør i hvert tilfælde om

- mængden er opadtil begrænset, nedadtil begrænset og begrænset,

- mængden har et største element og et mindste element,
- mængden har et supremum og et infimum.

1. $[2, 6]$
2. $]2, 6[$
3. $]-\infty, 24693]$
4. $\mathbb{Q}_+$

3. Betragt $\mathbb{R}$ med den sædvanlige ordning. Bevis i alle detaljer, at

1. $\sup[0, 1[= 1$
2. $\inf\left\{\frac{1}{n} \mid n \in \mathbb{N}\right\} = 0$

4. Lad $(M, \leq)$ være en totalt ordnet mængde, og antag at $\emptyset \neq A \subseteq B \subseteq M$. Antag endvidere, at de nedenstående infima og suprema eksisterer: Bevis da, at

$$\inf B \leq \inf A \leq \sup A \leq \sup B. \tag{15.20}$$

Giv et eksempel, hvor $\inf A = \inf B$ og $\sup B = \sup A$, selv om A er en ægte delmængde af B.

Gælder sætningen også, hvis vi ikke antager at A og B er ikke tomme?

5. Lad A og B være ikke tomme delmængder af $\mathbb{R}$ (udstyret med den sædvanlige ordning), hvorom det gælder at $a < b$ for alle $a \in A$ og $b \in B$.

1. Bevis i alle detaljer at $\sup A$ og $\inf B$ begge eksisterer, og at

$$\sup A \leq \inf B. \tag{15.21}$$

I beviset må du gerne bruge, at $\mathbb{R}$ har supremumsegenskaben.

2. Antag desuden, at $A \cup B = \mathbb{R}$. Bevis, at

$$\sup A = \inf B. \tag{15.22}$$

6. I definitionen af supremumsegenskaben krævede vi, at enhver *ikke tom* opadtil begrænset delmængde skulle have et supremum. Overvej, at det er vigtigt at begrænse kravet til ikke tomme delmængder. Betragt for eksempel $\mathbb{R}$ og delmængden $\emptyset$. Er $\emptyset$ opadtil begrænset? Har $\emptyset$ en mindste majorant?

7. Betragt mængden $A = \{1, 2, 3, 4, 6, 12\}$ med "gå op i relationen" altså ordningen $\leq$ defineret ved: $a \leq b \overset{def}{\Leftrightarrow} a \mid b$

1. Tegn dens Hasse diagram
2. Bestem en delmængde af A som ikke har noget største element.
3. Afgør om ordningen har supremumsegenskaben.

Kapitel 16

Polynomier

I analyse betragtes polynomier som en speciel slags reelle eller komplekse funktioner. I dette kapitel skal vi betragte polynomier fra en algebraisk synsvinkel, og vi skal vise nogle sætninger, som ligner de sætninger vi viste i kapitel 3 om de hele tal. Vi skal behandle polynomier med koefficienter i $\mathbb{Q}, \mathbb{R}$ og $\mathbb{C}$ under et, så vi antager bare at koefficienterne tilhører et legeme.

16.1 Definition og simple egenskaber

Definition 705 *Lad L være et legeme. Et **polynomium** med koefficienter i L (eller et polynomium over L) er en følge $P = (a_0, a_1, ..., a_n, ...)$ af elementer i L hvoraf kun endelig mange er forskellige fra 0. Hvis alle følgens elementer efter a_n er 0 skriver man også polynomiet symbolsk på formen*

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n. \tag{16.1}$$

*Elementerne a_i kaldes polynomiets **koefficienter**, og det største n for hvilket $a_n \neq 0$ kaldes polynomiets **grad** og betegnes* $\deg(P)$.

Leddene $a_i x^i$ kaldes polynomiets led. Hvis $a_i = 0$, udelades ledet oftest i udtrykket 16.1, og hvis $a_i = 1$ skrives ledet blot x^i.

*Polynomiet $(0, 0, 0, ...)$, som altså skrives symbolsk 0, kaldes **nulpolynomiet**, og det tillægges graden -∞.*

*Polynomier af formen $(a_0, 0, 0, 0, ...)$ kaldes **konstante polynomier**.*

*Koefficienten a_0 kaldes for **konstantleddet**, og hvis polynomiet har grad n kaldes koefficienten a_n den **ledende koefficient** i polynomiet.*

*Et polynomium kaldes **monisk**, hvis den ledende koefficient er 1.*

Mængden af polynomier med koefficienter i legemet L betegnes $L[x]$

Definition 706 *Lad L være et legeme. På $L[x]$ defineres de to kompositionsregler $+$ og $\cdot$ på følgende måde:*

$$(a_0, a_1, ..., a_n, ...) + (b_0, b_1, ..., b_n, ...) = (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...) \tag{16.2}$$

$$(a_0, a_1, ..., a_n, ...) \cdot (b_0, b_1, ..., b_n, ...) = (p_0, p_1, ..., p_n, ...), \tag{16.3}$$

hvor

$$p_i = \sum_{j+k=i} a_j b_k, \tag{16.4}$$

hvor der summeres over ikke negative hele tal

Bemærkning 707 *Anderledes udtrykt: hvis*

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \tag{16.5}$$

og

$$Q(x) = b_0 + b_1 x + b_2 x^2 + \cdots b_m x^m, \tag{16.6}$$

hvor $m \leq n$. Da er

$$P(x) + Q(x) = (a_0 + b_0) + (a_1 + b_1)\, x + (a_2 + b_2)\, x^2 + \cdots + (a_n + b_n)\, x^n \tag{16.7}$$

og

$$P(x) \cdot Q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)\, x + (a_0 b_2 + a_1 b_1 + a_2 b_0)\, x^2 + \cdots + a_n b_m x^{(n+m)}. \tag{16.8}$$

Man lægger altså sammen ledvist og ganger som om polynomiet var en flerleddet størrelse og x var et element i legemet.

Øvelse 708 *Overvej, at $+$ og $\cdot$ defineret ovenfor er kompositionsregler på $L[x]$.*

Definition 709 *Lad P betegne polynomiet $P = (a_0, a_1, ..., a_n, ...)$. Da betegner $-P$ polynomiet $(-a_0, -a_1, ..., -a_n, ...)$*

Sætning 710 *Der gælder følgende regneregler: Hvis P, Q og R er polynomier over et legeme gælder:*

$$P + Q = Q + P \tag{16.9}$$
$$(P + Q) + R = P + (Q + R) \tag{16.10}$$
$$P + 0 = 0 + P = P \tag{16.11}$$
$$P + (-P) = (-P) + P = 0 \tag{16.12}$$
$$(PQ)\, R = P(QR) \tag{16.13}$$
$$1 \cdot P = P \cdot 1 = P \tag{16.14}$$
$$P\,(Q + R) = PQ + PR \quad , \quad (P + Q)R = PR + QR \tag{16.15}$$
$$PQ = QP \tag{16.16}$$

Bevis. Overlades til læseren. ■

Bemærkning 711 *Når L er et legeme er $(L[x], +, \cdot)$ altså en kommutativ ring. $L[x]$ er dog ikke et legeme, thi et polynomium har i almindelighed ingen multiplikativ invers.*

Sætning 712 *Lad P og Q være polynomier over et legeme L. Da gælder*

$$\deg(P \cdot Q) = \deg(P) + \deg(Q) \tag{16.17}$$

Bevis. Hvis $\deg(P) = n$ og $\deg(Q) = m$ og deres ledende koefficienter er henholdsvis a_n og b_m som ovenfor, da er koefficienten til x $(^{n+m})$ lig med $a_n b_m$ og da a_n og b_m begge er $\neq 0$ er også $a_n b_m \neq 0$ ifølge nulreglen (8.62). Koefficienterne til de højere potenser af x er derimod 0.

