Asger Törnquist

DISTILLAT

ET SUPPLEMENT TIL KURSET DIS

Institut for Matematiske Fag · Københavns Universitet

Version: 18. juni 2019

1
Prolog

Destillat: sammendrag der indeholder de vigtigste elementer. Koncentrat. Fra latin, *destillare* (senlatin: *distillare*, deraf *distill* på engelsk).

Dette er et sæt noter under udarbejdelse til kurset DIS, som supplement til vores grundbog, Jesper Lützens "Diskrete matematiske metoder". For nogle emner er noterne et sammendrag, eller koncentrat, af det, der står i vores grundbog. Andre gange er noterne en uddybelse af det, der står om samme emne i grundbogen. Ikke alle emner fra grundbogen er med i disse noter.
Jeg håber, noterne vil hjælpe deltagerne i DIS med at få maksimalt udbytte af kurset.

Asger Törnquist

2
Udsagn, prædikater, og kvantorer

Matematiske resultater bevises ved at bruge logisk argumentation. I den henseende er matematik anderledes end andre naturvidenskabelige fag, hvor resultater typisk opnås ved eksperimenter i et laboratorium, eller observationer direkte i naturen.

Det er *yderst vigtigt* at den studerende i løbet af de første studieår lærer at lave beviser og at argumentere logisk korrekt.

Vi skal senere i kurset kigge nærmere på udsagnslogik, som er den grundlæggende model for logisk argumentation, men indtil da har vi brug for en basal (men lidt upræcis, naiv) forståelse af hvad et udsagn er, og hvad et prædikat er.

2.1 Udsagn

Vores midlertidige, naive definition på begrebet udsagn er:

> *Et udsagn er noget vi udtrykker, som kan tillægges en sandhedsværdi* **Sand** *eller* **Falsk**.

Konkrete eksempler på udsagn er: "*Margrethe II er dronning af Danmark*" eller "*Solen skinner*". Hvis det første udsagn fortolkes på den oplagte måde, så er det sandt (men det er næppe stadig sandt om 50 år). Derimod er det klart at det andet udsagns sandhedsværdi afhænger af dagen og tidspunktet, hvilket illustrerer en vigtig pointe:

> *Et udsagns sandhedsværdi afhænger af konteksten (situationen) hvori udsagnet fortolkes.*

Et udsagn skal dog altid entydigt kunne tillægges en af de to sandhedsværdier når konteksten er fastlagt.[1]

Eksempler på matematiske udsagn er: "$5 < 2$", eller "$e^{i\pi} = -1$", eller "$\sqrt{2}$ kan ikke udtrykkes som en heltalsbrøk". Hvis disse udsagn fortolkes på den oplagte måde, så er det første udsagn falskt, mens de andre to er sande.

[1] Typiske eksempler på udtryk, som ikke er udsagn er spørgsmål. F. eks. er "Hvad er der i TV?" ikke et udsagn.

2.2 *Prædikater*

I matematik bruger vi ofte variable når vi udtrykker os. F. eks. kunne en matematiker finde på at skrive "$x > 5$", eller "$x^2 + 1 = 0$". Sådanne udtryk kaldes *prædikater* eller *åbne udsagn*.

Indtil værdien af de variable er fastlagt er disse udtryk strengt taget ikke udsagn, idet man ikke kan afgøre sandhedsværdien af f. eks. $x > 5$ uden at vide "hvad x er" (sagt mere korrekt: Hvilken værdi x tillægges).

Typiske eksempler på prædikater er polynomielle ligninger og uligheder som f. eks.

$$x^3 - 5x^2 + 7x + 1 = 0.$$

Igen, det er ikke før x tillægges en værdi at ovenstående bliver et udsagn, og sandhedsværdien af udsagnet er ligeledes afhængig af x's værdi. (Bemærk at udsagnet bliver sandt præcis når x's værdi er en løsning til ligningen $x^3 - 5x^2 + 7x + 1 = 0$.)

Man kan naturligvis også have prædikater med mange variable, f. eks.

$$xyz + 5x^2y - 27 > 0$$

og her er det først når samtlige variables værdier kendes at vi kan afgøre sandhedsværdien.

Et lidt anderledes eksempel på et prædikat, som viser at man skal læse prædikater med omhu, er prædikatet

$$\int_{-1}^{y} x^3 dx > 0.$$

Der er tilsyneladende to variable (x og y) i dette prædikat, men x kan ikke gives en arbitrær værdi her, idet det jo er integrationsvariablen. Det er kun y der kan gives en arbitrær (reel) værdi, og derfor skal dette prædikat læses som et prædikat i kun *én* variabel. Man siger at variablen x er *bundet* hvorimod variablen y er *fri*.

Notation: Abstrakt skrives prædikater ofte som $P(\ldots)$, $Q(\ldots)$, $R(\ldots)$, hvor "$\ldots$" er en liste af den indgående (frie) variable. I eksemplerne ovenfor kunne vi f. eks. lade $P(x)$ være prædikatet $x^3 - 5x^2 + 7x + 1 = 0$, vi kunne lade $Q(x,y,z)$ være prædikatet $xyz + 5x^2y - 27 > 0$, og vi kunne lade $R(y)$ være prædikatet $\int_{-1}^{y} x^3 dx > 0$.

Advarsel nr. 1: man sætter **ikke** lighedstegn mellem prædikater[2]. Hvis vi f. eks. ovenfor bruger $P(x)$ til at benævne prædikatet $x^3 - 5x^2 + 7x + 1 = 0$, så skriver vi **ikke**

$$P(x) = x^3 - 5x^2 + 7x + 1 = 0.$$

Det er strengt forbudt at gøre dette. I den særlige situation hvor man *definerer* et prædikat må man gerne sætte et kolon[3], eksempelvis

$$P(x) : x^3 - 5x^2 + 7x + 1 = 0,$$

[2] Aldrig, aldrig, aldrig lighedstegn *mellem* prædikater!

[3] Dette er ikke licens til at sætte koloner alle mulige steder i forbindelse med prædikater. Der er kun ganske bestemte situationer hvor den notation kan bruges, og en af dem er når man definerer et prædikat.

hvis man da ikke, som jeg gjorde ovenfor, blot skriver i ord at $P(x)$ *er* prædikatet $x^3 - 5x^2 + 7x + 1 = 0$.

Advarsel nr. 2: En udbredt misforståelse er at forveksle prædikater med funktioner. **Prædikater er ikke det samme som funktioner**.

F. eks., hvis $P(x)$ er prædikatet $x^3 - 5x^2 + 7x + 1 = 0$, da er $P(x)$ **ikke** funktionen i x som har foreskriften $x^3 - 5x^2 + 7x + 1$. **Nej!** Husk i stedet følgende:

Et **prædikat** $P(x)$ **er et udsagn om** x *(dvs. det siger noget om x der enten er sandt eller falsk, afhængig af hvilken værdi x gives), hvorimod en* **funktion** $f(x)$ **er noget, der til et givent** x **tilknytter en værdi** *(en "funktionsværdi").*

Advarsel 3: Læseren har sandsynligvis tænkt på ovenstående eksempler på prædikater som havende variable der kan tage talværdier, f. eks. i de reelle eller komplekse tal. Det er fint, men der er intet til hinder for at fortolke x i prædikatet $x^3 - 5x^2 + 7x + 1 = 0$ som en $n \times n$ matrix, hvis 0 så fortolkes som $n \times n$ nulmatricen. Prædikater skal altså, ligesom udsagn, fortolkes inden for en kontekst, og det er en del af denne kontekst at specificere hvilket "domæne" de variable går over (mere præcist: kan tage værdier inden for).

2.3 Konnektiver

Man kan danne nye udsagn og prædikater vha. de *logiske konnektiver*, som er de logiske symboler $\neg, \vee, \wedge, \implies$ og $\iff$.

Symbol	**Symbolets navn**	**Forklaring**
$\neg$	negation	læses "ikke"
$\vee$	disjunktion	læses "eller"
$\wedge$	konjunktion	læses "og"
$\implies$	implikation	læses "medfører"
$\iff$	biimplikation	læses "hvis og kun hvis"

I følgende tabel er P og Q variable der kan tage værdieren "sand" (S) eller "falsk" (F). Tabellen definerer, hvordan sandhedsværdien af udsagnene $\neg P$, $P \vee Q$, $P \wedge Q$, $P \implies Q$, og $P \iff Q$ afhænger af sandhedsværdien af P og Q.

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \implies Q$	$P \iff Q$
S	S	F	S	S	S	S
S	F	F	F	S	F	F
F	S	S	F	S	S	F
F	F	S	F	F	S	S

EKSEMPLER. 1) Hvis $P(x)$ er prædikatet $x^3 - 5x^2 + 7x + 1 = 0$, da er $\neg P$ prædikatet $\neg(x^3 - 5x^2 + 7x + 1 = 0)$ et prædikat der siger

"der gælder **ikke** at $x^3 - 5x^2 + 7x + 1 = 0$". (Almindeligvis skriver man i stedet $x^3 - 5x^2 + 7x + 1 \neq 0$.)

2) Hvis i stedet $P(x)$ prædikatet $(x-3)^2 = 0$ og $Q(x)$ er prædikatet $x > 0$, da er $P \implies Q$ prædikatet $(x-3)^2 \implies x > 0$. Dette prædikat udtrykker at "hvis $(x-3)^2 = 0$ så gælder $x > 0$".

Bemærkning. Vi siger senere mere om logik og konnektiverne i kapitlet om logik. Lad mig dog komme med et par yderligere advarsler (udover dem, der blev givet ovenfor):

Advarsel 4: Ovenstående symboler må **ikke** spredes med rund hånd og tilfældighed udover den matematik man skriver, inklusive hjemme- og afleveringsopgaver.

For det første skal man, hvis man bruger ovenstående symboler, mene det man skriver! Skriver man således $\implies$ i en afleveringsopgave, så skal man kunne forsvare at man mener at det, der står før $\implies$ medfører det, der står efter.

For det andet er det **ikke** ligegyldigt om man skriver $\implies$ eller $\iff$, idet $\implies$ og $\iff$ jo ikke betyder det samme.

For det tredie, så er det at skrive lange kæder af udsagn bundet sammen af stribevis af $\iff$ er dårlig skrivestil (i de fleste tilfælde). Desuden tror mange tilsyneladende at $\iff$ og $=$ betyder nogenlunde det samme (suk!), men at man bare ser klogere ud hvis man skriver $\iff$ i stedet for $=$ i sine opgaver. Igen må det understreges at $\iff$ og $=$ ikke betyder det samme, og man skal derfor skrive det symbol, der korrekt udtrykker det man vil sige. *Er man ikke klar over hvilket symbol man bør bruge, så må man tænke grundigt over hvad det er man prøver at udtrykke*.

Mit råd til jer er at I så vidt muligt undgår at bruge konnektivsymbolerne, og i stedet skriver i ord hvad I mener. Det er det, jeg har gjort de fleste steder i disse noter, og det er det Jesper Lützen har gjort i sin bog.

Advarsel 5: Symbolet $\implies$ udtrykker et betinget udsagn, dvs. et udsagn af formen "hvis... så...".

Det volder tit vanskeligheder at forstå hvordan betingede udsagn fungerer. Hvis jeg skriver $P \implies Q$, betyder det så at både P og Q er sande? (Nej!)

Det er en god idé at huske på, at i vores hverdag bruges betingede udsagn som regel til at diskutere fremtiden. F. eks. kunne man sige "Hvis Socialdemokratiet vinder næste valg, så bliver Mette Frederiksen statsminister". Sandheden af dette udsagn er helt sikkert interessant for politiske kommentatorer at debatere, men husk på, at *selv hvis udsagnet er sandt, så betyder det ikke at Socialdemokratiet vinder næste valg*. For det ved vi jo ikke endnu. Humlen ved betingede udsagn er netop, at de tillader os at tale om noget hypotetisk, dvs. noget der sker *hvis* bestemte betingelser er opfyldt, også selvom de betingelser ikke er opfyldt lige nu, eller måske aldrig bliver det.

2.4 Kvantorer og kvantifikation

Man kan danne et nyt prædikat ud fra et gammelt ved *kvantifikation* over en eller flere variable. Der er to slags kvantifikation, *eksistentiel kvantifikation*, som udtrykkes med symbolet $\exists$ ("eksistenskvantoren"), og *universel kvantifikation*, som udtrykkes ved symbolet $\forall$ ("alkvantoren").

EKSISTENTIEL KVANTIFIKATION. Lad os igen tage prædikatet $P(x)$ fra før, dvs. $P(x)$ er $x^3 - 5x^2 + 7x + 1 = 0$. Når vi skriver

$$(\exists x)\ x^3 - 5x^2 + 7x + 1 = 0,$$

da udtrykker det udsagnet "der findes x så at $x^3 - 5x^2 + 7x + 1 = 0$", eller mere korrekt: "der findes en værdi a som variablen x kan gives, og hvor der gælder at $a^3 - 5a^2 + 7a + 1 = 0$".

Bemærk at kvantifikationen over x gør, at x ikke er en fri variabel i $(\exists x)P(x)$. Man siger at kvantifikationen over x *binder* x. Da der ikke er nogen frie variable i $(\exists x)\ P(x)$ er dette prædikat et udsagn (dvs., det er enten sandt eller falsk, afhængig af den kontekst hvor det fortolkes).

Øvelse 1 *Fortolk $P(x)$ i konteksten af de reelle tal (specielt er x en variabel der tager reelle værdier). Afgør om udsagnet $(\exists x)P(x)$ er sandt eller falsk.*

Som et andet eksempel på eksistentiel kvantifikation, lad $Q(x,y,z)$ være prædikatet $xyz + 5x^2y - 27 > 0$. Da er

$$(\exists y)\ xyz + 5x^2y - 27 > 0$$

et prædikat med to frie variable (x og z). Variablen y er ikke længere fri da kvantifikationen $(\exists y)$ binder y. Prædikatet $(\exists y)Q(x,y,z)$ udtrykker at "om x og z gælder det, at der findes (eksisterer) y sådan at $xyz + 5x^2y - 27 > 0$". M.a.o., $(\exists y)Q(x,y,z)$ er et *eksistentielt udsagn* om x og z.