Ligheden gælder også når et af polynomierne eller begge er nulpolynomiet (ved passende konventioner om regning med $-\infty$; overvej). ■

Øvelse 713 *Overvej at der heraf følger at kun konstante polynomier forskellig fra nulpolynomiet har en multiplikativ invers.*

Korollar 714 *Lad P og Q være polynomier over et legeme L. Hvis $PQ = 0$, så gælder $P = 0$ eller $Q = 0$.*

Bevis. Overlades til læseren. ■

Sætning 715 *Hvis L er et legeme er $L[x]$ altså et integritetsområde.*

Bemærkning 716 *Lad P og Q være polynomier over et legeme L. Der gælder*

$$\deg(P + Q) \leq max(\deg(P), \deg(Q)). \tag{16.18}$$

Dette ses let fra definitionen af addition af polynomier. (Se Bemærkning 707.) I eksemplet $P(x) = x + 1, Q(x) = -x$ er $P(x) + Q(x) = 1$, så $\deg(P) = \deg(Q) = 1$, $\deg(P+Q) = 0$. Dette viser, at der behøver ikke gælde lighedstegn i (16.18).

Bemærkning 717 *Man kan faktisk også definere polynomier med koefficienter i en ring R ganske som vi definerede polynomier over et legeme. Den resulterende mængde af polynomier $R[x]$ er også en ring, men den er ikke i almindelighed et integritetsområde, med mindre R selv er et integritetsområde. Flere af sætningerne i dette kapitel gælder også for polynomier over en ring og endnu flere gælder for polynomier over et integritetsområde som $\mathbb{Z}$, men for simpelheds skyld vil vi kun betragte polynomier over legemer. Læseren kan selv prøve at spotte, hvor vi bruger at koefficienterne ligger i et integritetsområde eller et legeme.*

16.2 Division

Definition 718 *Lad P og D være polynomier over et legeme L. Da siges D at være en **divisor** i P, hvis der findes et polynomium Q over L, så*

$$P = QD. \tag{16.19}$$

Sætning 719 *Lad P, Q, S og D være polynomier over et legeme L. Antag at D er en divisor i P og Q. Da gælder at*

1. *D er en divisor i $P + Q$.*
2. *D er en divisor i SP.*

Bevis. Overlades til læseren ■

Bemærkning 720 *Da $L[x]$ som bemærket ovenfor ikke er et legeme, kan man ikke i almindelighed finde et kvotientpolynomium, så $P = QD$. Man kan altså ikke i almindelighed dividere et polynomium P med et andet polynomium D, så divisionen går op. Det er helt parallelt til de hele tal. Og som i de hele tal kan man i stedet dividere med rest:*

Sætning 721 ***Polynomiers division med rest**: Lad P og D være polynomier over et legeme L, hvor D ikke er nulpolynomiet. Da findes entydigt bestemte polynomier Q og R med $\deg(R) < \deg(D)$ så at*

$$P = QD + R. \tag{16.20}$$

Bevis. Lad $\deg D = m$. Eksistensen vises ved fuldstændig induktion efter graden n af P.

Induktionsstart: Hvis $n < m$ er $P = 0D + P$ en opskrivning af den ønskede form.

Induktionsskridtet: Antag nu at $m \leq n$, og at sætningen er sand for polynomier P med grad mindre end n, og antag at $\deg P = n$. Lad den ledende koefficient i P være a_n og lad den ledende koefficient i D være d_m. Da har polynomiet $a_n d_m^{-1} D x^{n-m}$ samme ledende koefficient som P, hvorfor $P - a_n d_m^{-1} D x^{n-m}$ har grad lavere end P. Ifølge induktionsantagelsen kan vi derfor finde polynomier Q' og R' med $\deg(R') < \deg(D)$ så at

$$P - a_n d_m^{-1} D x^{n-m} = Q'D + R'. \tag{16.21}$$

Deraf fås at P har en fremstilling af den ønskede form:

$$P = \left(Q' + a_n d_m^{-1} x^{n-m}\right) D + R'. \tag{16.22}$$

For at vise entydigheden, antages at der foruden fremstillingen (16.20) findes en anden fremstilling

$$P = Q_1 D + R_1 \tag{16.23}$$

med $\deg(R_1) < \deg(D) = m$. Da gælder altså

$$(Q - Q_1) D = R - R_1, \tag{16.24}$$

hvoraf

$$\deg(Q - Q_1) + \deg D = \deg(R - R_1). \tag{16.25}$$

Nu er $\deg(R - R_1) < \deg(D) = m$. Derfor må $(Q - Q_1)$ være nulpolynomiet, hvorfor $(R - R_1)$ også er nulpolynomiet. Altså er $Q = Q_1$ og $R = R_1$ så entydigheden er bevist. ■

Ovenstående bevis giver en metode til at bestemme Q og R. Den svarer til at stille divisionsstykket op som et almindeligt divisionsstykke med tal. I stedet for at forklare det i al generalitet gives her et eksempel:

Algoritme 722 *Polynomiers division: Betragt følgende polynomier i* $\mathbb{Q}(x)$*:*

$$P(x) = 4x^4 + 6x^3 + 3x^2 + x + 5 \tag{16.26}$$

og

$$D(x) = x^2 + 2x + 1. \tag{16.27}$$

Da kan divisionsstykket for eksempel opstilles således:

$$\begin{array}{llllll}
4x^4 & +6x^3 & +3x^2 & +x & +5 & : x^2 + 2x + 1 = 4x^2 - 2x + 3 \\
4x^4 & +8x^3 & +4x^2 & & & \textit{kvotient} \uparrow \\
\hline
0 & -2x^3 & -x^2 & +x & & \\
 & -2x^3 & -4x^2 & -2x & & \\
\hline
 & 0 & 3x^2 & +3x & +5 & \\
 & & 3x^2 & +6x & +3 & \\
\hline
 & & 0 & -3x & +2 & \longleftarrow \textit{rest}
\end{array}$$

Altså gælder:

$$4x^4 + 6x^3 + 3x^2 + x + 5 = \left(x^2 + 2x + 1\right)\left(4x^2 - 2x + 3\right) + (-3x + 2) \tag{16.28}$$

16.3 Rødder i polynomier

Definition 723 *Lad L være et dellegeme af L'. Lad endvidere $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ være et polynomium med koefficienter i L og lad $a \in L'$. Da defineres $P(a) \in L'$ ved*

$$P(a) = a_0 + a_1a + a_2a^2 + \cdots + a_na^n. \tag{16.29}$$

*Man siger at $P(a)$ er fremkommet ved at **indsætte** a i polynomiet.*

*Elementet a kaldes en **rod** i $P(x)$, hvis $P(a) = 0$.*

Bemærkning 724 *På denne måde kan man opfatte P som en afbildning $L' \longrightarrow L'$ defineret ved $a \longrightarrow P(a)$. Det er den almindelige måde at opfatte polynomier på i analyse.*

Elementet a er en rod i $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, hvis a er en løsning til ligningen

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0. \tag{16.30}$$

Man siger også at a er rod i ligningen (16.30), men man siger ikke at a er en løsning til polynomiet.

Øvelse 725 *Overvej at ethvert førstegradspolynomium har netop én rod.*

Sætning 726 *Lad L være et dellegeme af L'. Lad endvidere $P(x)$ og $Q(x)$ være et polynomier med koefficienter i L, og lad $a \in L'$. Da gælder*

$$(P+Q)(a) = P(a) + Q(a) \tag{16.31}$$
$$(PQ)(a) = P(a)Q(a). \tag{16.32}$$

Bevis. Det følger af den måde vi har defineret sum og produkt af polynomier. Kompositionsreglerne er jo defineret i overensstemmelse med regnereglerne i et legeme, når x opfattes som et almindeligt element i legemet. ■

Korollar 727 *Lad $P, Q, D \in L[x]$ og $P(x) = Q(x) \cdot D(x)$. Da gælder*

$$(a \text{ rod i } P(x)) \Leftrightarrow (a \text{ rod i } P(x)) \vee (a \text{ rod i } D(x)).$$

Bevis. Overlades til læseren. ■

Sætning 728 *Lad L være et legeme, og lad $a \in L$ og $P(x) \in L[x]$. Resten ved division af $P(x)$ med $(x-a)$ er $P(a)$.*

Bevis. Resten R ved division af $P(x)$ med $(x-a)$ er et polynomium af grad mindre end $(x-a)$. Det er altså et konstant polynomium a_0. Ifølge (721) gælder at

$$P(x) = Q(x)(x-a) + R(x) = Q(x)(x-a) + a_0. \tag{16.33}$$

Ifølge (16.31) og (16.32) gælder derfor at

$$P(a) = Q(a)(a-a) + a_0 = a_0. \tag{16.34}$$

■

Sætning 729 *Lad L være et legeme og lad $a \in L$ og $P(x) \in L[x]$. Da er a rod i $P(x)$, hvis og kun hvis $(x-a)$ er en divisor i $P(x)$.*

Bevis. Ifølge forrige sætning findes der et polynomium $Q(x) \in L[x]$, så

$$P(x) = Q(x)(x-a) + P(a). \tag{16.35}$$

Hvis a er rod i $P(x)$ er $P(a) = 0$, så

$$P(x) = Q(x)(x-a). \tag{16.36}$$

Altså er $(x-a)$ en divisor i $P(x)$.

Omvendt, hvis $(x-a)$ er en divisor i $P(x)$, så er resten ved division af $P(x)$ med $(x-a)$ lig med 0. Men ifølge forrige sætning betyder det at $P(a) = 0$, så a er en rod i $P(x)$. ■

Sætning 730 *Lad L være et legeme, og lad $P(x) \in L[x]$ med $\deg(P(x)) = n \geq 1$. Da har $P(x)$ højst n rødder i L.*

Bevis. Beviset føres ved induktion efter n.

Induktionsstart: Lad $\deg(P(x)) = 1$. Da er $P(x)$ af formen $P(x) = ax + b$ med $a \neq 0$. Hvis α er en rod i $P(x)$, skal der altså gælde at $a\alpha + b = 0$, hvoraf $\alpha = -b/a$. Elementet $-b/a$ er altså den eneste rod i $P(x)$.

Induktionsskridtet: Lad $\deg(P(x)) = n$, og antag at polynomier af grad $n-1$ højst har $n-1$ rødder. Der er nu to tilfælde: Enten har $P(x)$ ingen rødder, eller også har $P(x)$ mindst én rod. I det første tilfælde har vi vist, at $P(x)$ højst har n rødder. I det andet tilfælde, antag at α er en rod i $P(x)$. Da gælder ifølge forrige sætning at $(x - \alpha)$ er en divisor i $P(x)$, så der findes et polynomium $Q(x)$ så at

$$P(x) = Q(x)(x - a). \tag{16.37}$$

Hvis nu $\beta \neq \alpha$ er en rod i $P(x)$, gælder altså

$$0 = P(\beta) = Q(\beta)(\beta - a), \tag{16.38}$$

og da $(\beta - a) \neq 0$, må der ifølge nulreglen gælde at $Q(\beta) = 0$. Altså er β en rod i $Q(x)$. Ifølge (16.17) er $\deg(\ Q) = \deg(P) - \deg(x - \alpha) = n - 1$, så ifølge induktionsantagelsen har $Q(x)$ højst $n - 1$ rødder, hvoraf følger at $P(x)$ højst har n rødder.

Sætningen følger nu af princippet om simpel induktion. ■

16.4 Største fælles divisor. Euklids algoritme

Definition 731 *Lad L være et legeme lad $P(x), Q(x), D(x) \in L[x]$. Hvis $D(x)$ er en divisor i både $P(x)$ og i $Q(x)$ så siges $D(x)$ at være en fælles divisor i $P(x)$ og i $Q(x)$.*

$D(x)$ kaldes en største fælles divisor i $P(x)$ og i $Q(x)$ hvis følgende to betingelser er opfyldt:

1. *$D(x)$ er en fælles divisor i $P(x)$ og i $Q(x)$.*

2. *Hvis $S(x)$ er en fælles divisor i $P(x)$ og i $Q(x)$, da er $S(x)$ en divisor i $D(x)$.*

Sætning 732 *Lad L være et legeme, lad $P(x), Q(x) \in L[x]$ og antag at enten $P(x)$ eller $Q(x)$ ikke er nulpolynomiet. Da har $P(x)$ og $Q(x)$ en største fælles divisor, og hvis vi kræver den er monisk, da er den entydigt bestemt. Den største fælles divisor kan findes ved Euklids algoritme.*

Algoritme 733 *Lad L være et legeme lad $P(x), Q(x) \in L[x]$ med $Q(x) \neq 0$ og*

$\deg Q(x) \leq \deg P(x)$. *Vi bruger nu divisionssætningen 721 successivt:*

$$P = Q_1 Q + R_1 \ , \quad hvor \quad \deg R_1 < \deg Q \tag{16.39}$$
$$Q = Q_2 R_1 + R_2 \ , \quad hvor \quad \deg R_2 < \deg R_1 \tag{16.40}$$
$$R_1 = Q_3 R_2 + R_3 \ , \quad hvor \quad \deg R_3 < \deg R_2 \tag{16.41}$$
$$\vdots \tag{16.42}$$
$$R_{k-2} = Q_k R_{k-1} + R_k \ , \ hvor \quad \deg R_k < \deg R_{k-1} \tag{16.43}$$
$$R_{k-1} = Q_{k+1} R_k + 0 \tag{16.44}$$

Denne algoritme må stoppe ved en rest, som er 0*, thi graden af restpolynomierne er en strengt aftagende følge af ikke-negative hele tal, og en sådan følge kan kun være endelig. Vi vil nu vise at den sidste rest i Euklids algoritme, som ikke er nulpolynomiet (altså R_k ovenfor) er en største fælles divisor i $P(x)$ og $Q(x)$.*

Bevis. for sætning 732: Først vises *eksistensen*:

Hvis Q er nulpolynomiet og $P \neq 0$ da er P en største fælles divisor i P og Q (overvej). Antag derfor at $Q(x) \neq 0$ og $\deg Q(x) \leq \deg P(x)$.

1. Først vises at R_k i Euklids algoritme er en fælles divisor i $P(x)$ og $Q(x)$: Af (16.44) ses, at R_k er en divisor i R_{k-1}. Af (16.43) og sætning 719 ses, at R_k også er en divisor i R_{k-2}. Osv. Af (16.40) ses, at R_k er en divisor i Q og endelig ses af (16.39), at R_k også er divisor i P.

2. Antag nu at S er en divisor i P og Q. Da følger det af (16.39) og sætning 719 at S er divisor i R_1. Ved således at gå nedad i følgen af ligninger fås til slut af (16.44), at S er en divisor i R_k.

Dernæst vises *entydigheden.* Antag altså at D_1 og D_2 er største fælles divisorer i P og Q. Da D_1 er en divisor i P og Q og D_2 er en største sådanne, gælder pr. definition at D_1 er en divisor i D_2. Tilsvarende ses det at D_2 er en divisor i D_1. Men så må de have samme grad, og der må gælde at $D_1 = aD_2$ for et $a \in L$, og $D_2 = bD_1$ for et $b \in L$. Men så er $a = b^{-1}$, og $a \neq 0$. To største fælles divisorer i P og Q afviger altså højst med en multiplikativ konstant forskellig fra 0. Der er derfor præcist en monisk største fælles divisor. ■

Definition 734 *Lad L være et legeme lad $P(x) \in L[x]$ med* $\deg(P) \geq 1$*. Da kaldes P **reducibelt** (over L), hvis der findes polynomier Q og S med* $\deg(Q) \geq 1$ *og* $\deg(S) \geq 1$*, så $P = QS$. Hvis P ikke er reducibelt, kaldes det **irreducibelt**.*

Bemærkning 735 *Irreducible polynomier spiller samme rolle i teorien for polynomier, som primtallene gør i teorien for de hele tal. For en videre behandling af polynomier henvises til algebrakurserne.*

16.5 Algebraens fundamentalsætning

Sætning 736 *Lad L være et legeme og $P(x) \in L[x]$, med $\deg(P) \geq 1$. Da kan $P(x)$ på skrives på formen*

$$P(x) = (x-a_1)^{n_1}(x-a_2)^{n_2}\cdots(x-a_k)^{n_k}Q(x) \tag{16.45}$$

hvor $a_1, a_2, ..., a_k$ er de forskellige rødder i $P(x)$, og $Q(x)$ er et polynomium i $L[x]$ uden rødder i L og $n_i$erne er naturlige tal. Denne opskrivning er entydig på nær faktorernes rækkefølge.