UNIVERSEL KVANTIFIKATION. Lad igen $P(x)$ være $x^3 - 5x^2 + 7x + 1 = 0$. Når vi skriver

$$(\forall x)\ x^3 - 5x^2 + 7x + 1 = 0$$

da udtrykker det udsagnet "for all x gælder $x^3 - 5x^2 + 7x + 1 = 0$", eller mere korrekt: "For alle værdier a som variablen x kan tilskrives gælder $a^3 - 5a^2 + 7a + 1 = 0$".

Bemærk at kvantifikationen over x gør at x ikke længere er en fri variabel i $(\forall x)P(x)$. Da der ikke er nogen fri variable i $(\forall x)P(x)$ er dette prædikat et udsagn (dvs., det er enten sandt eller falsk, afhængig af den kontekst hvor det fortolkes).

Øvelse 2 *Fortolk $P(x)$ i konteksten af de reelle tal. Er udsagnet $(\forall x)P(x)$ sandt eller falsk?*

Som et andet eksempel på universel kvantifikation, tag igen $Q(x,y,z)$ til at være prædikatet $xyz + 5x^2y - 27 > 0$. Da er

$$(\forall y)\ xyz + 5x^2y - 27 > 0$$

et prædikat med to frie variable (x og z). (Variablen y er ikke længere fri da kvantifikationen $(\forall y)$ binder y.) Prædikatet $(\forall y)Q(x,y,z)$ udtrykker at "om x og z gælder det, at for alle y er $xyz + 5x^2y - 27 > 0$". M.a.o., $(\forall y)Q(x,y,z)$ er et *universelt udsagn* om x og z.

Kvantorer og negation. Lad $P(x)$ være et prædikat med x som fri variabel. Bemærk at $\neg(\exists x)P(x)$ (dvs. "der findes ikke x så at $P(x)$") udtrykker det samme som at $(\forall x)\neg P(x)$ ("for alle x gælder ikke at $P(x)$").

På samme måde indser vi, at $\neg(\forall x)P(x)$ (dvs. "det gælder ikke for alle x at $P(x)$") udtrykker det samme som $(\exists x)\neg P(x)$ (dvs. "der findes x så at $P(x)$ ikke holder").

Dette giver anledning til følgende regler for kvantorer og negation:

$$\neg(\exists x) \textit{ kan erstattes af } (\forall x)\neg \textit{ (og omvendt)}$$

og

$$\neg(\forall x) \textit{ kan erstattes af } (\exists x)\neg \textit{ (og omvendt).}$$

Prædikater med mange kvantorer. Nu stiger kunsten! Vi skal se på gentagen brug af kvantifikation, og starter med at se på eksempler hvor $\forall$ efterfølges af $\exists$, eller hvor $\exists$ efterfølges af $\forall$, dvs. hvor kvantorerne $\forall$ og $\exists$ **alternerer**.

Lad os betragte prædikatet i to variable

$$P_0(x,y) : 3x^2y - xy + 5y = 7.$$

Ved først at bruge eksistentiel kvantifikation over y får vi prædikatet

$$P_1(x) : (\exists y)\ 3x^2y - xy + 5y = 7.$$

Herefter bruger vi universel kvantifikation over x i P_1 og opnår udsagnet

$$P_2 : (\forall x)(\exists y)\ 3x^2y - xy + 5y = 7.$$

Dette udsagn siger: For alle værdier som x kan tage findes en værdi som y kan tage, således ligningen $3x^2y - xy + 5y = 7$ er opfyldt.

Øvelse 3 *Fortolk P_2 inden for de reelle tal. Er udsagnet P_2 sandt?*

Lad os nu prøve i stedet af gå den anden vej rundt: Først bruges alkvantoren over x i P_0 og vi får

$$Q_1(y) : (\forall x)3x^2y - xy + 5y = 7.$$

Dernæst bruger vi eksistenskvantoren på y:

$$Q_2 : (\exists y)(\forall x)3x^2y - xy + 5y = 7.$$

Dette udsagn udtrykker: Der findes en værdi som y kan tage sådan at enhver værdi som x kan tage er en løsning til ligningen $3x^2y - xy + 5y = 7$.

Øvelse 4 *Fortolk Q_2 inden for de reelle tal. Er udsagnet Q_2 sandt?*

Læseren har forhåbentlig i de to foregående øvelser indset at P_2 er sandt, mens Q_2 er falskt, hvis de fortolkes inden for de reelle tal. Den eneste forskel mellem P_2 og Q_2 er rækkefølgen på kvantorerne $\forall$ og $\exists$, men denne rækkefølge er afgørende for betydningen af hhv. P_2 og Q_2.[4]

Eksemplet med P_2 og Q_2 ovenfor illustrerer følgende vigtige pointe:

Alternerende kvantorer *må* **aldrig** *ombyttes uden videre, idet prædikatets betydning næsten altid ændres hvis rækkefølgen af kvantorerne ændres.*

Ovenstående gælder dog kun alternerende kvantorer, idet der gælder følgende:

Sætning 2.4.1 *Lad $P(x_1, \ldots, x_n)$ være et prædikat i n variable, og lad $1 \leq i < j \leq n$. Da gælder:*

1) Prædikaterne $(\exists x_i)(\exists x_j)P(x_1, \ldots, x_n)$ og $(\exists x_j)(\exists x_i)P(x_1, \ldots, x_n)$ er ensbetydende.

2) Prædikaterne $(\forall x_i)(\forall x_j)P(x_1, \ldots, x_n)$ og $(\forall x_j)(\forall x_i)P(x_1, \ldots, x_n)$ er ensbetydende.

Øvelse 5 *Betragt udsagnene*

$$(\exists x)(\forall y)3x^2y - xy + 5y = 7$$

og

$$(\forall y)(\exists x)3x^2y - xy + 5y = 7.$$

Fortolk dem inden for de reelle tal. Er disse udsagn sande eller falske?

Øvelse 6 *Hvis vi i stedet fortolker udsagnene i foregående øvelse inden for de komplekse tal, er de da sande eller falske?*

2.5 Et sidste ord om notation og kvantorer

Der er ikke fodslag i matematikken hvad angår notation omkring kvantorer. Nogle forfattere sætter et kolon efter en streng af kvantorer, f. eks.

$$\forall y\ \exists x : 3x^2y - xy + 5y = 7$$

[4] Vigtigheden af kvantorernes orden kan sammenlignes med vigtigheden af ordnen ved summation og integration, f. eks. $\sum_{i=1}^{\infty}\left(\int_0^{2\pi}\frac{1}{i}\sin(x)dx\right) = 0$, hvorimod integranten i $\int_0^{2\pi}\left(\sum_{i=1}^{\infty}\frac{1}{i}\sin(x)\right)dx$ er udefineret.

mens andre bare skriver

$$\forall y\ \exists x\ 3x^2y - xy + 5y = 7,$$

hvilket dog kan være lidt svært at læse ("$x\ 3x^2y$"). Andre igen sætter en parentes *efter* en streng af kvantorer

$$\forall y\ \exists x\ (3x^2y - xy + 5y = 7).$$

Jeg har ovenfor sat parentes *rundt om* kvantorerne, e.g.

$$(\forall y)(\exists x)\ 3x^2y - xy + 5y = 7.$$

Denne notation (som er lidt tung) skyldes tilsyneladende Tarski, den store Polske logiker, der som professor på UC Berkeley skabte en skole inden for matematisk logik. Notationen spredte sig til universiteterne i resten af Californien, og kaldes derfor nogen gange "Californisk notation".

Jeg anbefaler at man for sig selv vælger den notation blandt ovenstående man bedst kan lide, og som man synes er lettest at læse.

3
Første kig på mængder, og særligt talmængder

Indhold: *Repetition af basale mængdebegreber og korrekt brug af mængdenotation. Talmængderne* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. *Elementære mængdeoperationer. Funktioner (foreløbig definition). Strukturen af de naturlige tals mængde* $\mathbb{N}$*: Induktionsaksiomet, velordningsprincippet. Definition ved rekursion.*

3.1 Basale mængdebegreber og mængdenotation

Mængdelære behandles mere indgående senere, og dette afsnit er blot repetition og udpensling af materiale der forhåbentlig er kendt i en eller anden grad. Det er dog *uhyre vigtigt* at man bliver fortrolig med at bruge de basale mængdebegreber og den tilhørende notation korrekt, så læs det grundigt.

En *mængde* er en samling eller familie af matematiske objekter, og objekterne i en mængde kaldes mængdens *elementer* eller *medlemmer*. Hvis A er en mængde og x er et objekt, da betyder $x \in A$ at x er et element i A; symbolet $\in$ kaldes *medlemskabsrelationen*. Man læser $x \in A$ som "x er i A", eller"x er medlem i A" eller "x er element i A". Hvis x *ikke* er medlem i A da skrives $x \notin A$.

Notationen $A \subseteq B$ betyder at A er en *delmængde* af B, dvs. ethvert element i A er et element i B. Man læser $A \subseteq B$ som "A er en delmængde af B" eller "A er indeholdt i B". Hvis både $A \subseteq B$ og $B \subseteq A$ da er $A = B$ (overvej!).[1]

Følgende er særligt vigtige mængder: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ og $\mathbb{C}$. [2] Mængden

$$\mathbb{N} = \{1, 2, 3, \ldots, n, \ldots\},$$

er mængden[3] af *naturlige tal*. Mængden

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

er mængden af *hele tal*. $\mathbb{Q}$ er mængden af *rationale tal*, dvs. tal der kan skrives som en brøk $\frac{m}{n}$, hvor $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. Endelig er $\mathbb{R}$ mængden af *reele tal*, og $\mathbb{C}$ mængden af *komplekse tal*. Bemærk at $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

[1] Metode: Skal man vise for mængde A og B at $A = B$ gøres dette ofte ved at vise de to inklusioner $A \subseteq B$ og $B \subseteq A$.

[2] Bemærk at $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ og $\mathbb{C}$ har uendeligt mange medlemmer.

[3] Bemærk at $\mathbb{N}$ (og $\mathbb{Z}$) er angivet ved at liste elementerne mellem de krøllede paranteser $\{$ og $\}$. At kunne forstå og bruge denne notation er vigtigt.

Den *tomme mængde* $\emptyset$ er et andet vigtigt eksempel. Den tomme mængde har ingen elementer, dvs. $x \notin \emptyset$ for alle x.

Mængdebyggeren.[4] En uhyre vigtig måde at angive en delmængde af en given mængde på er ved hjælp af *mængdebyggernotationen*, hvor en delmængde defineres ved hjælp af et prædikat (dvs., åbent udsagn).

Er A en mængde og $P(x)$ prædikat om variablen x, så er

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

(del-) mængden af de elementer i $x \in A$ hvor $P(x)$ er sand. Bemærk at *før* opdelingssymbolet (her kolon, men ofte bruges en lodret streg $|$ i stedet) angives hvilken mængde x tilhører, og efter opdelingen angives hvilken egenskab x skal opfylde, og denne egenskab udtrykkes ved et prædikat om x.

Eksempler: Lad $P(x)$ være prædikatet "$x \geq 0$". Så er

$$\{x \in \mathbb{Z} : P(x)\} = \{x \in \mathbb{Z} : x \geq 0\}$$

mængden $\{0, 1, 2, 3, \ldots\}$.[5]

Hvis i stedet $P(x)$ er prædikatet "$x \neq x$", så er

$$\{x \in \mathbb{N} : P(x)\} = \{x \in \mathbb{N} : x \neq x\} = \emptyset.$$

Overvej!

Hvis $P(x)$ er prædikatet "der findes $m \in \mathbb{Z}$ og $n \in \mathbb{N}$ så at $x = \frac{m}{n}$", så er

$$\{x \in \mathbb{R} : P(x)\} = \mathbb{Q}.$$

Elementære mængdeoperationer. Lad A og B være mængder. Vi definerer:

$$A \cup B = \{x : x \in A \textbf{ eller } x \in B\} \text{ (\textit{foreningsmængde})}$$
$$A \cap B = \{x : x \in A \textbf{ og } x \in B\} \text{ (\textit{fællesmængde} eller \textit{snit})}$$
$$A \setminus B = \{x : x \in A \textbf{ og } x \notin B\} \text{ (\textit{mængdedifferens})}$$
$$A \triangle B = (A \setminus B) \cup (B \setminus A) \text{ (\textit{symmetrisk differens})}$$

Hvis i tredje linje vi har $B \subseteq A$, så kaldes $A \setminus B$ også "komplementærmængden" til B i A. Hvis A er underforstået skrives til tider $\complement B$, B^c eller $\sim B$ i stedet for $A \setminus B$. Notationen $A \setminus B$ er dog næsten altid at foretrække, idet den gør A eksplicit.

Bemærk at vi i definitionen af $\cup$, $\cap$ og $\setminus$ har misbrugt mængdebyggernotationen en anelse. Det burde nemlig specificeres på venstre side af : hvilken mængde x skal tilhøre. Med hensyn til $\cap$ og $\setminus$ kan vi bruge mængden A (overvej!), og i definitionen af $A \cup B$ kan vi tage en mængde C der opfylder $A \subseteq C$ og $B \subseteq C$. At en sådan mængde C altid findes er et af mængdelærens aksiomer (grundprincipper).

Funktioner. Vi indfører det abstrakte, mængdeteoretiske funktionsbegreb i en senere forelæsning. Indtil da skal du tænke på funktioner på

[4] Mængdebyggernotationen er, trods overfladisk typografisk lighed, *ikke* det samme som når vi lister en mængdes elementer mellem krøllede paranteser som gjort ovenfor. Lær at bruge begge notationer korrekt.

[5] Mængden $\{0, 1, 2, 3, \ldots\}$ betegnes almindeligvis med enten $\mathbb{N}_0$ eller ω.

samme måde som du altid har gjort: Ved en funktion f fra en mængde A til en mængde B, i symboler $f : A \to B$, forstås en regel der for ethvert $x \in A$ knytter et (og kun et) element $f(x) \in B$.

Eksempel og definition: Funktionen $\mathcal{S} : \mathbb{N} \to \mathbb{N}$ er givet ved foreskriften $\mathcal{S}(n) = n + 1$.

Uordnede og ordnede par; cartesisk produkt. Givet a og b, da kaldes mængden $\{a, b\}$ det *uordnede par* af a og b; der gælder

$$x \in \{a, b\} \text{ hvis og kun hvis } x = a \text{ eller } x = b.$$

Da $\{a, b\} = \{b, a\}$ har den orden vi lister elementerne ingen betydning for det uordnede par.