Bevis. Eksistens: Hvis $P(x)$ ikke har nogle rødder i L er vi færdige. Hvis $P(x)$ har rødder i L betegner vi disse med $a_1, a_2, ..., a_k$. Fra Sætning 729 vides at $(x-a_1)$ går op i $P(x)$. Lad n_1 betegne det største naturlige tal så $(x-a_1)^{n_1}$ går op i $P(x)$ (overvej at der findes en sådan maximal eksponent). Da kan $P(x)$ skrives $P(x) = (x-a_1)^{n_1}Q_1(x)$, hvor a_1 ikke er rod i $Q_1(x)$ (overvej!). Fortsættes således med de øvrige rødder (brug evt. induktion) ses at $P(x)$ kan skrives på formen (16.45) hvor $Q(x)$ ikke har nogen af $P(x)'s$ rødder. Da nu rødderne i $Q(x)$ er rødder i $P(x)$ har $Q(x)$ altså ingen rødder i L.

Entydighed: Vi skal vise at potenserne $n_1, ..., n_k$ og polynomiet $Q(x)$ er entydigt bestemt. Det bevises ved induktion efter graden af $P(x)$.

1. *Induktionsstarten*: Hvis $\deg(P(x)) = 1$ har P én rod a_1 (ifølge Øvelse 725) , så opskrivningen (16.45) har formen $(x-a_1)Q(x)$. Graden af $Q(x)$ må være 0, så $Q(x) = a$ hvor $a \in L$. Men a er derfor koefficienten til x i førstegradspolynomiet, som jo er entydigt bestemt.

2. *Induktionsskridtet*: Antag at opskrivningen er entydig for polynomier af grad n. Lad $P(x)$ være et polynomium af grad $n+1$. Vi skal da vise at dets opskrivning på formen (16.45) er entydig. Antag derfor at $P(x)$ kan skrives på to måder

$$\begin{aligned} P(x) &= (x-a_1)^{n_1}(x-a_2)^{n_2}\cdots(x-a_k)^{n_k}Q(x) && (16.46)\\ &= (x-b_1)^{m_1}(x-b_2)^{m_2}\cdots(x-b_k)^{m_l}Q_1(x) && (16.47)\end{aligned}$$

   Hvis $P(x)$ ikke har nogen rødder i L følger af Sætning 729 at der ikke er nogen førstegradsfaktorer og at $P(x) = Q(x) = Q_1(x)$ og opskrivningen er derfor entydig.

   Hvis derimod $P(x)$ har en rod $a' \in L$ følger det af en simpel generalisering af Korollar 727 at a' er en rod i en af faktorerne i hvert af de to produkter. Derfor må a' være lig med et af $a_i$erne og et af $b_i$erne. Vi kan uden tab af generalitet antage at $a' = a_1 = b_1$. Nu kan vi dividere identiteten (16.46) igennem med $(x-a_1)$ og vi får

$$\begin{aligned}&(x-a_1)^{n_1-1}(x-a_2)^{n_2}\cdots(x-a_k)^{n_k}Q(x)\\ &= (x-a_1)^{m_1-1}(x-b_2)^{m_2}\cdots(x-b_k)^{m_l}Q_1(x).\end{aligned}$$

Hvis $n_1 - 1 = 0$ må også $m_1 - 1 = 0$ og den første faktor kan derfor fjernes. Under alle omstændigheder har vi nu opskrevet en identitet mellem to $n$te grasds polynomier på den krævede form, og den er entydig ifølge induktionsantagelsen. Altså må også de to oprindelige opskrivninger af $P(x)$ være ens bortset fra faktorernes rækkefølge.

■

Definition 737 *Eksponenten n_i i faktoriseringen (16.45) kaldes* ***multipliciteten*** *af roden a_i. Hvis multipliciteten er 1 kaldes roden* ***simpel****.*

Sætning 738 ***Algebraens fundamentalsætning****. Ethvert ikke-konstant polynomium over de komplekse tal (altså i $\mathbb{C}[X]$) har en kompleks rod.*

Bevis. Beviset udelades. Det bygger på de reelle tals fuldstændighed. ■

Korollar 739 *Ethvert polynomium $P(x)$ over de komplekse tal kan faktoriseres på formen*

$$P(x) = a(x - a_1)^{n_1}(x - a_2)^{n_2} \cdots (x - a_k)^{n_k}, \tag{16.48}$$

hvor $a_1, a_2, ..., a_k$ er rødderne i $P(x)$ og a er et komplekst tal forskelligt fra 0. Med andre ord, polynomiet kan faktoriseres i førstegradsfaktorer.

Bevis. Ifølge sætning 736 kan $P(x)$ skrives på formen (10a.46) hvor $Q(x)$ ikke har nogen rødder i $\mathbb{C}$. Men ifølge algebraens fundamentalsætning må $Q(x)$ så være en konstant a. ■

Bemærkning 740 *Det følger af Sætning 736 at opskrivningen (16.48) er entydigt bestemt op til faktorernes orden.*

Bemærkning 741 *Når et polynomium kan skrives som 16.48 kan vi opfatte a_i som en rod i polynomiet n_i gange. Da graden af $P(x)$ må være $n_1 + n_2 + \cdots + n_k$, kan korollaret til algebraens fundamentalsætning derfor også formuleres: Et komplekst n'te gradspolynomium har n komplekse rødder talt med multiplicitet. Denne sætning kaldes normalt også* ***algebraens fundamentalsætning.***

Sætning 742 *Et polynomium med reelle koefficienter $P(x) \in \mathbb{R}[x]$ er et specielt komplekst polynomium. I det tilfælde kommer de ikke-reelle rødder i komplekst konjugerede par. Med andre ord: Hvis $z_0 = a + ib$ (hvor $a, b \in \mathbb{R}$) er en kompleks rod i et reelt polynomium, er $\overline{z_0} = a - ib$ også en rod i polynomiet.*

Bevis. Lad z_0 være en rod i polynomiet $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, det vil pr. definition sige at $P(z_0) = a_0 + a_1z_0 + a_2z_0^2 + \cdots + a_nz_0^n = 0$. Antag nu at alle koefficienterne i polynomiet er reelle. Ved brug af de velkendte regneregler:

$$\overline{a} + \overline{b} = \overline{(a + b)}, \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

for komplekse tal fås da:

$$\begin{aligned} P(\overline{z_0}) &= a_0 + a_1\overline{z_0} + a_2\overline{z_0}^2 + \cdots + a_n\overline{z_0}^n \\ &= \overline{a_0} + \overline{a_1}\cdot\overline{z_0} + \overline{a_2}\cdot\overline{z_0}^2 + \cdots + \overline{a_n}\cdot\overline{z_0}^n \\ &= \overline{a_0} + \overline{a_1 z_0} + \overline{a_2 z_0^2} + \cdots + \overline{a_n z_0^n} \\ &= \overline{a_0 + a_1 z_0 + a_2 z_0^2 + \cdots + a_n z_0^n} \\ &= \overline{P(z_0)} = \overline{0} = 0 \end{aligned}$$

Altså er $\overline{z_0}$ en rod i polynomiet $P(x)$. ■

Lemma 743 *Lad $z_0 \in \mathbb{C}$. Da gælder:*

$$(x - z_0)\cdot(x - \overline{z_0}) = x^2 - (2\operatorname{Re} z_0)\, x + |z_0|^2$$

Bevis. Gang ud! ■

Lemma 744 *Lad $P(x)$ og $D(x)$ være reelle polynomier og $Q(x)$ et komplekst polynomium hvorom det gælder at*

$$P(x) = Q(x)\cdot D(x).$$

Da er $D(x)$ også et reelt polynomium (altså alle koefficienterne er faktisk reelle)

Bevis. Quotientpolynomiet $Q(x)$ kan findes ved at dividere polynomiet $P(x)$ med $D(x)$ ved brug af polynomiers division. Men den ovennævnte algoritme vil resultere i et reelt polynomium, når den bruges på to reelle polynomier. ■

Sætning 745 *Ethvert reelt polynomium kan skrives som et produkt af reelle første- og andengradspolynomier.*

Bevis. Vi vil bevise sætningen ved fuldstændig induktion efter graden af polynomiet. Så lad $P(x)$ betegne et reelt polynomium.

1. *Induktionsstart*: Hvis $P(x)$ har grad 1 er det allerede et produkt af første- og andengradsfaktorer.

2. *Induktionsskridtet*: Antag at alle reelle polynomier af grad m eller mindre kan skrives som et produkt af reelle første- og andengradsfaktorer. Lad $P(x)$ være et polynomium af grad $m+1$. Ifølge algebraens fundamentalsætning har $P(x)$ en komplex rod z_0. Ifølge Sætning (729) kan $P(x)$ da skrives på formen $P(x) = (x - z_0)\cdot Q(x)$ hvor $Q(x)$ er et komplekst polynomium af grad m. Hvis z_0 er reel har vi altså skrevet $P(x) = P_1(x)\cdot P_2(x)$, hvor P_1 er et reelt førstegradspolynomium.

   Hvis derimod z_0 ikke er reel er $\overline{z_0}$ ifølge Sætning (742) en anden rod i $P(x) = (x - z_0)\cdot Q(x)$, hvorfor $\overline{z_0}$ må være en rod i $Q(x)$. Ifølge Sætning (729) og Lemma (743) kan $P(x)$ da skrives på formen

$$\begin{aligned} P(x) &= (x - z_0)\cdot(x - \overline{z_0})\cdot Q'(x) \\ &= \left(x^2 - (2\operatorname{Re} z_0)\, x + |z_0|^2\right)\cdot Q'(x) \end{aligned}$$

hvor $Q'(x)$ er et komplekst polynomium af grad $m-1$.

I begge tilfælde kan vi altså skrive $P(x) = P_1(x) \cdot P_2(x)$, hvor P_1 er et reelt første- eller andengradspolynomium og $P_2(x)$ er et polynomium af grad m eller $m-1$. Af Lemma (744) følger at $P_2(x)$ er et *reelt* polynomium af grad n eller $m-1$. Men ifølge induktionsantagelsen kan $P_2(x)$ så faktoriseres i reelle første- og andengradsfaktorer. Dermed er det bevist at $P(x)$ kan faktoriseres i reelle første- og andengradsfaktorer.

Ifølge princippet om fuldstændig induktion har vi derved bevist sætningen for alle reelle polynomier. ■

16.6 Opgaver

1. Lav polynomiers division med rest på de to polynomier i $\mathbb{R}[x]$:

$$2x^5 - 4x^4 - x^3 + 3x^2 - 5 \tag{16.49}$$

og

$$x^3 + x - 2 \tag{16.50}$$

2. Bestem den største fælles divisor for de to polynomier i opgave 1.

3. Bestem den største fælles divisor for følgende polynomier i $\mathbb{R}[x]$:

$$x^5 + 6x^3 + 5x \tag{16.51}$$

og

$$x^4 + 3x^3 + 8x^2 + 3x + 7 \tag{16.52}$$

4. Bestem to polynomier af forskellig grad i $\mathbb{R}[x]$ som har $x^2 + x - 1$ som største fælles divisor.

5. Bevis at et polynomium i $\mathbb{R}[x]$ af grad 2 eller 3 er reducibelt, hvis og kun hvis det har en reel rod.

6. Det oplyses at polynomiet $x^4 + 4$ har den komplekse rod $1 + i$. Bestem de øvrige komplekse rødder i polynomiet.

7. Opfat et reelt eller komplekst polynomium $P(x)$, som en reel eller en kompleks funktion. Lad $P'(x)$ betegne det afledede (differentierede) polynomium og lad a være et reelt eller komplekst tal.

a. Vis at

a er dobbeltrod (altså en rod af multiplicitet 2) i $P(x) \Leftrightarrow a$ er rod i både $P(x)$ og $P'(x)$.

Du må gerne bruge de sædvanlige regler for differentiation.

b. Formuler og bevis en lignende betingelse for, hvornår a er en rod af multiplicitet n.

8. Skriv polynomiet $x^3 - x^2 + 4x - 4$ som en sum af irreducible reelle første- og andengradsfaktorer.

9. Lad L være et legeme lad $P(x) \in L[x]$ med $\deg(P) \geq 1$.

a. Bevis at $P(x)$ kan skrives som et produkt af irreducible polynomier over $L(x)$. Du kan lade dig inspirere af beviset for aritmetikkens hovedsætning.

b. Overvej hvordan de irreducible polynomier i $\mathbb{R}[x]$ ser ud, og formuler derfra en sætning om, hvilken form det ovenstående produkt af irreducible polynomier ser ud over $\mathbb{R}$.

c. Hvordan ser de irreducible polynomier ud i $\mathbb{C}[x]$?

Kapitel 17

Talsystemets opbygning

17.1 Motiverende indledning

I Indledningen gav vi en aksiomatisk beskrivelse af de reelle tal, og vi kunne så betragte de naturlige tal, de hele tal og de rationale tal som delmængder af de reelle tal. I dette kapitel vil vi skitsere en alternativ behandling af tallene. I stedet for at starte med et aksiomssystem for den store mængde af reelle tal, kan man successivt *konstruere* talmængderne, begyndende med den mindste, nemlig de naturlige tal, som konstrueres ud fra mængdelæren. Derfra kan man successivt konstruere udvidelser til de hele tal, de rationale tal, de reelle tal og endelig de komplekse tal.

Der er tre grunde, til at man vil konstruere tallene på denne måde, i stedet for at nøjes med en aksiomatisk beskrivelse:

1. En historisk-psykologisk-didaktisk grund. En successiv konstruktion af tallene følger til en vis grad den historiske udvikling af talbegrebet og følger også i store træk den måde vi som børn og unge mennesker selv har lært os tallene.

2. En æstetisk-filosofisk grund: Når det er muligt at indføre alle tallene uden at acceptere andre aksiomer end mængdelærens aksiomer, er det mere tilfredsstillende at gå sådan til værks, snarere end at skulle acceptere alle de andre aksiomer, vi opstillede i Indledningen (mængdelærens aksiomer var naturligvis også stiltiende forudsat i denne beskrivelse). Dette hænger sammen med det princip i filosofi, som kaldes Ockham ragekniv (Ockham's razor), ifølge hvilket en videnskab bør opbygges på det mindste antal hypoteser.