Det *ordnede par* betegnes (a, b), og her er rækkefølgen vigtig. Der gæder:

$$(x, y) = (a, b) \text{ hvis og kun hvis } x = a \text{ og } y = b.$$

Eksempel: Det uordnede par at 3 og 5 er $\{3, 5\} = \{5, 3\}$. Det ordnede par af 3 og 5 er $(3, 5)$, hvorimod det ordnede par af 5 og 3 er $(5, 3)$. Bemærk $(3, 5) \neq (5, 3)$.

Definition 3.1.1 *Lad A og B være mængder. Det* cartesiske produkt *af A og B er mængden*

$$A \times B = \{(a, b) : a \in A \text{ og } b \in B\},$$

dvs. mængden af alle ordnede par der kan dannes ved først at tage et element i A og derefter et element fra B.[6]

Eksempel: $\mathbb{R} \times \mathbb{R}$ er den mængde, vi almindeligvis tænker på som planen i elementær geometri.

(Senere i kurset vil vi indføre produkt af flere end to mængder.)

[6] Bemærk at vi igen har misbrugt mængdebyggeren en anelse, idet det ikke er specificeret før : hvilken mængde (a, b) skal tilhøre. Bare rolig: Mængdelærens aksiomer sikrer, at der findes en mængde som har alle tænkelige par (a, b), hvor $a \in A$ og $b \in B$, som medlemmer. Se afsnittet om substitutionsaksiomet i slutningen af dette kapitel (ikke pensum).

3.2 De naturlige tals mængde

Vi skal nu se nærmere på mængden $\mathbb{N}$. Denne mængde er uden tvivl den vigtigste mængde i matematik, idet den er forbindelsen mellem det endelige og det uendelige: Elementerne i $\mathbb{N}$, dvs. $1, 2, 3, \ldots$, repræsenterer endelige antal, men $\mathbb{N}$ selv er ikke en endelig mængde.

Der gælder to grundlæggende principper (aksiomer) for de naturlige tals mængde, som spiller en central rolle i mange beviser: Det er *Induktionsaksiomet* og *Velordningsprincippet*.

Induktionsaksiomet: Hvis A er en mængde og der gælder at

1. $1 \in A$; og
2. hvis $n \in A$ så er $n + 1 \in A$

så er $\mathbb{N} \subseteq A$.

En anden måde at formulere Induktionsaksiomet er: $\mathbb{N}$ er den mindste mængde der indeholder 1 og som er lukket under funktionen $\mathcal{S}(n) = n + 1$. Med denne formulering er aksiomets sandhed indlysende. (Overvej!)

Det er vigtigt at forstå at den anden linje i induktionsaksiomet er et *betinget* udsagn: Det siger *ikke* at $n \in A$, det siger blot at *hvis* $n \in A$ *så* er $n + 1 \in A$. Det er væsentligt at forstå dette.[7]

Induktionsaksiomet muliggør *bevis ved (matematisk) induktion*, en vigtig metode. Selvom aksiomet kan anvendes direkte i sådanne beviser, så bruges oftere følgende "prædikatformulering".

[7] Et almindeligt pædagogisk billede af induktionsaksiomet er at forestille sig de naturlige tal som en uendelig række af domino brikker, der er stillet op sådan at hvis den n'te brik vælter, så vælter også den $(n+1)$'te brik. Da gælder at hvis vi vælter den første brik, så vil alle brikker vælte.

Sætning 3.2.1 ("Bevis ved induktion") *Lad $P(n)$ være et prædikat (åbent udsagn) om $n \in \mathbb{N}$. Antag:*

1. *$P(1)$ er sand; og*
2. *hvis $P(n)$ er sand for et $n \in \mathbb{N}$ så er $P(n+1)$ sand.*

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

Bevis: Vi bruger Induktionsaksiomet. Lad

$$A = \{n \in \mathbb{N} : P(n)\}.$$

Per antagelse gælder da at $1 \in A$ og at hvis $n \in A$ så er $n + 1 \in A$. Induktionsaksiomet giver derfor at $\mathbb{N} \subseteq A$. Da $A \subseteq \mathbb{N}$ følger at $A = \mathbb{N}$. Fra definitionen af A følger nu at $P(n)$ er sand for alle $n \in \mathbb{N}$. □

Føgende eksempel er en typisk anvendelse af bevis ved induktion.

EKSEMPEL. Bevis følgende formel for summen af de første n ulige tal

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

er sand for alle $n \in \mathbb{N}$.

Løsning. Formlen ovenfor udtrykker noget (lighed), der enten er sandt eller falsk for en given værdi af n, og derfor er det et prædikat om n. Kald derfor kalde formlen ovenfor $P(n)$.

Induktionsstart: P(1) er sand idet det blot siger at $1 = 1^2$.

Induktionstrin: Antag at $P(n)$ er sand. Så gælder altså $\sum_{i=1}^{n}(2i - 1) = n^2$, og vi kan derfor lave følgende udregning:

$$\sum_{i=1}^{n+1}(2i-1) = (\sum_{i=1}^{n}(2i-1)) + (2(n+1)-1) = n^2 + 2n + 1 = (n+1)^2.$$

Dette viser at $P(n+1)$ er sand hvis $P(n)$ er sand.

Nu har vi vist at de to betingelser i Sætningen om bevis ved induktion er opfyldt, og derfor kan vi konkludere at $P(n)$ er sand for alle n, som ønsket. □

Følgende sætning er en tilsyneladende stærkere variant af Sætning 3.2.1, som vi ofte vil få brug for i kurset. Den muliggør bevis ved såkaldt *fuldstændig induktion*.

Sætning 3.2.2 ("Bevis ved fuldstændig induktion") *Lad $Q(n)$ være et prædikat om $n \in \mathbb{N}$. Antag:*

1. *$Q(1)$ er sand; og*
2. *hvis $Q(1), \ldots, Q(n)$ er sande (for et $n \in \mathbb{N}$) så er $Q(n+1)$ sand.*

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

Bemærk at 2. i foregående sætning er et betinget udsagn, hvis hypotese (antecedent) er $Q(1) \wedge \cdots \wedge Q(n)$, og hvis konklusion er $Q(n+1)$. I Sætning 3.2.1 er 2. et betinget udsagn hvis hypotese er $P(n)$ og konklusion er $P(n+1)$. Derfor er hypotesen i 2. i Sætning 3.2.2 stærkere end hypotesen i 2. i Sætning 3.2.1. Det er denne ekstra styrke der udnyttes i beviser, der bruger fuldstændig induktion i stedet for "almindelig" induktion.

Bevis for Sætning 3.2.2. **Øvelse! Skal afleveres som første obligatoriske opgave d. 12. September, 2018.** (Helst i forelæsningen eller til øvelserne, og helst printet ud eller i tydelig håndskrevet format. Men email afleveringer accepteres hvis de sendes både til Asger og Alex senest 23:59 d. 12. september.)

Hint: Definer et nyt prædikat $P(n)$ ved

$$P(n) : (\forall i)\ 1 \leq i \leq n \implies Q(i).$$

Dette prædikat (med den fri variabel n) siger, med andre ord, at for alle $1 \leq i \leq n$ gælder $Q(i)$. Brug Sætning 3.2.1 på prædikatet P. □

Velordningsprincippet er en anden fundamental egenskab ved de naturlige tals mængde:

Velordningsprincippet. Enhver **ikke-tom** delmængde $A \subseteq \mathbb{N}$ har et mindste element, dvs. et element $a \in A$ hvorom der gælder at $x \geq a$ for alle $x \in A$.

Læseren bør overbevise sig selv om at velordningsprincippet er indlysende gyldigt.

Velordningsprincippet og induktionsaksiomet er to sider af samme mønt: Man kan bevise velordningsprincippet fra induktionsaksiomet, og man kan bevise induktionsaksiomet fra velordningsprincippet. Derfor er det ingen overraskelse at beviser, der føres ved induktion, ofte kan gennemføres ved at bruge velordningsprincippet i stedet. Som regel bliver beviset dog så indirekte, dvs. ved modstrid. Følgende er et typisk eksempel.

EKSEMPEL. Brug velordningsprincippet til at bevise at

$$1+3+5+\cdots+(2n-1)=n^2$$

for alle $n \in \mathbb{N}$.

Løsning. Lad som før

$$A=\{n\in\mathbb{N}:\sum_{i=1}^{n}(2i-1)=n^2\},$$

og lad $B=\mathbb{N}\setminus A$. Vi vil vise at $B=\emptyset$.

Hvis ikke $B=\emptyset$, så findes ifølge velordningsprincippet et mindste element $n\in B$. Vi kan ikke have at $n=1$, idet $1=1^2$ og derfor $1\in A$. Derfor må vi have $n>1$. Da n er mindst følger at $n-1\in A$, dvs. $\sum_{i=1}^{n-1}(2i-1)=(n-1)^2$. Men da følger

$$\sum_{i=1}^{n}(2i-1)=(\sum_{i=1}^{n-1}(2i-1))+2n-1=(n-1)^2+2n-1=n^2,$$

og derfor at $n\in A$, i modstrid med at $n\in B$. □

Man ser at det foregående bevis indeholder de samme ingredienser som beviset for samme ved induktion, men at ingredienserne blandes lidt anderledes. I dette tilfælde er induktionsbeviset nok enklere, men det er langt fra altid tilfældet: Ofte bliver meget omstændelige induktionsbeviser enklere ved at bruge velordningsprincippet i stedet.

Definition ved rekursion. Vi runder dette kapitel af ved kort at tale om definition af funktioner på $\mathbb{N}$ ved *rekursion*, her i en meget simpel version. Dette er en uhyre vigtig måde at definere funktioner (og mange andre ting) på i moderne matematik.

Sætning 3.2.3 (Definition ved rekursion, simpel version.) *Lad $g:\mathbb{N}\times A\to A$ være en funktion og lad $a_1\in A$. Da findes en og kun en funktion $f:\mathbb{N}\to A$ som opfylder $f(1)=a_1$ og*

$$f(n+1)=g(n+1,f(n)).$$

Beviset for sætningen kræver en anelse mere mængdeteori, så vi udskyder det. I stedet giver vi et par eksempler på funktionsdefinition ved rekursion.

EKSEMPEL. Lad $g:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ være funktionen $g(m,n)=mn$, og lad $a_1=1$. Lad f være givet ved rekursion. Så er $f(1)=1$, $f(2)=g(2,f(1))=g(2,1)=2$, $f(3)=g(3,f(2))=g(3,2)=6$, osv. Generelt er $f(n)=n!$, hvilket kan bevise ved induktion.

EKSEMPEL. Lad $g:\mathbb{N}\times(\mathbb{N}\times\mathbb{N})\to\mathbb{N}\times\mathbb{N}$ være $g(m,(i,j))=(j,i+j)$, og lad $f(1)=(1,1)$. Da er $f(2)=g(2,f(1))=(1,2)$, $f(3)=g(3,f(2))=g(3,(1,2))=(2,3)$, $f(4)=g(4,(2,3))=(3,5)$, osv.

Dermed giver 2. koordinaten af $f(n)$ det n'te tal i *Fibonacci følgen*:

$$1,1,2,3,5,8,13,21,34,55,\ldots.$$

Bemærkning. Ofte angives definitioner ved rekursion mere uformelt end det er gjort ovenfor. I det første eksempel vil man ofte blot skrive: Definer $f : \mathbb{N} \to \mathbb{N}$ rekursivt ved $f(1) = 1$ og $f(n+1) = (n+1)f(n)$. Eller hvis man ønsker at definere en funktion $F : \mathbb{N} \to \mathbb{N}$ hvor $F(n)$ er det n'te tal i Fibonacci følgen, så vil man blot skrive: Lad $F(1) = F(2) = 1$, og lad $F(n) = F(n-2) + F(n-1)$ for $n > 2$.

Det kræver lidt tilvending at forstå sådanne rekursive definitioner, idet de på overfladen ser cirkulære ud: F defineres ved F selv, hvilket synes absurd. Pointen er naturligvis at $F(n)$ ovenfor defineres ud fra *tidligere* definerede værdier, nemlig $F(n-2)$ og $F(n-1)$. Så $F(3)$ kan udregnes *alene fordi* vi har angivet til at begynde med at $F(1) = F(2) = 1$. Så kan $F(4)$ udregnes fordi $F(2)$ og $F(3)$ nu er kendt, osv.

I det kommende kapitel om logik vil rekursive definitioner dukke op igen når vi definerer hvad et formelt udsagn er. Det er derfor vigtigt at man lærer at forstå sådanne definitioner.

En advarsel om ordene induktion og rekursion. Induktion bruges i beviser, rekursion bruges i definitioner. Derfor er korrekt sprogbrug at sige "*vi beviser ved induktion...*" og "*vi definerer rekursivt...*". Desværre ser man tit at selv erfarne matematikere bytter om på ordene (e.g. "definerer induktivt" — suk!), hvilket er forkert sprogbrug. Pinligt!

*3.3 Substitutionsaksiomet**

Vi afsluttet med en kommentar om en almindelig udvidelse af brugen af mængdebyggernotationen. Dette er ikke en del af pensum.

Husk, at mængdebyggeren kan anvendes når vi har en mængde A og et prædikat $P(x)$ til at danne mængden

$$\{x \in A : P(x)\},$$

dvs. delmængden af A bestående af de elementer i A om hvilke $P(x)$ er sand.

Man ser dog ofte en lidt anderledes udseende anvendelse af mængdebyggeren. F. eks. kan man støde på følgende definition af de lige tal:

$$\{2n : n \in \mathbb{N}\}.$$

Det er klart hvordan man skal forstå det, men det er ikke klart at mængdebyggeren tillader dette. Følgende princip (formelt kalder "substitutionsaksiomet") er det der tillader denne udvidede brug af mængdebyggeren.

Udvidet mængdebyggerprincip. Lad $P(x,y)$ være et prædikat i to variable, og lad X være en mængde. Antag at der gælder at for hvert $x \in X$ findes *præcis ét* y således at $P(x,y)$ er sand, og betegn for hvert x med $\varphi(x)$ dette entydige y. Da skriver vi

$$\{\varphi(x) : x \in X\}$$

for mængden af de y hvorom der gælder, at der findes $x \in X$ så at $P(x,y)$ er sand.