3. En matematisk-logisk grund: I forbindelse med ethvert aksiomatisk system er det afgørende at vide at aksiomerne ikke strider mod hinanden, på sådan en måde at man inden for systemet både kan bevise en sætning og samtidigt denne sætnings negation. Hvis aksiomerne strider mod hinanden på denne måde siger vi at systemet er inkonsistent. Det er klart, at man ikke er interesseret i at arbejde med inkonsistente aksiomatiske systemer, men kun med konsistente systemer, altså sådanne, hvor man ikke kan bevise en sætning og den samme

sætnings negation. Inkonsitente systemer er uinteressante, ikke bare fordi de ikke beskriver noget i (den forhåbentlige konsistente) virkelighed, men også fordi man i et inkonsistent system kan bevise enhver sætning ved et modstridsbevis: Hvis systemet er inkonsistent, findes der et udsagn p så både p og $\neg p$ kan bevises. Derfor er udsagnet $p \wedge \neg p$ sandt, hvorfor $\neg q \Rightarrow (p \wedge \neg p)$ er et sandt udsagn for alle udsagn q. Men i (2.11) så vi at $\neg q \Rightarrow (p \wedge \neg p)$ er logisk ækvivalent med q. Altså kan ethvert udsagn q (og dermed også $\neg q$) bevises (indirekte) i et inkonsistent aksiomatisk system.

Desværre er det ofte meget vanskeligt at bevise, at et aksiomatisk system er konsistent. Ja faktisk siger en berømt sætning af Gödel[1], at det er umuligt at vise konsistensen af mængdelærens aksiomer (og dermed også af aksiomerne af de reelle tal) inden for systemet selv, med mindre systemet er inkonsistent (for i så fald kan alle sætninger i systemet jo bevises). Det betyder, at man ikke kan bevise, at den sædvanlige matematik er konsistent. Der er dog ingen grund til bekymring. Selv efter et århundredes arbejde med mængdelæren er der ikke dukket nogle inkonsistenser op, og hvis det usandsynlige skulle ske, at man finder en inkonsistens i mængdelæren, så vil man nok blot skulle reparere lidt på aksiomerne, så man undgår inkonsistenserne og alligevel får en mængdelære, som gør det den skal. Det ville næppe betyde, at man skulle ændre noget væsentligt i den videregående matematik, og det ville ikke betyde at alle anvendelserne af matematiske resultater skulle tænkes om. Broer ville ikke falde sammen, og vejrudsigter ville hverken blive værre eller bedre.

Man skal dog være så forsigtig som mulig med aksiomerne i et aksiomssystem. Hvert nyt aksiom giver større risiko for at systemet er inkonsistent. Derfor er det en fordel at nøjes med mængdelærens aksiomer. Hvis vi konstruerer de reelle tal ud fra mængdelæren, så ved vi, at vi ikke har tilføjet nye inkonsistenser end de inkonsistenser der måtte være i mængdelærens aksiomssystem. Med andre ord, ved at konstruere de reelle tal viser vi, at hvis mængdelærens aksiomssystem er konsistent, så er aksiomssystemet for de reelle tal også konsistent.

Alle udvidelserne fra $\mathbb{N}$ til $\mathbb{Z}$ til $\mathbb{Q}$ til $\mathbb{R}$ til $\mathbb{C}$ har det til fælles, at de muliggør noget, som ikke var muligt i den lille talmængde. Og vi konstruerer udvidelsen, så dette bliver muligt.

I $\mathbb{N}$ kan vi ikke altid trække fra (tallene har ikke en additiv invers). Så vi konstruerer $\mathbb{Z}$, så det bliver muligt.

I $\mathbb{Z}$ kan vi ikke altid dividere (tallene har ikke en multiplikativ invers). Så vi konstruerer $\mathbb{Q}$, så det bliver muligt (bortset fra division med 0)

I $\mathbb{Q}$ har en ikke tom opadtil begrænset delmængde ikke altid et supremum. Vi konstruerer $\mathbb{R}$, så det bliver tilfældet.

I $\mathbb{R}$ har et polynomium ikke altid en rod. Vi konstruerer $\mathbb{C}$, så det bliver tilfældet.

I denne bog skal vi kun give en detaljeret redegørelse for konstruktionen af de rationale tal fra de hele tal. De øvrige konstruktioner på vejen fra mængdelæren til de komplekse tal skal kun antydes.

[1] Kurt Gödel (1906-1978)

17.2 Konstruktion af $\mathbb{Q}$ ud fra $\mathbb{Z}$

I dette afsnit antager vi, at vi har de hele tal til rådighed, med de egenskaber vi beskrev i sætning 118. Vi vil så konstruere de rationale tal herudfra. Konstruktionen er inspireret af (men principielt helt uafhængig af) vores skolelærdom om de rationale tal skrevet som brøker a/b, hvor $a, b \in \mathbb{Z}$ og $b \neq 0$, og af ideen om at brøker kan forlænges og forkortes, uden at det ændrer ved det rationale tal. Vi har lært i skolen at to brøker a/b og a'/b' er ens, hvis og kun hvis $ab' = ba'$. Dette giver os ideen til at definere de rationale tal som par af hele tal, eller rettere som ækvivalensklasser af par af hele tal:

Definition 746 *På mængden $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ defineres en relation på følgende måde:*

$$(a, b) \sim (a', b') \overset{def}{\Leftrightarrow} ab' = ba' \tag{17.1}$$

Sætning 747 *Den derved definerede relation er en ækvivalensrelation på $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.*

Bevis. Refleksivitet og symmetri er trivielle.

Transitivitet: Antag at $(a, b) \sim (a', b')$ og $(a', b') \sim (a'', b'')$. Da gælder pr. definition at

$$ab' = ba' \quad \text{og} \quad a'b'' = b'a''. \tag{17.2}$$

Ved at gange venstesiderne med hinanden og højresiderne med hinanden fås

$$ab'a'b'' = ba'b'a'' \tag{17.3}$$

eller på grund af kommutativiteten

$$(ab'')(a'b') = (ba'')(a'b'). \tag{17.4}$$

Hvis $a' \neq 0$ er $a'b' \neq 0$ og så har vi lov til at forkorte med $a'b'$. I så fald får vi at $ab'' = ba''$, hvad der pr. definition betyder at $(a, b) \sim (a'', b'')$.

Hvis $a' = 0$ fås fra (17.2) at $ab' = ba' = 0$, og da $b' \neq 0$, slutter vi heraf, at $a = 0$. På samme måde sluttes at $a'' = 0$. Derfor er $ab'' = 0 = ba''$, så også i dette tilfælde er $(a, b) \sim (a'', b'')$. ■

Definition 748 *Ækvivalensklasserne for den i definition 746 definerede ækvivalensrelation på $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ kaldes **rationale tal**. Mængden af rationale tal benævnes $\mathbb{Q}$. Ækvivalensklassen $[(a, b)]$ bestemt ved parret (a, b) betegnes a/b eller $\frac{a}{b}$ og kaldes brøken bestemt ved a og b. a kaldes brøkens tæller og b dens nævner.*

Sætning 749 *Lad $\frac{a}{b}, \frac{a'}{b'} \in \mathbb{Q}$ og $c \in \mathbb{Z}$ $(c \neq 0)$. Da gælder*

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = ba' \tag{17.5}$$

$$\frac{a}{b} = \frac{ca}{cb}. \tag{17.6}$$

Bevis.

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow (a,b) \sim (a',b') \Leftrightarrow ab' = ba'. \tag{17.7}$$

Beviset for den sidste identitet overlades til læseren ■

Definition 750 *Når vi ganger en brøks tæller og nævner med samme hele tal forskelligt fra nul, siger vi at vi* ***forlænger*** *brøken. Når vi derimod dividerer tæller og nævner med en fælles divisor i tæller og nævner, siger vi, at vi* ***forkorter*** *brøken.*

Bemærkning 751 *Det fremgår af (17.6) at et rationalt tal ikke ændres, hvis man forlænger eller forkorter brøken.*

To brøker $\frac{a}{b}, \frac{c}{d}$ kan således altid opskrives, så de har ***fælles nævner****. Man forlænger bare den første med d og den anden med b, hvorved de kommer på formen $\frac{ad}{bd}$ og $\frac{bc}{bd}$. Ved eventuelt at forlænge med -1, kan man altid sørge for, at en brøks nævner bliver positiv.*

Nu vil vi indføre kompositionsreglerne addition og multiplikation på $\mathbb{Q}$.

Definition 752 *Lad $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ Da defineres to kompositionsregler $+$ og $\cdot$ ved*

$$\frac{a}{b} + \frac{c}{d} \stackrel{def}{=} \frac{ad+bc}{bd}, \tag{17.8}$$

$$\frac{a}{b}\frac{c}{d} \stackrel{def}{=} \frac{ac}{bd} \tag{17.9}$$

Bemærkning 753 *Ligesom da vi definerede kompositionsreglerne for regning med restklasser, skal vi overveje at den ovenstående definition er uafhængig af de valgte repræsentanter. Vi skal altså vise følgende sætning:*

Sætning 754 *Antag at $\frac{a}{b} = \frac{a'}{b'}$ og $\frac{c}{d} = \frac{c'}{d'}$. Da gælder at*

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \tag{17.10}$$

$$\frac{ac}{bd} = \frac{a'c'}{b'd'} \tag{17.11}$$

Bevis. Vi viser første lighed. Anden lighed overlades til læseren.

Da $\frac{a}{b} = \frac{a'}{b'}$ og $\frac{c}{d} = \frac{c'}{d'}$, følger af (17.5), at $ab' = ba'$ og $cd' = dc'$, hvoraf

$$(ab')(dd') = (ba')(dd') \quad \text{og} \quad (cd')(bb')(dc')(bb'), \tag{17.12}$$

så

$$adb'd' + bcb'd' = a'd'bd + b'c'bd, \tag{17.13}$$

hvorfor

$$(ad+bc)\,b'd' = (a'd'+b'c')\,bd, \tag{17.14}$$

som ifølge (17.5) netop betyder at

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}. \tag{17.15}$$

■

Bemærkning 755 *Det er værd at bemærke at addition af to brøker med fælles nævner er speciel simpelt:*

$$\frac{a}{b}+\frac{c}{b}=\frac{a+c}{b}. \tag{17.16}$$

Overvej dette.

Sætning 756 $(\mathbb{Q},+,\cdot)$ *defineret ovenfor er et legeme. Det additive neutralelement er brøken* $0/1$*, og den additivt inverse til* a/b *er* $(-a)/b$*. Det multiplikative neutralellement er* $1/1$*, og den multiplikative inverse til en brøk* a/b $(a\neq 0)$ *er brøken* b/a*.*

Bevis. Her bevises den distributive lov. Resten af beviset overlades til læseren.

Lad der være givet tre rationale tal. Ifølge bemærkning 751 kan vi opskrive dem som brøker med fælles nævner:$a/d, b/d$ og c/d. Da gælder:

$$\frac{a}{d}\left(\frac{b}{d}+\frac{c}{d}\right)=\frac{a}{d}\frac{b+c}{d}=\frac{a\,(b+c)}{d^2} \tag{17.17}$$

$$\frac{a}{d}\frac{b}{d}+\frac{a}{d}\frac{c}{d}=\frac{ab}{d^2}+\frac{ac}{d^2}=\frac{ab+ac}{d^2}. \tag{17.18}$$

I følge den distributive lov på $\mathbb{Z}$ er de to højresider ens, hvorfor de to venstresider også er ens. Dette er netop den distributive lov i $\mathbb{Q}$. ■

Bemærkning 757 *Vi kan opfatte de hele tal som liggende inde i* $\mathbb{Q}$*. Vi skal bare identificere det hele tal* a *med brøken* $a/1$*. Dette kan vi gøre, fordi regnereglerne i* $\mathbb{Z}$ *og i* $\mathbb{Q}$ *passer overens. der gælder nemlig at*

$$\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}, \tag{17.19}$$

$$\frac{ab}{1}=\frac{a}{1}\frac{b}{1}. \tag{17.20}$$

Mere præcist kan vi sige, at $\left(\left\{\frac{a}{1}\in\mathbb{Q}\mid a\in\mathbb{Z}\right\},+,.\right)$ *er isomorf med* $(\mathbb{Z},+,.)$*. Fra nu af laver vi denne identifikation.*

Man kan dermed sige at legemet $(\mathbb{Q},+,\cdot)$ *er en udvidelse af integritetsområdet* $(\mathbb{Z},+,.)$*. Det eneste vi indtil nu har brugt om* $\mathbb{Z}$ *er at det er et integritetsområde. Man kan lave en lignende konstruktion af et legeme for et vilkårligt integritetsområde. Konstruktionen fører til det man kalder for integritetsområdes* ***brøklegeme****.*

Ud over den algebraiske struktur skal $\mathbb{Q}$ også udstyres med en ordning, som gør $\mathbb{Q}$ til et ordnet legeme. Husk at et ordnet legeme er beskrevet ved aksiomssystemet for de reelle tal (se Introduktionen) på nær supremumsegenskaben. Vi skal her bruge de alternative aksiomer O1 og O2 i stedet for aksiomerne for $\leq$. Vi skal derfor definere en mængde $\mathbb{Q}_+$ af positive rationale tal. Definitionen skal naturligvis bygge på ordningen på $\mathbb{Z}$:

Definition 758 *Vi definerer mængden $\mathbb{Q}_+$ af positive rationale tal som*

$$\mathbb{Q}_+ = \{a/d \in \mathbb{Q} \mid a > 0 \wedge d > 0\}. \tag{17.21}$$

Lemma 759 *Lad $c/d \in \mathbb{Q}_+$ og $d > 0$. Da er $c > 0$.*

Bevis. Da $c/d \in \mathbb{Q}_+$ eksisterer $a, b \in \mathbb{Z}_+$ så $c/d = a/b$. Men så er $ad = cb$ og da $ad > 0$ må altså $cb > 0$. Hvis nu $c \leq 0$ ville $cb \leq 0$ hvad der er i modstrid med $cb > 0$. altså er $c > 0$. ■

Sætning 760 *Med denne definition af $\mathbb{Q}_+$ bliver $(\mathbb{Q}, +, \cdot)$ et ordnet legeme.*

Bevis. Vi skal checke om betingelserne O1 og O2 i Introduktionen er opfyldt.

O1: Det er let at se at hvis a/d og b/d begge ligger i $\mathbb{Q}_+$, så vil $a/d \cdot b/d$ og $a/d + b/d$ også ligge i $\mathbb{Q}_+$ (man skal bare huske, at ifølge bemærkning 751 kan enhver brøk skrives med positiv nævner).

O2: Givet et rationalt tal repræsenteret ved en brøk a/d med positiv nævner $d > 0$. Da gælder

$$a/d \in \mathbb{Q}_+ \Leftrightarrow a > 0 \tag{17.22}$$

$$a/d = 0 \Leftrightarrow a = 0 \tag{17.23}$$

$$-(a/d) = (-a)/d \in \mathbb{Q}_+ \Leftrightarrow -a > 0. \tag{17.24}$$

Da der for et helt tal a gælder præcist et af udsagnene $a > 0, a = 0$ og $-a > 0$ er O.2 eftervist.

Nu kan en total ordning $\leq$ på $\mathbb{Q}$ defineres ved

$$x \leq y \Leftrightarrow (y - x) \in \mathbb{Q}_+ \cup \{0\}.$$

. ■

Bemærkning 761 *Hvis $a, b \in \mathbb{Q}$ og $a \leq b$ så vil $a/1 \leq b/1$. Ordningen på $\mathbb{Z}$ stemmer altså overens med ordningen på $\mathbb{Q}$, så at der ikke opstår problemer med identifikationen af det hele tal a med det rationale tal $a/1$*

Sætning 762 *Lad a/d og b/d ($d > 0$) være to rationale tal, som vi som her har bragt på fælles positiv nævner. Da gælder*

$$\frac{a}{d} \leq \frac{b}{d} \Leftrightarrow a \leq b. \tag{17.25}$$

Bevis. Overlades til læseren. ■

Derved har vi fået konstrueret en mængde af rationale tal, som har alle de gode egenskaber, som de rationale tal skal have: Det er et ordnet legeme.