Hvis vi tager eksemplet fra før, da kan vi lade $P(n,y)$ være prædikatet $y = 2n$, og $\varphi(n) = 2n$. Da er $\varphi(n)$ for hvert $n \in \mathbb{N}$ det entydige y så at $P(n,y)$. Derfor tillader det udvidede mængdebyggerprincip at vi danner mængden

$$\{\varphi(n) : n \in \mathbb{N}\}$$

dvs. mængden $\{2n : n \in \mathbb{N}\}$.

4
Elementær talteori

I dette kapitel ser vi nærmere på den algebraiske struktur af $\mathbb{N}$ og $\mathbb{Z}$. Det gennemgående tema er divisorer i hele tal.

Definition 4.0.1 *(a) Lad $a, d \in \mathbb{Z}$. Vi siger at d er en* **divisor** *i a, og at a er et* multiplum *af d, hvis der findes $q \in \mathbb{Z}$ så at $a = qd$.*[1] *I så fald skriver vi $d|a$, hvilket læses "d går op i a".*

[1] Vores definition inkluderer muligheden at $a = 0$, men $a = 0$ udgør et lidt fjollet særtilfælde: Alle tal er divisorer i 0, og ethvert multiplum af 0 er 0.

Lad os lave nogle basale, men nyttige, observationer om denne definition:

(1) Bemærk at

$$a = 1a = (-1)(-a)$$

og derfor er ± 1 og $\pm a$ altid divisorer i a.[2] Specielt er $|a|$ divisor i a.

[2] Man kalder ± 1 og $\pm a$ de **trivielle divisorer** i a.

(2) Hvis $a = qd$ da er $a = (-q)(-d)$ og $-a = (-q)d = q(-d)$ hvorfra det følger at hvis d er divisor i a da er $\pm d$ divisor i $\pm a$. Derfor følger at hvis d er divisor i a da er $|d|$ divisor i $|a|$.

(3) Hvis d er divisor i $a \neq 0$, så gælder $-|a| \leq d \leq |a|$, og specielt har a kun endeligt mange divisorer. For at se dette er det naturligvis nok at vise at $|d| \leq |a|$ (overvej). Da $|d|$ er divisor i $|a|$ findes q så at $|a| = q|d|$. Der må gælde at $q \geq 1$, for ellers fås modstriden $|a| \leq 0$. Men uligheden $q \geq 1$ giver ved multiplikation med $|d|$ på begge sider at $|a| = q|d| \geq |d|$, som ønsket.

4.1 Division med rest

Lad $a, d \in \mathbb{Z}$ hvor $d > 0$. Det vil naturligvis langt fra altid være tilfældet at d er divisor i a. Når vi har gjort vores bedste forsøg på at skrive a som et multiplum af d kan der nemlig være "noget tilbage", en *rest*, der er mindre end d og derfor ikke kan deles yderligere med d. F. eks. går $d = 3$ ikke op i $a = 10$. Det tætteste vi kan komme er $9 = 3 \cdot 3$, og så har vi altså resten $1 = 10 - 9$.

Følgende sætning siger at division med rest altid er mulig.

Sætning 4.1.1 (Division med rest) *Lad $a \in \mathbb{Z}$ og $d \in \mathbb{N}$. Da findes entydigt bestemte tal*[3] *$r, q \in \mathbb{Z}$ sådan at*

$$a = qd + r$$

[3] r kaldes *resten af a ved division med d*; q kaldes *kvotienten*.

og $0 \leq r < d$.

Tilfældet $r = 0$ i sætningen sker selvfølelig præcis når d er divisor i a. Før vi beviser sætningen beviser vi et Lemma, der er vigtigt i sig selv.

Lemma 4.1.2 (Den "arkimediske egenskab" for $\mathbb{Z}$) *Lad $d \in \mathbb{N}$, $a \in \mathbb{Z}$. Da findes et $q, q' \in \mathbb{Z}$ sådan at*

$$qd \leq a < (q+1)d$$

og

$$q'd < a \leq (q'+1)d$$

Bevis. Hvis $a = 0$ kan vi tage $q = 0$ og $q' = -1$.

Antag dernæst at $a > 0$. Betragt mængden

$$M = \{k \in \mathbb{N} : kd > a\}.$$

Denne mængde er ikke tom idet $k = a+1 \in M$. (Dette følger da $d \geq 1$ og derfor har vi $(a+1)d \geq a+1 > a$.) Ifølge velordningsprincippet har M derfor et mindste element, kald det m. Lad $q = m-1$. Per definition gælder da at $(q+1)d > a$. Desuden må vi have at $qd \leq a$, for ellers gælder $q \in M$, i modstrid med at $m = q+1$ er det mindste element i M.

Beviset for eksistensen af q' overlades til læseren, se øvelsen nedenfor.

Endelig bemærkes at hvis $a < 0$, da følger den første ulighed for a ved at bruge den anden ulighed på $-a$, og den anden ulighed for a følger ved at bruge den første ulighed på $-a$. (Overvej nøje!) □

Øvelse 7 *I det foregående bevis mangler vi at finde q' i tilfældet $a > 0$. Gør dette. Hint: Betragt f. eks. mængden*

$$M' = \{k' \in \mathbb{N} : k'd \geq a\}.$$

Øvelse 8 *Vis at q (og q') i det foregående lemma er entydige, f. eks. ved at vise at hvis q er som ønsket i lemmaet, så er q det mindste element i mængden M (defineret i foregående bevis).*

Bevis for Sætning 4.1.1:
Eksistens: Det foregående lemma giver $q \in \mathbb{Z}$ sådan at $qd \leq a < (q+1)d$. Ved at trække qd fra i denne ulighed fås

$$0 \leq a - qd < (q+1)d - qd = d.$$

Hvis vi derfor lader $r = a - qd$ da er $a = qd + r$ og $0 \leq r < d$, som ønsket.
Entydighed: Hvis både $a = qd + r$ og $a = q'd + r'$ hvor $0 \leq r, r' < d$, da fås fra den foregående ulighed at $-d < r - r' < d$. Da $r = a - qd$ og $r' = a - q'd$ følger at

$$-d < (qd - a) - (q'd - a) < d.$$

Da a går ud i den foregående ulighed, og $qd - q'd = (q - q')d$, har vi altså at $-d < (q - q')d < d$, hvilket kun kan lade sig gøre hvis $q - q' = 0$. Altså er $q = q'$, og derfor har vi

$$r = a - qd = a - q'd = r'.$$

Da vi nu har $q = q'$ og $r = r'$ har vi altså vist entydigheden. □

Bemærkning. I skolen lærer man at dividere med rest ved *succesive approximationer*. Fra et abstrakt synspunkt består metoden i, at hvis man ønsker at dividere $a \in \mathbb{N}$ med $d \in \mathbb{N}$, da finder man først q_1 så at $0 \leq a - dq_1 < a$. Hvis $a - dq_1 < d$ er vi færdige. Ellers findes q_2 så at $0 \leq (a - dq_1) - dq_2 < a - dq_1$. Hvis $a - dq_1 - dq_2 < d$ er vi færdige, osv. I praksis udnyttes ti-talssytemet til at finde gode "gæt" til q_1, q_2, osv., ved at kigge på det mest betydende ciffer i a, $a - q_1 d$, osv.

EKSEMPEL. Find resten af 3551 ved division med 27.

Løsning. I første forsøg tager vi $q_1 = 100$, og får $3551 - 27 \cdot 100 = 851$. Så tager vi $q_2 = 30$ og får $851 - 27 \cdot 30 = 851 - 810 = 41$. Endelig får vi $41 - 27 \cdot 1 = 14 < 27$ og er færdige[4] , for nu er

$$3551 = 27 \cdot (100 + 30 + 1) + 14 = 27 \cdot 131 + 14.$$

Entydigheden i division med rest sætningen sikrer nu at resten ved division af 3551 med 27 er 14.

[4] Da jeg gik i skole lærte man at skrive udregningen i et skema som følger:

$$\begin{aligned} 3551 &: 27 \\ -100 \cdot 27 = \underline{-2700} & \\ 851 & \\ -30 \cdot 27 = \underline{-810} & \\ 41 & \\ -1 \cdot 27 = \underline{-27} & \\ 14 & \end{aligned}$$

På den sidste linje står resten. Man kan finde kvotienten ved at ligge tallene foran 27 sammen og skifte fortegn. (Min matematiklærer i skolen kunne ikke svare på hvorfor man skulle skifte fortegn. Sådan "var det bare" — suk!)

Opgave 4.1.3 *Lad $a, d \in \mathbb{N}$, $d > 1$. En* base d repræsentation *af a er et udtryk på formen*

$$a = a_0 d^0 + a_1 d^1 + a_2 d^2 \cdots + a_n d^n$$

hvor $a_0, \ldots, a_n \in \mathbb{N}_0$ og $0 \leq a_i < d$ for alle $i \leq n$, og $a_n \neq 0$. (Bemærk: $d^0 = 1$.)

(a) Find base 10 repræsentationen af tallene 84 og 127.

(b) Find base 2 repræsentationen af tallene 84 og 127. (Hvis man sidder helt fast, så er hintet til (c) nedenfor faktisk også et hint til (b), særligt det med den "største potens", her af $d = 2$.)

(c) Lad $d > 1$ været givet. Vis at ethvert tal $a \in \mathbb{N}$ har en entydig base d repræsentation.

Hint til (c): Du skal både vise eksistens og entydighed. Fuldstændig induktion eller velordningsprincippet er velegnede. Eksistensdelen kan eventuelt gribes an efter følgende skitse: Givet a, lad $n \in \mathbb{N}_0$ være den største potens af d sådan at $d^n \leq a$. Brug division med rest sætningen på a og d^n, og brug din induktionsantagelse (eller minimalitetsantagelse) på resten.

4.2 Største fælles divisor og Euclids algoritme

Definition 4.2.1 *Lad $a, b \in \mathbb{Z}$.*

1. *Hvis $d|a$ og $d|b$ da kaldes d en* **fællles divisor** *for a og b.*
2. *Hvis $a \neq 0$ eller $b \neq 0$, da har a eller b kun endeligt mange divisorer, og derfor har a og b en* **største fælles divisor**, *som vi betegner enten (a,b) eller $\mathrm{sfd}(a,b)$. Hvis $a = b = 0$ er $\mathrm{sfd}(a,b)$ ikke defineret.*
3. *Tallene a og b kaldes* **indbyrdes primiske** *hvis $\mathrm{sfd}(a,b) = 1$.*

Øvelse 9 *Lad $a, b \in \mathbb{Z}$ og antag at de ikke begge er lig 0. Vis:*

1. $\mathrm{sfd}(|a|,|b|) = \mathrm{sfd}(a,b)$*;*
2. *hvis $a \neq 0 \neq b$ da er $\mathrm{sfd}(a,b) \leq \min\{|a|,|b|\}$;*
3. *hvis $b = 0$ da er $\mathrm{sfd}(a,b) = |a|$.*

Euclids algoritme er en metode til at bestemme $\mathrm{sfd}(a,b)$. Idéen til algoritmen kommer fra følgende lemma.

Lemma 4.2.2 *Lad $a, b, q, r \in \mathbb{Z}$, $b \neq 0$, og antag at $a = bq + r$. Da er*

$$\mathrm{sfd}(a,b) = \mathrm{sfd}(b,r).$$

Bevis. Det er narturligvis nok at vise at enhver fælles divisor for a og b også er divisor i r, og at enhver fælles divisor for b og r er en divisor i a. (Overvej!)

Antag derfor at d er divisor i både a og b, og find $m, m' \in \mathbb{Z}$ så at $a = dm$ og $b = dm'$. Da $a = bq + r$ har vi

$$r = a - bq = dm - dm'q = d(m - m'q),$$

hvilket viser at d er divisor i r.

På lignende vis ses at enhver fælles divisor for b og r er divisor i a; detaljerne overlades til læseren, se næste øvelse. □

Øvelse 10 *Færdiggør det foregående bevis ved at vise at hvis d er en fælles divisor for b og r da er d divisor i a.*

Euclids algoritme. Lad $a, b \in \mathbb{N}$ og antag at $b < a$. Ved rekursion definerer vi nu en følge $a_0, a_1, a_2, \ldots$. Sæt $a_0 = a$ og $a_1 = b$, og definér derfra a_{i+2}, hvor $i \in \mathbb{N}_0$, ved:

- Hvis $a_{i+1} = 0$ da er $a_{i+2} = 0$.
- Hvis $a_{i+1} \neq 0$ da er a_{i+2} resten af a_i ved division med a_{i+1}.

Sætning 4.2.3 *Lad $a, b \in \mathbb{N}$, $b < a$, og lad $(a_i)_{i \in \mathbb{N}_0}$ være defineret som ovenfor.*

1. *Der gælder at* $a_i \leq \max\{0, a_0 - i\}$*, og derfor findes* $2 \leq i \leq a_0$ *sådan at* $a_i = 0$.

2. *Hvis* i *er mindst sådan at* $a_i = 0$ *da er* $\text{sfd}(a,b) = a_{i-1}$.

Følgen $(a_i)_{i\in\mathbb{N}}$ kan udregnes konkret for konkrete a og b ved at bruge den rekursive definition. Definitionen er i den forstand en algoritme. Derved kan man bestemme $\text{sfd}(a,b)$ i konkrete tilfælde, hvilket vi nu giver et eksempel på. Inden vi beviser sætningen giver vi eksempel på konkret brug af Euclids algoritme.

EKSEMPEL PÅ BRUG AF EUCLIDS ALGORITME.

Bestem $\text{sfd}(885, 375)$.

Løsning. Lad $a_0 = 885$ og $a_1 = 375$ i Euclids algoritme. Divideres a_0 med a_1 med rest fås $885 = 2 \cdot 375 + 135$, så $a_2 = 135$. Divideres a_1 med a_2 med rest fås $375 = 135 \cdot 2 + 105$, så $a_3 = 105$. Divideres a_2 med a_3 med rest fås $135 = 105 \cdot 1 + 30$, så $a_4 = 30$. Divideres a_3 med a_4 med rest fås $105 = 30 \cdot 3 + 15$, så $a_5 = 15$. Divideres a_4 med a_5 med rest fås $30 = 15 \cdot 2 + 0$. Derfor er $a_6 = 0$. Sætning 4.2.3 giver nu at $\text{sfd}(885, 375) = a_5 = 15$.

Bevis for sætning 4.2.3. (1) Vi beviser ved induktion[5] at $a_i \leq \max\{0, a_0 - i\}$. For $i = 0$ er dette klart, og for $i = 1$ følger det fra at $a_1 = b < a = a_0$.

Antag derfor at uligheden er bevist for $i \geq 1$, og betragt a_{i+1}. Hvis $a_{i+1} = 0$ er der intet at bevise, så antag $a_{i+1} \neq 0$. Da er a_{i+1} resten af a_{i-1} ved division med a_i, så $a_{i+1} < a_i$. Fra induktionsantagelsen følger så at

$$a_{i+1} < a_i \leq a_0 - i.$$

Derfor gælder at $a_{i+1} \leq a_0 - (i+1)$ (overvej!), hvilket viser induktionstrinnet.

(2) Vi starter med at bevise følgende:

Påstand: Hvis $a_i \neq 0$ da er $\text{sfd}(a_i, a_{i+1}) = \text{sfd}(a,b)$.

Bevis for påstanden: Ved induktion efter $i \in \mathbb{N}_0$. For $i = 0$ er der intet at vise. For at vise induktionstrinnet, antag at udsagnet holder for i, og antag at $a_{i+1} \neq 0$. Da er a_{i+2} resten af a_i ved division med a_{i+1}. Ifølge Lemma 4.2.2 gælder da $\text{sfd}(a_{i+1}, a_{i+2}) = \text{sfd}(a_i, a_{i+1})$, og induktionsantagelsen giver så $\text{sfd}(a_{i+1}, a_{i+2}) = \text{sfd}(a,b)$, som ønsket. Dette afslutter beviset for påstanden.

Det følger fra påstanden at hvis i er mindst sådan at $a_i = 0$, da er $\text{sfd}(a_{i-1}, a_i) = \text{sfd}(a,b)$. Men da $a_i = 0$ er $\text{sfd}(a_{i-1}, a_i) = a_{i-1}$. Derfor er $a_{i-1} = \text{sfd}(a,b)$, som ønsket. □

[5] Idet følgen $(a_i)_{i\in\mathbb{N}_0}$ er defineret ved rekursion vil næsten ethvert bevis for en fundamental egenskab ved følgen ske ved induktion. Det er en god regel at huske at definitioner ved rekursion giver anledning til beviser ved induktion.

Bezouts Lemma

Vi runder dette afsnit af med at vise følgende nyttige resultat:

Sætning 4.2.4 ("Bezouts Lemma") *Lad $a, b \in \mathbb{Z}$, og antag at enten $a \neq 0$ eller $b \neq 0$. Da findes hele tal $x, y \in \mathbb{Z}$ sådan at*

$$\mathrm{sfd}(a, b) = xa + yb.$$

Idéen til beviset for sætning 4.2.4 kommer fra følgende lemma, som når lagene skræles bort egentlig blot er en simpel udregning.

Lemma 4.2.5 *Lad $a, b \in \mathbb{N}$ hvor $a > b$, og lad $a = qb + r$, $0 \leq r < b$ være resultatet af division med rest af a med b. Antag at $z, w \in \mathbb{Z}$ er sådan at $\mathrm{sfd}(b, r) = zb + wr$, og lad $x = w$ og $y = z - qw$. Da er*

$$\mathrm{sfd}(a, b) = xa + yb.$$

Bevis. Fra Lemma 4.2.2 har vi $\mathrm{sfd}(a, b) = \mathrm{sfd}(b, r)$. Da $r = a - qb$ gælder derfor

$$\begin{aligned}\mathrm{sfd}(a, b) = \mathrm{sfd}(b, r) &= zb + wr = zb + w(a - qb) \\ &= wa + (z - qw)b = xa + yb,\end{aligned}$$

som ønsket. □

Bevis for sætning 4.2.4. Vi beviser sætningen i tilfældet hvor $a > b > 0$. De andre tilfælde skal læseren selv redegøre for i øvelsen nedenfor.

Beviset føres ved modstrid: Hvis ikke sætningen er sand, så findes der ifølge velordningsprincippet et mindste $a > 0$ sådan at der findes $0 < b < a$ sådan at *ingen* $x, y \in \mathbb{Z}$ opfylder

$$\mathrm{sfd}(a, b) = xa + yb.$$

Ved division med rest kan vi skrive $a = bq + r$, hvor $0 \leq r < b$. Da $b < a$ findes der $z, w \in \mathbb{Z}$ sådan at $\mathrm{sfd}(b, r) = zb + wr$. Men nu følger fra Lemma 4.2.5 at der findes $x, y \in \mathbb{Z}$ så at $\mathrm{sfd}(a, b) = xa + yb$, hvilket er en modstrid. □

Bemærkning. Foregående bevis er et eksempel på at velordningsprincippet nogen gange giver et lidt mere strømlinet bevis end induktion ville gøre. Læseren opmuntres dog til at lave følgende øvelse og omformulere foregående bevis til et bevis ved fuldstændig induktion.

Øvelse 11 *Brug fuldstændig induktion (i stedet for velordningsprincippet) til at bevise Sætning 4.2.4 i tilfældet $a > b > 0$.*

Øvelse 12 *Færdiggør beviset for Sætning 4.2.4 ved at redegøre for tilfældende 1) $a = 0$, 2) $b = 0$, 3) $a = \pm b$, og endelig 4) $a \neq \pm b$ og $a \neq 0$ og $b \neq 0$.*

Hint: Alle tilfældene er lette. I tilfælde 4 bør man udnytte at vi allerede ved at sætningen er sand for $a > b > 0$.

Øvelse 13 *Bevis følgende vigtige Korollar til Bezouts Lemma:*

Korollar 4.2.6 *Lad $a, b \in \mathbb{Z}$, som ikke begge er 0. Hvis d er en fælles divisor for a og b da gælder $d \mid \text{sfd}(a, b)$.*

EKSEMPEL PÅ BEZOUTS LEMMA I PRAKSIS: AT "REGNE BAGLÆNS" I EUCLIDS ALGORITME. Koefficienterne x, y i Bezouts lemma kan man i praksis finde ved at bruge Euclids algoritme "baglæns". Dette giver vi nu et eksempel på.

Problem: Bestem $x, y \in \mathbb{Z}$ sådan at $15 = x \cdot 885 + y \cdot 375$.

Løsning: Vi har allerede set i det foregående eksempel at $\text{sfd}(885, 375) = 15$, og derfor siger Bezouts lemma at de ønskede x og y findes.

Da vi brugte Euclids algoritme til at finde frem til at $\text{sfd}(885, 375) = 15$ lavede vi følgende udregninger (som alle er divisioner med rest):

$$\begin{aligned} 885 &= 2 \cdot 375 + 135 \\ 375 &= 2 \cdot 135 + 105 \\ 135 &= 1 \cdot 105 + 30 \\ 105 &= 3 \cdot 30 + 15. \end{aligned}$$

Lad os isolere resterne på højresiden:

$$\begin{aligned} 885 - 2 \cdot 375 &= 135 \\ 375 - 2 \cdot 135 &= 105 \\ 135 - 1 \cdot 105 &= 30 \\ 105 - 3 \cdot 30 &= 15. \end{aligned}$$

Ved at substituere den næstsidste linje i den sidste fås

$$15 = 105 - 3 \cdot (135 - 105) = 4 \cdot 105 - 3 \cdot 135.$$

Ved at bruge den 2. linje ovenfor (dvs. $375 - 2 \cdot 135 = 105$) i det foregående udtryk fås

$$15 = 4 \cdot (375 - 2 \cdot 135) - 3 \cdot 135 = 4 \cdot 375 - 11 \cdot 135.$$

Ved at substituere den 1. linje ovenfor (dvs. $885 - 2 \cdot 375 = 135$) i det foregående fås

$$15 = 4 \cdot 375 - 11 \cdot (885 - 2 \cdot 375) = -11 \cdot 885 + 26 \cdot 375.$$

Dermed er $x = -11$ og $y = 26$ som ønsket.

Bemærkning. Den kvikke læser vil sikkert bemærke at vi ved tilbageregning i Euclids algoritme slet ikke behøver at substituere og regne (helt så meget). Lemma 4.2.5 giver nemlig en eksplicit formel vi kan bruge til hver skridt baglæns. I det første baglæns skridt er $z = 1$, $w = -3$ og $q = 1$, så Lemma 4.2.5 giver $x = -3$ og $y = 1 - 1 \cdot (-3) = 4$. I næste baglæns skridt er $z = -3$, $w = 4$

og $q = 2$, hvilket giver $x = 4$ og $y = -3 - 2 \cdot 4 = 11$. I næste trin er $z = 4$, $w = -11$ og $q = 2$ hvilket giver $x = -11$ og $y = 4 - 2 \cdot (-11) = 26$. Dermed er tilbageregningen færdig og vi har derfor at $15 = -11 \cdot 885 + 26 \cdot 375$.

Bemærkning. Den læser, der er interesseret i at kigge nærmere på tilbageregning i Euclids algoritme i relation til Bezouts Lemma kan lave Opgave* nedenfor, hvor man giver et alternativt bevis for Bezouts Lemma som udnytter idéen om tilbageregning (via Lemma 4.2.5).

Øvelse 14 *Lad $a, b \in \mathbb{Z}$, hvor $a \neq 0$ eller $b \neq 0$. Antag at*

$$m = xa + yb.$$

Vis at $\mathrm{sfd}(a,b)|m$. *Konkludér at* sfd *er det mindste positive tal der kan skrives som en $\mathbb{Z}$-kombination af a og b.*

Øvelse 15 *Lad $a, b \in \mathbb{Z}$, hvor $a \neq 0$ eller $b \neq 0$, og antag at d er en fælles divisor for a og b. Da er* $\mathrm{sfd}(a,b) = d \cdot \mathrm{sfd}(\frac{a}{d}, \frac{b}{d})$.

Hint: Brug Bezouts Lemma og de to (!) foregående øvelser til at vise både "$\leq$" og "$\geq$".

Bemærkning: Foregående opgave kan nogen gange spare os for lidt arbejde ved at vi på forhånd fjerner oplagte fælles divisorer inden vi går videre med Euclids algoritme. F. eks. er det oplagt at 5 er en fælles divisor i 885 og 375 (idet de ender på 5), og at $885 = 5 \cdot 177$ og $375 = 5 \cdot 75$. Begynder vi på Euclids algoritme på 177 og 75 fås $177 = 2 \cdot 75 + 27$. Det er nu oplagt at 3 er en fælles divisor i 75 og 27, så vi kan nøjes med finde sfd for $25 = 75/3$ og $9 = 27/3$, men det er oplagt 1. Derfor er

$$\begin{aligned}\mathrm{sfd}(885,375) &= 5 \cdot \mathrm{sfd}(177,75) = 5 \cdot \mathrm{sfd}(75,27) \\ &= 5 \cdot 3 \cdot \mathrm{sfd}(25,9) = 5 \cdot 3 \cdot 1 = 15.\end{aligned}$$

(Første $=$ skyldes Øvelse 15, anden $=$ skyldes Euclids algoritme (mere præcist Lemma 4.2.2), og tredie $=$ bruger Øvelse 15 igen.)

Opgave*. I denne opgave giver vi et bevis for Bezouts Lemma der udnytter Euclids algoritme. Vi antager $a > b > 0$, idet Øvelse 12 redegør for de andre tilfælde.

Lad $a_0, a_1, a_2, \ldots$ være følgen som Euclids algoritme giver når $a_0 = a$ og $a_1 = b$. Lad q_i, for $i \geq 1$, være sådan at $a_{i-1} = q_i a_i + a_{i+1}$.

Lad $i \geq 2$ være størst så at $a_i \neq 0$. Definér rekursivt for $0 \leq j < i$ at $x_{i-0} = 1$, $y_{i-0} = 0$, og $x_{i-(j+1)} = y_{i-j}$ og

$$y_{i-(j+1)} = x_{i-j} - q_{i-j} y_{i-j}.$$

Vis, f.eks. ved induktion efter $0 \leq j \leq i$, at

$$\mathrm{sfd}(a_{i-j}, a_{i+1-j}) = x_{i-j} a_{i-j} + y_{i-j} a_{i+1-j}.$$

(Hint: Udnyt Lemma 4.2.5). Brug ovenstående med $j = i$ til at konkludere at

$$\mathrm{sfd}(a, b) = x_0 a + y_0 b,$$

og dermed at $x_0, y_0 \in \mathbb{Z}$ er som ønsket i Bezouts Lemma.

Bemærkning. Foregående bevis for Bezouts Lemma udnytter præcis idéen om at "regne baglæns" i Euclids algoritme. Koefficienterne x_{i-j}, y_{i-j} som vi definerer rekursivt i beviset er præcis de koefficienter vi finder i praksis når vi "regner baglæns".

4.3 Primtal

Tallene 4 og 6 kan skrives som et produkt af mindre tal, nemlig hhv. $2 \cdot 2$ og $2 \cdot 3$, men tallene $2, 3, 5, 7$ kan ikke — de er i den forstand "udelelige", en slags atomer i aritmetikken. Sådanne "udelelige" tal kaldes primtal, og defineres officielt som følger:

Definition 4.3.1 *1) Et naturligt tal $p \in \mathbb{N}$ kaldes et* **primtal** *hvis p har præcis to positive divisorer,* 1 *og* $p \neq 1$.

2) Et naturligt tal der har flere end to positive divisorer kaldes et **sammensat tal**.

Bemærk at tallet 1 hverken er et primtal eller et sammensat tal, det har nemlig *præcis en* positiv divisor. Bemærk at hvis $a > 1$ ikke er et primtal, da er det et sammensat tal.

Læseren kan hurtigt overbevise sig selv om at de første 10 primtal er

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$$

Nedenfor beviser vi at der findes uendeligt mange primtal. I det efterfølgende afsnit viser vi et hovedresultat, *aritmetikkens fundamentalsætning*, som siger at ethvert naturligt tal entydigt kan repræsenteres som et produkt at primtal.