17.3 Konstruktion af taluniverset; en skitse

Efter nu at have set hvordan konstruktionen af $\mathbb{Q}$ ud fra $\mathbb{Z}$ foregår i detaljer, skal vi til slut antyde, hvordan de øvrige successive udvidelser af taluniverset foregår.

1. Fra mængdelæren til $\mathbb{N}_0$: Definer rekursivt:

   (a) $0 = \emptyset$

   (b) $1 = \{0\} = \{\emptyset\}$

   (c) $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$ ...

   Indfør da efterfølgerfunktionen på oplagt måde på mængden af alle disse mængder. Så er Peanos aksiomer opfyldt, og man kan indføre regneoperationerne (kompositionsreglerne) + og ·, samt en ordning. Det vises at disse opfylder de regneregler (aksiomer) som blev nævnt i sætning 118

2. Fra $\mathbb{N}$ til $\mathbb{Z}$. Vi definerer et helt tal x som en ækvivalensklasse af par (m, n) af naturlige tal (tænk på $m - n$), idet vi siger at (m, n) er ækvivalent med (m_1, n_1), hvis $m + n_1 = m_1 + n$. På naturlig vis defineres regneoperationerne, og ordningen, og det vises at disse opfylder de regneregler (aksiomer) som blev nævnt i sætning 118. Endelig vises at man kan indlejre de naturlige tal i $\mathbb{Z}$.

3. Fra $\mathbb{Z}$ til $\mathbb{Q}$. Det var det vi gjorde i forrige afsnit..

4. Fra $\mathbb{Q}$ til $\mathbb{R}$. Dette er det vanskeligste trin. Det kan gøres på to måder:

   (a) Et **Dedekind-snit** i de rationale tal defineres som et par af delmængder (A, B) af de rationale tal, som opfylder

   $$A \cap B = \emptyset \tag{17.26}$$
   $$A \cup B = \mathbb{Q} \tag{17.27}$$
   $$\forall a \in A, \forall b \in B : a < b \tag{17.28}$$

   Vi siger nu at et sådant Dedekind-snit er et reelt tal (bortset fra en enkelt teknikalitet) og kalder mængden heraf for $\mathbb{R}$. Vi definerer så regneoperationer og ordning på $\mathbb{R}$, så det bliver et ordnet legeme, som indeholder en kopi af $\mathbb{Q}$, og viser at det faktisk bliver et fuldstændigt ordnet legeme. For eksempel bliver hullet $\sqrt{2}$ i $\mathbb{Q}$ udfyldt af snittet (A, B) hvor $A = \left\{a \in \mathbb{Q} \mid \left(a^2 < 2\right) \vee a < 0\right\}$ og $B = \mathbb{Q} \setminus A$.

   (b) Man betragter alle **Cauchyfølger** af rationale tal. På denne mængde indføres en ækvivalensrelation som siger at to Cauchyfølger (a_i) og (b_i) er ækvivalente hvis $(a_i - b_i) \to 0$ for $i \to \infty$. Ækvivalensklasserne kaldes reelle tal, og mængden af dem benævnes $\mathbb{R}$. Der indføres nu regneoperationer + og · og en ordning, og det vises at den derved fremkomne struktur er et fuldstændigt ordnet legeme

som indeholder en kopi af $\mathbb{Q}$. Her fyldes hullet $\sqrt{2}$ ud af den ækvivalensklasse af Cauchyfølger af rationale tal, som repræsenteres af Cauchyfølgen

$$1;\ 1,4;\ 1,41;\ 1,414;\ 1,4142 \tag{17.29}$$

altså (a_i) hvor a_i er de første i cifre i decimaludviklingen af $\sqrt{2}$.

5. Fra $\mathbb{R}$ til $\mathbb{C}$. Vi definerer et komplekst tal som et par (x, y) af reelle tal (tænk på $x + iy$). Denne udvidelse har du nok set.

Bemærkning 763 *Vi kan gå endnu videre, idet vi kan lave en model af den Euklidiske plangeometri inden i $\mathbb{R}^2$, og af rumgeometrien inden i $\mathbb{R}^3$.*

17.4 Opgaver

1. Gennemfør konstruktionen af $\mathbb{Z}$ ud fra $\mathbb{N}$. Indfør $+$ og $\cdot$, og vis at $\mathbb{Z}$ bliver er ring.

Kapitel 18

Appendiks. Velordningsprincippet og den arkimediske egenskab

Sætning 764 ***Den arkimediske egenskab***[1]**.** *Til ethvert reelt tal findes der et større naturligt tal. Formelt skrevet:*

$$\forall a \in \mathbb{R} \exists n \in \mathbb{N} : a < n$$

Bevis. Beviset føres ved modstrid. Antag altså at negationen gælder, dvs. at $\exists a \in \mathbb{R} \forall n \in \mathbb{N} : a \geq n$. Hvis a er et sådant reelt tal vil det være et overtal for $\mathbb{N}$, så $\mathbb{N}$ er opadtil begrænset. Da $\mathbb{N}$ ikke er tom, følger af supremumsegenskaben at der findes et supremum b for $\mathbb{N}$. Da b er det mindste overtal og $b-1 < b$ er $b-1$ ikke et overtal. Derfor findes der et $n \in \mathbb{N}$ så $b-1 < n$. Men så er $b < n+1$, og da $n+1 \in \mathbb{N}$, strider det mod at b er et overtal for $\mathbb{N}$. ■

Sætning 765 ***Velordningsprincippet.*** *Enhver ikke-tom mængde af naturlige tal har et mindste element.*

Bevis. Lad A være en ikke tom mængde af naturlige tal. Da A er nedadtil begrænset af 1 er $-A$ opadtil begrænset af -1, så ifølge supremumsegenskaben har $-A$ et supremum $-a$. Men så er a et infimum for A. Da a er det største undertal findes der et naturligt tal $n_0 \in A$ så $n_0 - a \leq 1/4$. Heraf følger at $a \in]n_0 - 1, n_0]$. Da der ikke ligger nogen elementer fra A i $]n_0 - 1, n_0[$ eller i $]-\infty, a[$ (da a er et undertal) ligger der ingen elementer fra A i $]-\infty, a[\cup]n_0 - 1, n_0[=]-\infty, n_0[$. Dvs. alle elementer i A er større eller lig med n_0 som altså er et minimalt element i A.

[1] Efter den græske matematiker Arkimedes (287-212 f.Kr.)

Sætning 766 *Lad a være et helt tal og d et naturligt tal. Da findes der hele tal q og q' så*

$$qd \leq a < (q+1)d \quad og \tag{18.1}$$
$$q'd < a \leq (q'+1)d \tag{18.2}$$

■

Bevis. Hvis $a = 0$ kan vi vælge $q = 0$ og $q' = -1$

Antag dernæst at $a > 0$. Betragt mængden

$$M = \{k \in \mathbb{N} \mid a < kd\}.$$

Denne mængde er ikke-tom, idet $(a+1) \in M$ (det følger, da $1 \leq d$, hvorfor $a < a+1 \leq (a+1)d$). Ifølge velordningsprincippet har M altså et mindste element m. Vi vil nu vise at $q = m-1$ opfylder (18.1). Per definition af M gælder at $a < md = (q+1)d$. Desuden må vi have $qd = (m-1)d < a$ for ellers ville $(m-1) \in M$ i modstrid med at m er det mindste element i M.

Beviset for eksistens af q' i (18.2)for et positivt a kan føres på samme måde ved at betragte mængden

$$M' = \{k \in \mathbb{N} \mid kd \geq a\}.$$

Endelig bemærkes at hvis $a < 0$, da følger eksistensen af q i (18.1) af eksistensen af q' i (18.2) brugt på det positive tal $-a$. Og omvendt følger eksistensen af q' i (18.2) af eksitensen af q i (18.1) brugt på $-a$. Overvej dette. ■

Index