Øvelse 16 *Vis at* 2 *er det eneste lige primtal.*

Proposition 4.3.2 *Lad p være et primtal og $a \in \mathbb{Z}$. Vis at hvis $p \not| a$ da er p og a indbyrdes primiske, dvs.* $\mathrm{sfd}(a, p) = 1$.

Øvelse 17 *Bevis foregående proposition.*

Øvelse 18 *Bevis følgende karakterisinger af hhv. primtal og sammensatte tal*

(a) Et naturligt tal p er et primtal hvis og kun hvis $p \geq 2$ og de eneste divisorer i p er de trivielle.

(b) Et naturligt tal n er et sammensat tal hvis og kun hvis $n \geq 4$ og der findes $a, b \in \mathbb{N}$ sådan at $1 < a, b < n$ og $n = ab$.

Uendeligt mange primtal

Hvis $d|a$ og d er et primtal, da kalder vi d en *primdivisor* i a.

Lemma 4.3.3 *Ethvert naturligt tal $a > 1$ har en primdivisor.*

Bevis. Hvis ikke, så findes der et *mindste* $a > 1$ sådan at a ikke har nogen primdivisorer. Så kan a ikke være et primtal, og derfor er a et sammensat tal, dvs. vi kan skrive a som $a = bc$, hvor $1 \leq b, c < a$. Minimaliteten af a medfører at b (og c) har en primdivisor p. Men da $b|a$ følger fra $p|b$ at $p|a$, hvilket viser at a har en primdivisor. Modstrid. □

Sætning 4.3.4 *Der findes uendeligt mange primtal.*

Bevis. Antag for en modstrid at der findes præcis n primtal som vi lister: $p_1, \ldots, p_n$. Betragt tallet

$$a = p_1 \cdots p_n + 1.$$

Bemærk at a og $p_1 \cdots p_n$ er indbyrdes primiske. (Dette følger fra at $1 = a - p_1 \cdots p_n$, og derfor er enhver fælles divisor for a og $p_1 \cdots p_n$ en divisor i 1.)

Ifølge foregående lemma har a en primdivisor, p. Da $p_1, \ldots, p_n$ lister alle primtal gælder at $p = p_i$ for et $i \leq n$. Derfor er p en fælles divisor for a og $p_1 \cdots p_n$, i modstrid med at disse to tal er indbyrdes primiske. □

4.4 Aritmetikkens fundamentalsætning

Definition 4.4.1 *Lad $a \in \mathbb{N}$. En* **primopløsning**[6] *af a er et produkt*

$$a = p_1^{n_1} \cdots p_k^{n_k}$$

hvor $p_1 < \cdots < p_k$ er en strengt voksende følge af $k \geq 0$ primtal, og $n_1, \ldots, n_k \in \mathbb{N}$.[7]

[6] En primopløsning kaldes også en *primfaktorisering* (engelsk: *prime factorization*).

[7] I det lidt sære tilfælde hvor $k = 0$, dvs. hvor vi tager produktet af *ingen* tal, vedtager vi at produktet er $= 1$. Med andre ord: 1 er (definitionsmæssigt) et produkt af nul faktorer.

EKSEMPLER PÅ PRIMOPLØSNINGER.

$$\begin{aligned}
4 &= 2^2 \\
6 &= 2^1 \cdot 3^1 = 2 \cdot 3 \\
7 &= 7^1 \\
12 &= 2^2 \cdot 3^1 = 2^2 \cdot 3 \\
29 &= 29^1 \\
56 &= 2^3 \cdot 7^1 = 2^3 \cdot 7 \\
3960 &= 2^3 \cdot 3^2 \cdot 5^1 \cdot 11^1 = 2^3 \cdot 3^2 \cdot 5 \cdot 11.
\end{aligned}$$

Følgende er et hovedresultat i elementær talteori.

Sætning 4.4.2 (Aritmetikkens fundamentalsætning) *Ethvert naturligt tal har en entydig primopløsning.*

I denne sætning er eksistensdelen (noget usædvanligt) ret nem at bevise, mens entydighedsdelen kræver mere arbejde. Derfor viser vi først eksistensen af primopløsninger, og derefter arbejder vi os igennem entydighedsproblemet.

Bevis for eksistens af primopløsning i sætning 4.4.2.

Vi bruger velordningsprincippet: Hvis der er et naturligt tal, der ikke har en primopløsning, så findes et mindste sådant tal, $n \in \mathbb{N}$. Bemærk at $n > 1$, idet 1 pr definition har en (degeneret og triviel) primopløsning.

Da $n > 1$ har n en primdivisor. Lad p være den mindste sådanne primdivisor. Skriv $n = pq$ for et $q \in \mathbb{N}$. Der må gælde at $q \neq 1$, for ellers er $n = p^1$, i modstrid med at n ikke har en primopløsning.

Da $1 < q < n$ har q en primopløsning, $q = q_1^{n_1} \cdots q_k^{n_k}$ hvor $k \geq 1$. Da p er den mindste primdivisor i n er $p \leq q_1$. Hvis $p < q_1$ er

$$n = p^1 q_1^{n_1} \cdots q_k^{n_k}$$

en primopløsning af n, og hvis $p = q_1$ da er

$$n = q_1^{n_1+1} \cdots q_k^{n_k}$$

en primopløsning af n. I alle tilfælde har vi vist at n har en primopløsning, i modstrid med at n var det mindste tal uden en primopløsning. □

Øvelse 19 *Giv et bevis for eksistensen af primopløsninger ved at bruge fuldstændig induktion i stedet for velordningsprincippet.*

ANALYSE AF ENTYDIGHEDSPROBLEMET I SÆTNING 4.4.2.

Det bevis for Aritmetikkens Fundamentalsætning, som jeg i den første version af noterne havde skrevet, fandt jeg i løbet af forelæsningen ud af var unødvendigt kompliceret. Derfor har jeg skrevet et nyt bevis, som er simplere. Det ligger også tættere op ad beviset som Lützen giver i DMM.

Før vi kaster os ud i at bevise de forskellige lemmaer osv. der er brug for til entydighedsdelen af aritmetikkens fundamentalsætning, så lad os klargøre hvad problemet er.

Hvis n er et tal der har to primopløsninger

$$n = p_1^{n_1} \cdots p_k^{n_k} = q_1^{m_1} \cdots q_l^{m_l},$$

da er vores mål at vis at $k = l$, og $p_1 = q_1, \ldots, p_k = q_k$, og $n_1 = m_1, \ldots, n_k = m_k$.

Det er klart at hvis n har to primopløsninger som ovenfor, da er ethvert p_i er primdivisor i n og derfor i produktet $q_1^{m_1} \cdots q_l^{m_l}$, og ethvert q_i er divisor i n og derfor i produktet $p_1^{n_1} \cdots p_k^{n_k}$.

Hvis vi fra $p_i|(q_1^{m_1}\cdots q_l^{m_l})$ kunne slutte at $p_i|q_j^{m_j}$ for et $j \leq l$, da ville problemet *reduceres til at forstå hvilke primdivisorer primtalspotensen $q_j^{m_j}$ har*, hvilket virker overskueligt. Sagt på en lidt anden måde: Vi må først koncentrere os om at forstå tilfældet hvor $k = l = 1$, altså hvor $p_1^{n_1} = q_1^{m_1}$. Til dette formål beviser vi følgende lemma:

Lemma 4.4.3 *Lad $d, p, q \in \mathbb{N}$. Antag at p og q er et primtal og at $p|q^n$. Da er $p = q$.*

Når dette lemma er bevist vender vi tilbage til problemet at forstå hvad der sker når et primtal går op i et produkt af potenser af (forskellige) primtal. Følgende lemma siger, at det går som vi havde håbet: Hvis et primtal går op i en primopløsning, så går den op i en af faktorerne. Den præcise formulering er:

Lemma 4.4.4 *Lad $n, m, p \in \mathbb{N}$, $n > 1$, p et primtal. Antag at*

$$n = q_1^{n_1}\cdots q_k^{n_k}$$

er en primopløsning af n, og at $p|n$. Da er $p = q_i$ for et $i \leq k$.

Specielt gælder at hvis n har en primopløsning som ovenfor, da er q_1 den mindste primdivisor i n.

Entydighedsbeviset i detaljer

Udgangspunktet for Lemma 4.4.3 og 4.4.4 er følgende konsekvens af Bezouts Lemma.

Proposition 4.4.5 *Lad $n, a, b \in \mathbb{Z}$, og antag at n og a er indbyrdes primiske. Hvis $n|ab$, da gælder $n|b$.*

Bevis. Lad $q \in \mathbb{Z}$ så at $ab = qn$. Da n og a er indbyrdes primiske findes ifølge Bezouts lemma $x, y \in \mathbb{Z}$ sådan at $1 = xn + ya$. Ganges ligningen med b fås

$$b = xnb + yab = xbn + yqn = (xb + yq)n,$$

hvorfra det ses at $n|b$. □

Korollar 4.4.6 ("Det lille primtalslemma") *Lad p være et primtal, $a, b \in \mathbb{Z}$. Antag $p|ab$. Da gælder $p|a$ eller $p|b$.*

Bevis. Antag at $p|ab$. Hvis $p|a$ er der intet at vise. Antag derfor at p ikke er divisor i a. Da p er et primtal følger da at $\mathrm{sfd}(p, a) = 1$ (overvej nøje!). Fra foregående proposition følger at nu at $p|b$. □

Øvelse 20 *Bevis følgende mere generelle version af det lille primtalslemma: Hvis p er et primtal og $p|a_1\cdots a_k$, hvor $a_1, \ldots, a_k \in \mathbb{Z}$ og $k \geq 2$, da findes $i \leq k$ sådan at $p|a_i$.*

Med dette Korollar følger Lemma 4.4.3 let.

Bevis for Lemma 4.4.3. Lad primtal p og q være givet. Lad $P(n)$ være følgende prædikat (hvor variablen n går over de naturlige tal):

$$P(n) : \textit{Hvis } p|q^n \textit{ så er } p = q.$$

Vi beviser at $P(n)$ er sand for alle n ved induktion efter n.

Basistrin: Hvis $n = 1$, da siger $P(1)$ blot at hvis $p|q$, da er $p = q$. Dette følger direkte fra at q er et primtal.

Induktionstrin: Antag at $P(n)$ er sand. Vi skal vise at $P(n+1)$ er sand. Antag derfor at $p|q^{n+1}$. Da gælder at $p|q \cdot q^n$, og fra det lille primtalslemma følger at $p|q$ eller $p|q^n$. I det første tilfælde følger $p = q$ præcis som i basistrinnet. I det andet tilfælde giver induktionsantagelsen at $p = q$. □

Øvelse 21 *1) Vis følgende generalisering af Lemma 4.4.3: Hvis q er et primtal og $d, n \in \mathbb{N}$, og $d|q^n$, da er $d = q^m$ for et $0 \leq m \leq n$.*

Med andre ord: Mængden af positive divisorer i primtalspotensen q^n er præcis

$$\{1, q, q^2, \ldots, q^n\}.$$

2) Brug 1) til at vise, at hvis $p \neq q$ er primtal og $m, n \in \mathbb{N}$, da er p^m og q^n indbyrdes primiske.

Hint*: I 1) kan man bruge induktion efter n og Proposition 4.4.5. Man kan vise 2) ved f.eks. at kombinere 1) med Lemma 4.4.3.*

Bevis for Lemma 4.4.4. Lad $P(k)$ være følgende prædikat:

$$P(k)\text{: } \textit{Hvis } n = q_1^{n_1} \cdots q_k^{n_k} \textit{ er en primopløsning af } n \textit{ med } k \textit{ primtal, og } p|n, \textit{ da er } p = q_i \textit{ for et } 1 \leq i \leq k.$$

Vi beviser at $P(k)$ er sand ved induktion efter k, dvs. antallet af forskellige primtal i opløsningen.

Basistrin: Hvis $k = 1$, da er $n = q_1^{n_1}$. Hvis $p|n$ da følger fra direkte Lemma 4.4.3 at $p = q_1$ (overvej).

Induktionstrin: Antag at $P(k)$ er sand, og antag at

$$p|(q_1^{n_1} \cdots q_k^{n_k} q_{k+1}^{n_{k+1}})$$

hvor $q_1 < \cdots < q_{k+1}$ er primtal og $n_1, \ldots, n_k, n_{k+1} \in \mathbb{N}$. Fra det lille primtalslemma følger at $p|q_1^{n_1} \cdots q_k^{n_k}$ eller $p|q_{k+1}^{n_{k+1}}$ (overvej). I det første tilfælde giver induktionsantagelsen at $p = q_i$ for et $1 \leq i \leq k$. I det andet tilfælde giver Lemma 4.4.3 at $p = q_{k+1}$ (overvej). I alle tilfælde fås at der findes $1 \leq i \leq k+1$ så at $p = q_i$. Dette afslutter induktionstrinnet.

Princippet om simpel induktion giver nu at $P(n)$ er sand for alle $n \in \mathbb{N}$.

Bermærk at hvis $n = q_1^{n_1} \cdots q_k^{n_k}$ og p er et primtal sådan at $p|n$, da er $p \geq q_1$, idet vi ovenfor jo beviste at der må gælde at $p = q_i$ for et $1 \leq i \leq n$, og definitionen af primopløsning kræver at $q_1 \leq q_i$ for alle $1 \leq i \leq k$. Specielt følger at q_1 den mindste primdivisor i n når $n = q_1^{n_1} \cdots q_k^{n_k}$ er en primopløsning af n. □

Bevis for entydighedsdelen af Sætning 4.4.2. Lad $P(n)$ være prædikatet defineret som følger:

$P(n)$: *Hvis*

$$n = p_1^{n_1} \cdots p_k^{n_k} = q_1^{m_1} \cdots q_l^{m_l},$$

er to primopløsninger af n, da er $k = l$, *og* $p_1 = q_1, \ldots, p_k = q_k$, *og* $n_1 = m_1, \ldots, n_k = m_k$.

Vi viser ved fuldstændig induktion at $P(n)$ er sandt for alle n.

Basistrin: Vi har vedtaget at $n = 1$ har det "tomme produkt' som primopløsning. Derfor er $P(1)$ sand pr. definition.

Induktionstrin: Antag at $P(1), \ldots, P(n)$ er sand. Vi skal vise at $P(n+1)$ er sand. Antag derfor at

$$n+1 = p_1^{n_1} \cdots p_k^{n_k} = q_1^{m_1} \cdots q_l^{m_l}.$$

Fra "specielt" i Lemma 4.4.4 følger at p_1 er den mindste primdivisor i $n+1$, og ligeledes at q_1 er den mindst primdivisor i $n+1$. Derfor er $p_1 = q_1$.

Vi påstår at $n_1 = m_1$. Hvis ikke, da er enten $n_1 < m_1$ eller $m_1 < n_1$. Er $n_1 < m_1$ tilfældet, da er $(n+1)/p_1^{n_1} \in \mathbb{N}$, og

$$\frac{n+1}{p_1^{n_1}} = p_2^{n_2} \cdots p_k^{n_k} = q_1^{m_1 - n_1} q_2^{m_2} \cdots q_l^{m_l}.$$

Det følger så af "specielt' delen af Lemma 4.4.4 at p_2 er den mindste primdivisor i $(n+1)/p_1^{n_1}$, og ligeledes at q_1 er den mindste primdivisor i $(n+1)/p_1^{n_1}$. Derfor er $p_2 = q_1$, i modstrid med at $q_1 = p_1 < p_2$. I tilfældet $n_1 < m_1$ opnås en modstrid på lignende måde. Derfor har vi vist at $n_1 = m_1$.

Det følger nu at

$$\frac{n+1}{p_1^{n_1}} = p_2^{n_2} \cdots p_k^{n_k} = q_2^{m_2} \cdots q_l^{m_l}.$$

Da $(n+1)/p_1^{n_1} < n$ og $(n+1)/p_1^{n_1} \in \mathbb{N}$ giver induktionsantagelsen at $k = l$, $p_2 = q_2, \ldots, p_k = q_k$ $(= q_l)$, og at $n_2 = m_2, \ldots, n_k = m_k$ $(= m_l)$. Da vi allerede har vist ovenfor at $p_1 = q_1$ og $n_1 = m_1$ har vi bevist at $P(n+1)$ er sand.

Det følger nu fra sætningen af fuldstændig induktion at $P(n)$ er sand for alle n. Dermed er det vist at ethvert naturligt tal har en entydig primopløsning, dvs. Aritmetikkens Fundamentalsætning er bevist. □

BEMÆRKNING. Læseren spekulerer sikkert på om der er en algoritme, f.eks. á la Euclids algoritme, til at bestemme primdivisorerne og primopløsningen af et givet tal. **En sådan algoritme kendes ikke**, desværre, og man regner med at der ikke findes nogen sådan algoritme[8]. Faktisk er mange krypteringssystemer (f.eks. såkaldt *RSA kryptering*) bygget på at det er meget vanskeligt at finde primdivisorerne i et givet (stort) tal, også for en computer med stor regnekraft.

[8] Det er dog muligt at give en algoritme der i princippet kan implementeres på en såkaldt kvantecomputer. Kvantecomputere er dog endnu ikke en praktisk realitet.

Opgave 4.4.7 *Lad $d, n \in \mathbb{N}$ og lad $n = p_1^{n_1} \cdots p_k^{n_k}$ være primopløsningen af n. Vis at $d|n$ hvis og kun hvis*

$$d = p_1^{m_1} \cdots p_k^{m_k}$$

hvor $0 \leq m_1 \leq n_1, \ldots, 0 \leq m_k \leq n_k$.

Opgave 4.4.8 *1) Find primopløsningerne for tallene* 432 *og* 972.

2) Brug del 1 (og ikke Euclids algoritme) til at finde $\mathrm{sfd}(432, 972)$.

Opgave 4.4.9 *Vis at hvis a er et sammensat tal da har a en primdivisor p, hvorom der gælder at $p \leq \sqrt{a}$.*

Hint: Overvej hvad der sker hvis alle divisorer i a var større end $\sqrt{a}$.

BEMÆRKNING. Foregående opgave er en hjælp når man skal finde primdivisorer i et givet tal a. Den siger nemlig at man kan starte med at kigge på tallene $\leq \sqrt{a}$.

Opgave 4.4.10 *1) Om tallene* 51597 *og* 415233 *oplyses det, at de har de samme primdivisorer. Find deres primopløsninger.*

Hint: Start med at finde $\mathrm{sfd}(51597, 415233)$ *vha. Euclids algoritme. Hvis du er opmærksom på* al *information du får ud af Euclids algortime behøver du i sidste ende kun at finde primdivisorer i et to-cifret og et tre-cifret tal.*

4.5 Noter

Talteori er fortsat et meget aktivt emne inden for matematisk forskning, og nogle af matematikkens kendteste og sværeste problemer stammer fra talteori:

1. *Fermats sidste sætning*. Der findes ingen $a, b, c, n \in \mathbb{N}$ og $n > 2$ som er løsninger til ligningen

   $$a^n + b^n = c^n.$$

   Pierre de Fermat skrev i margin til et manuskript fra 1637 at han havde et bevis for dette, men at der ikke var plads til det i margin.

Ingen ved om Fermat faktisk havde et bevis, men i 1995 publicerede Andrew Wiles som den første i historien et bevis, der i dag anses for korrekt. Wiles bevis er uhyre langt og kompliceret, og anvender idéer der går langt udover elementær talteori, bl.a. moderne algebraisk geometri. Fermat kunne umuligt have fundet det samme bevis, men det er naturligvis en mulighed at han fandt et elementært bevis (jeg har svært ved at tro det).

Hvis $n = 2$ er der uendeligt mange heltalsløsninger til ligningen, bla. $3^2 + 4^2 = 5^2$. Sådanne løsninger kaldes *pythagoraiske tripler*.

2. *Goldbach's formodning*. Ethvert lige tal $n > 2$ er en sum af to primtal. Formodningen (fra 1742) er fortsat ikke bevist eller modbevist, og udgør stadig et aktivt forskningsområde.

3. *Mersenne primtal*. Et tal på formen $2^n - 1$ kaldes et Mersenne tal. Når n er et sammensat tal, så er $2^n - 1$ også sammensat, se øvelsen nedenfor. Mersenne bemærkede at

$$2^2 - 1 = 5, 2^3 - 1 = 7, 2^5 - 1 = 31, \text{ og } 2^7 - 1 = 127$$

er primtal. Dog er $2^{11} - 1 = 23 \cdot 89$, så det ikke alle Mersenne tal med primtalseksponent er primtal. Det vides fortsat ikke om der findes uendeligt mange Mersenne primtal. Det største kendte Mersenne primtal er $2^{74207281} - 1$.

4. *Collatz formodning*. Vælg $n_0 \in \mathbb{N}$ arbitrært. Definér rekursivt at

   - hvis n_i er lige da er $n_{i+1} = \frac{n_i}{2}$;
   - hvis n_i er ulige, lad $n_{i+1} = 3n_i + 1$.

   Collatz formodning (fremsat i 1937) siger at der findes $i \in \mathbb{N}$ sådan at $n_i = 1$ ligegyldig hvilket tal n_0 vi startede med.

   Problemet anses af eksperter for at være helt og aldeles uløseligt med vores tids matematik.

   En (løselig, men svær) opgave med lidt af samme smag som Collatz formodning findes nedenfor, se opgave **??**.

Advarsel: Moderne talteoretisk forskning har egentlig meget lidt at gøre med den klassiske, elementære talteori vi har set i dette kapitel. I dag er emnet splittet op i *analytisk talteori*, *algebraisk talteori*, *aritmetisk kombinatorik*, osv., og disse emner trækker på avancerede analytiske, algebraiske, geometriske og kombinatoriske metoder. Målet er fortsat at studere de hele tals struktur, men da elementære metoder tilsyneladende er udtømt har man tyet til at importere metoder fra andre områder at matematikken.

Øvelse 22 *Vis at hvis $n = ab$ så er $2^a - 1$ divisor i $2^n - 1$.*

Den følgende opgave er ment som en udfordring til dem der har tid og lyst til at prøve kræfter med den.

Opgave 4.5.1 (En udfordring!) *Husk fra Opgave 4.1.3 at, givet $d \in \mathbb{N}$ hvor $d > 1$, da kan ethvert $a \in \mathbb{N}$ skrives entydigt i en base d representation*

$$a = a_0 d^0 + a_1 d^1 + \cdots + a_n d^n,$$

hvor $a_0, \ldots, a_n \in \mathbb{N}_0$, og $0 \leq a_i < d$ for alle $i \leq n$, og $a_n \neq 0$.

Vi definerer først en funktion $C_{d,b}$, som vi ikke skal bruge, men vi skal bruge en mere avanceret version af den, kaldet $H_{d,b}$, så for forståelsens skyld inkluderer jeg definitionen på $C_{d,b}$. For $d, b > 1$, definer funktionen

$$C_{d,b}(a_0 d^0 + a_1 d^1 + \cdots + a_n d^n = a_0 b^0 + a_1 b^1 + \cdots + a_n b^n.$$

F. eks. er $C_{2,3}(6) = C_{2,3}(2^1 + 2^2) = 3^1 + 3^2 = 12$. Dvs., $C_{d,b}$ udskifter basetallet (dvs. d) med b. Vi kan kalde $C_{d,b}$ for d,b-basisudskifte operatoren.

Definer nu ved ved rekursion den hereditære basisudskifte operator *ved $H_{d,b}(0) = 0$, $H_{d,b}(1) = 1$, og*

$$H_{d,b}(a_0 d^0 + a_1 d^1 + \cdots + a_n d^n) = a_0 b^{H_{d,b}(0)} + a_1 b^{H_{d,b}(1)} + \cdots + a_n b^{H_{d,b}(n)}.$$

F. eks. er

$$H_{2,3}(6) = H_{2,3}(2^1 + 2^2) = 3^{H_{2,3}(1)} + 3^{H_{2,3}(2^1)} = 3^1 + 3^{3^{H_{2,3}(1)}} = 3^1 + 3^{(3^1)} = 27 + 3 = 30.$$

Lad nu a være givet. Følgen $n_1(a), n_2(a), \ldots$ defineres ved rekursion som følger: $n_1(a) = a$, og hvis $n_i(a) > 1$, da lader vi

$$n_{i+1}(a) = H_{i+1,i+2}(n_i(a) - 1).$$

Hvis $n_i(a) = 1$ da lader vi $n_{i+1}(a) = 1$.

F. eks. er

$$\begin{aligned}
n_1(5) &= 5 \\
n_2(5) &= H_{2,3}(2^0 + 2^2) - 1 = 3^0 + 3^{H_{2,3}(2)} - 1 = 1 + 3^3 - 1 = 9 \\
n_3(5) &= H_{3,4}(3^3) - 1 = 4^4 - 1 = 15 \\
n_4(5) &= H_{4,5}(15) - 1 = H_{4,5}(15 \cdot 4^0) - 1 = 15 \cdot 5^0 - 1 = 14 \\
n_5(5) &= H_{5,6}(14) - 1 = 14 \cdot 5^0 - 1 = 14 \cdot 6^0 - 1 = 13 \\
&\vdots
\end{aligned}$$

Det ses let herfra at $n_{17}(5) = 1$.

Bevis at for at for alle $a \in \mathbb{N}$ gælder, at følgen $(n_i(a))_{i \in \mathbb{N}}$ efter endeligt mange trin tager værdien 1. Sagt på en anden måde: Bevis at

$$(\forall a \in \mathbb{N})(\exists m \in \mathbb{N})(\forall i \geq m)\ n_i(a) = 1.$$

5
Regning med rester og modulær aritmetik

I dette kapitel introducerer vi først regning med rester, og derefter opbygger vi en matematisk struktur der formaliserer resternes aritmetik. Denne strukturdannelse kaldes "modulær aritmetik", eller "regning med rest*klasser*".

For den studerende i DIS er modulær aritmetik et første kig på nye aritmetiske strukturer, der ligger udover de velkendte tal som $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$.

5.1 Regning med rester

Regning med rester er en form for matematik der var kendt af stort alle de tidlige civilisationer (i Kina, Babylon, Egypten, Grækenland), idet det er den aritmetik der er brug for til tidsregning, f.eks. til at lave kalendere, osv. Vi starter med et motiverende eksempel.

EKSEMPEL. I dette eksempel betragter vi rester ved division med 7. Resten af 100 modulo 7 er 2, idet $100 = 14 \cdot 7 + 2$, og resten af 1000 er 6, idet $1000 = 142 \cdot 7 + 6$. Betragt nu $100 + 1000 = 1100$. Resten af 1100 med 7 er 1, som følgende udregning viser:

$$\begin{aligned} 1100 &= 100 + 1000 = (14 \cdot 7 + 2) + (142 \cdot 7 + 6) \\ &= 156 \cdot 7 + 8 = 157 \cdot 7 + 1. \end{aligned}$$

Bemærk, at før det sidste lighedstegn ovenfor optræder summen af resterne af 100 og 1000 ved division med 7, som er 8, og at resten af 8 ved division med 7 er 1, hvilket også er resten af 1100 ved division med 7.

Det, der sker i foregående eksempel, nemlig at resten af summen af resterne er lig med resten af summen, er ikke nogen tilfældighed, hvilket følgende sætning viser. Faktisk viser sætningen også at samme "trick" virker for multiplikation.

Sætning 5.1.1 *Lad $n \in \mathbb{N}$ være givet. Lad $a, b \in \mathbb{Z}$, og lad at $0 \leq r_0 < n$ og $0 \leq r_1 < n$ være resterne af a, hhv. b, ved division med n. Da gælder*

1) Resten af $a+b$ ved division med n er lig med resten af r_0+r_1 ved division med n.

2) Resten af $a \cdot b$ ved division med n er lig med resten af $r_0 \cdot r_1$ ved division med n.

Bevis. 1) Lad $q_0, q_1 \in \mathbb{Z}$ være sådan at $a = q_0 n + r_0$ og $b = q_1 n + r_1$. Lad $0 \leq r' < n$ være resten af $r_0 + r_1$ ved division med n, og find q' sådan at $r_0 + r_1 = q'n + r'$. Da gælder:

$$\begin{aligned} a+b &= (q_0 n + r_0) + (q_1 n + r_1) = (q_0+q_1)n + (r_0+r_1) \\ &= (q_0+q_1)n + (q'n + r') = (q_0+q_1+q')n + r'. \end{aligned}$$

Fra entydigheden af division med rest følger fra foregående udregning at r' er resten af $a+b$ ved division med n, som ønsket.

2) Beviset følger samme ide som 1), og overlades til læseren (se næste øvelse). □

Øvelse 23 *Bevis 2) i foregående sætning.*

Foregående sætning viser at resterne ved division med (et fastsat) n har en fornuftig aritmetisk struktur, i den forstand at man kan "regne" direkte med resterne, og komme frem til det korrekte resultat. I de følgende afsnit opbygger vi på mere formel vis denne aritmetiske struktur. Inden da tager vi dog lige et eksempel mere.

EKSEMPEL. Det oplyses at 1. januar 2018 var en mandag. Hvilken ugedag var 1. januar 2000?

Løsning: Der er 18 år mellem 2000 og 2018. Blandt disse 18 år er der 5 skudår med 366 dage. Altså er der gået

$$13 \cdot 365 + 5 \cdot 366$$

dage siden 1. januar 2000. Hvis vi forestiller os at vi dividerer (med rest) foregående med 7, da vil vi få[1]

$$-(13 \cdot 365 + 5 \cdot 366) = q \cdot 7 + r,$$

hvor $0 \leq r < 7$. Bemærk at i det foregående er q antallet af hele uger vi skal tilbage i tiden for at finde mandagen *før* 1. januar 2000. Derfor er r antallet af dage udover den mandag, der skal tillægges for at nå 1. januar 2000.

Man *kunne* nu give sig til at dividere 7 op i $-(13 \cdot 365 + 5 \cdot 366)$ og finde r. Det gør vi ikke. Vi bruger i stedet foregående sætning, og "regner med resterne".

Resten af 13, 365, 5 og 366 ved division med 7 er hhv. 6, 1, 5 og 2, så resten af $-(13 \cdot 365 + 5 \cdot 366)$ ved division med 7 er det samme som resten af $-(6 \cdot 1 + 5 \cdot 2) = -16$ ved division med 7. Resten af -16 ved division med 7 er 5. Derfor er $r = 5$ ovenfor, og derfor var 1. januar 2000 netop 5 dage efter den sidste mandag før denne dato. Derfor var 1. januar 2000 en lørdag.

(Bemærk at det aldrig var nødvendigt at finde q ovenfor. Det er netop fordelen ved regning med rester.)

[1] Minus fordi vi regner *tilbage* i tiden!

5.2 Restklasser modulo n

Definition 5.2.1 *Lad $n \in \mathbb{N}$ være givet, og lad $a \in \mathbb{Z}$. Mængden*

$$[a]_n = \{a + nq : q \in \mathbb{Z}\} = \{b \in \mathbb{Z} : (\exists q \in \mathbb{Z})\ b = a + nq\}$$

kaldes a's restklasse modulo *n*.

Bemærk at $a \in [a]_n$, idet $a = a + n0$. Specielt er $[a]_n \neq \emptyset$.

Lemma 5.2.2 *Lad $n \in \mathbb{N}$ være givet, og lad $a, b \in \mathbb{Z}$. Da er følgende udsagn ækvivalente:*

i) $b \in [a]_n$.

ii) a og b har samme rest ved division med n.

iii) $[b]_n = [a]_n$

Bevis: i) $\Longrightarrow$ ii): Antag $b \in [a]_n$, og lad r være resten af a ved division med n. Da findes $q, q' \in \mathbb{Z}$ sådan at $b = a + qn$ og $a = q'n + r$. Derfor er $b = q'n + r + qn = (q + q')n + r$, hvilket viser at b har rest r ved division med n.

ii) $\Longrightarrow$ i): Antag a og b begge har rest r ved division med n. Så findes $q, q' \in \mathbb{Z}$ sådan at $a = qn + r$ og $b = q'n + r$. Derfor er $b = q'n + (a - qn) = a + (q' - q)n$, hvilket viser at $b \in [a]_n$. $\square$.

ii) $\Longrightarrow$ iii): Antag a og b har samme rest ved division med n. Det følger fra ækvivalensen af i) og ii) at hvis $x \in [a]_n$ da har x og a har samme rest ved division med n. Derfor har x og b samme rest ved division med n. Da følger af ækvivalensen af i) og ii) at $x \in [b]_n$. Dette viser at $[a]_n \subseteq [b]_n$. Den modsatte inklusion, dvs. $[b]_n \subseteq [a]_n$, bevises på samme måde, *mutatis mutandis*.

iii) $\Longrightarrow$ i): Da $b \in [b]_n$ følger, at hvis $[a]_n = [b]_n$ da er $b \in [a]_n$.$\square$

Øvelse 24 *Med n, a og b som i foregående lemma, vis at*

iv) $a \in [b]_n$

er ækvivalent med i), ii) *og* iii).

Bemærkning. Man kalder ofte et element i en restklasse for en *repræsentant* for restklassen. Dette skyldes ækvivalensen af *i)* og *iii)* i foregående lemma, som fortæller os at hvis C er en restklasse modulo n og $b \in C$ er et vilkårligt element i C, da gælder $C = [b]_n$. Et vilkårligt $b \in C$ i restklassen C repræsenterer altså C som $[b]_n$.

Øvelse 25 *Lad $n \in \mathbb{N}$ og $a \in \mathbb{Z}$. Lad r være resten af a ved division med n. Vis at $[r]_n = [a]_n$. Med andre ord, resten af a ved division med n er en repræsentant for restklassen $[a]_n$.*

Korollar 5.2.3 *Lad $n \in \mathbb{N}$ og $a, b \in \mathbb{Z}$.*

(1) Hvis $[a]_n \cap [b]_n \neq \emptyset$ så er $[a]_n = [b]_n$. Med andre ord: Restklasserne modulo (et fast) n er enten disjunkte, eller også er de identiske.

(2) Der findes præcis n restklasser modulo n, svarende til de n mulige rester ved division med n, og de er præcis

$$[0]_n, [1]_n, \ldots, \text{ og } [n-1]_n.$$

(3) Der gælder at

$$\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n,$$

dvs. $\mathbb{Z}$ er foreningen af de n disjunkte restklasser modulo n.

Bemærkning. På grund af (1) og (3) i foregående siger vi at restklasserne udgør en *klassedeling* af $\mathbb{Z}$. Vi vender tilbage til begrebet klassedeling i fuld generalitet når vi senere i kurset kigger på begrebet *ækvivalensrelationer*.

Bevis for korollaret. (1) Antag at $[a]_n \cap [b]_n \neq \emptyset$, og lad $c \in [a]_n \cap [b]_n$. Fra foregående lemma følger så at

$$[a]_n = [c]_n = [b]_n,$$

som ønsket.

(2) Fra foregående øvelse følger at $[r]_n = [a]_n$ når r er resten af a ved division med n. Da $0, 1, \ldots, n-1$ er de mulige rester ved division med n følger at de mulige restklasser modulo n præcis er

$$[0]_n, [1]_n, \ldots, [n-1]_n,$$

som ønsket.

(3) Det er klart at $[0]_n \cup [1]_n \cup \cdots \cup [n-1]_n \subseteq \mathbb{Z}$, idet $[a]_n \subseteq \mathbb{Z}$ for alle $a \in \mathbb{Z}$. For den omvendte inklusion, lad $x \in \mathbb{Z}$ og lad $0 \leq r < n$ være resten af x ved division med n. Så er $[x]_n = [r]_n$ (pga. foregående øvelse!), specielt er $x \in [r]_n$. Derfor gælder

$$x \in [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n,$$

hvilket viser inklusionen $\mathbb{Z} \subseteq [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n$. □

5.3 Kongruens modulo n

Definition 5.3.1 *Lad $n \in \mathbb{N}$ og $a, b \in \mathbb{Z}$. Vi siger a og b er* kongruente modulo n *hvis $n|(a-b)$. Hvis a og b er kongruente modulo n da skriver[2] vi $a \equiv_n b$.*

[2] En mere gammeldags notation for $a \equiv_n b$ er $a \equiv b \pmod{n}$. Jeg er personligt ikke fan af den gammeldags notation!

Proposition 5.3.2 *Lad $n \in \mathbb{N}$ være et givet naturlig tal, og lad $a, b \in \mathbb{Z}$. Da er følgende udsagn ækvivalente:*

1) $a \equiv_n b$.
2) a og b har samme rest modulo n.
3) $a \in [b]_n$.
4) $b \in [a]_n$.
5) $[a]_n = [b]_n$

Bevis Vi har allerede i Lemma 5.2.2 (og den efterfølgende øvelse) set at 2), 3), 4) og 5) er ækvivalente. Derfor er det nok at bevise at 1) og 3) er ækvivalente.

3) $\Longrightarrow$ 1): Hvis $a \in [b]_n$, da findes $q \in \mathbb{Z}$ så at $a = qn + b$. Derfor er $a - b = qn$, hvilket viser at $n|(a-b)$.

1) $\Longrightarrow$ 3): Hvis $n|(a-b)$, da findes $q \in \mathbb{Z}$ så at $a - b = qn$. Det følger at $a = qn + b$, og derfor er $a \in [b]_n$. □

Korollar 5.3.3 *Lad $n \in \mathbb{N}$ og $a \in \mathbb{Z}$. Da gælder at*

$$[a]_n = \{b \in \mathbb{Z} : a \equiv_n b\}.$$

Bevis. Fra foregående proposition har vi at $a \equiv_n b$ hvis og kun hvis $b \in [a]_n$. Altså har mængden på højresiden ovenfor samme elementer som mængden på venstresiden, og de to mængder er så identiske. □

Proposition 5.3.4 *Relationen $\equiv_n$ har følgende egenskaber:*

I) $a \equiv_n a$, ("$\equiv_n$ er **refleksiv***").*

II) Hvis $a \equiv_n b$ da er $b \equiv_n a$ ("$\equiv_n$ er **symmetrisk***").*

III) Hvis $a \equiv_n c$ og $c \equiv_n b$, da er $a \equiv_n b$ ("$\equiv_n$ er **transitiv***").*

Bevis. I) Da $n|(a-a)$.

II) Hvis $n|(a-b)$ så findes $q \in \mathbb{Z}$ så at $a - b = qn$. Så er $b - a = -qn$, og derfor gælder at $n|(b-a)$.

III) Antag at $n|(a-c)$ og $n|(c-b)$. Da findes $q, q' \in \mathbb{Z}$ så at $a - c = qn$ og $c - b = q'n$. Derfor gælder

$$a - b = (a-c) + (c-b) = qn + q'n = (q+q')n,$$

hvilket viser at $n|(a-b)$, som ønsket □.

Øvelse 26 . *Giv et alternativt bevis for foregående Proposition der udnytter at 1) og 2) i Proposition 5.3.2 er ækvivalente.*

Bemærkning. Relationen $\equiv_n$ har egenskaberne refleksivitet, symmetri, og transitivitet til fælles med lighedsrelationen, $=$, som opfylder de samme tre egenskaber (overvej). Det betyder dog **absolut ikke** at $\equiv_n$ er det samme som $=$, langt fra. Alligevel har $\equiv_n$ og $=$ en slags abstrakt broderskab. Vi vender tilbage til egenskaberne refleksivitet, symmetri, og transitivitet når vi senere i kurset introducerer ækvivalensrelationer.

Følgende lemma bør opfattes som en generalisering af Sætning 5.1.1.

Lemma 5.3.5 *Lad $n \in \mathbb{N}$ være givet, og lad $a, a', b, b' \in \mathbb{Z}$. Antag at $a \equiv_n a'$ og at $b \equiv_n b'$. Da gælder*

$$a + b \equiv_n a' + b'$$

og

$$a \cdot b \equiv_n a' \cdot b'.$$

Bevis. Da $a \equiv_n a'$ og $b \equiv_n b'$ kan vi finde $q, q' \in \mathbb{Z}$ sådan at $a - a' = qn$ og $b - b' = q'n$. Så gælder at

$$(a+b) - (a'+b') = (a-a') + (b-b') = qn + q'n = (q+q')n,$$

hvilket viser at $n|((a+b) - (a'+b'))$.

Tilsvarende har vi

$$ab - a'b' = a(b-b') + b'(a-a') = aq'n + b'qn = (aq' + b'q)n,$$

hvilket viser at $n|(ab - a'b')$, som ønsket. □

Øvelse 27 *Giv et bevis for foregående Lemma som udnytter Sætning 5.1.1 og ækvivalensen af 1) og 2) i Proposition 5.3.2 i stedet.*

Korollar 5.3.6 *Lad $n \in \mathbb{N}$ være givet, og lad $a, a', b, b' \in \mathbb{Z}$. Antag at $[a]_n = [a']_n$ og at $[b]_n = [b']_n$. Da gælder*

$$[a+b]_n = [a'+b']_n$$

og

$$[a \cdot b]_n = [a' \cdot b']_n.$$

Bevis. Dette er blot en omformulering af foregående lemma som udnytter ækvivalensen af 1) og 5) i Proposition 5.3.2. □

5.4 Regning med restklasser

Lad igen $n \in \mathbb{N}$ være givet. I dette afsnit ser vi på mængden af restklasser modulo, som vi betegner $\mathbb{Z}/n$. Med andre ord,

$$\mathbb{Z}/n = \{[a]_n : a \in \mathbb{Z}\}.$$

Det er vigtigt at forstå at $\mathbb{Z}/n$ er en *mængde af mængder*[3], idet hvert element i $\mathbb{Z}/n$ jo er en restklasse modulo n, og derfor er delmængde af $\mathbb{Z}$.

[3] Det kan tage lidt tid før man vænner sig til denne nye abstraktion. Vi skal se meget mere på mængder af mængder i kapitlet "Mere mængdelære". Det er dog en god ide at vænne sig til idéen nu.

Øvelse 28 *Vis at $\mathbb{Z}/n = \{[a]_i : 0 \leq a < n\}$, og at mængden $\mathbb{Z}/n$ har præcis n elementer. Hint: Brug f. eks. Korollar 5.2.3.*

Vi forsøger nu at definere de aritmetiske operationer $+$ og $\cdot$ på $\mathbb{Z}/n$. Vi nedskriver først definitionen, og beviser bagefter at den giver mening.

Definition 5.4.1 *Lad $n \in \mathbb{N}$, lad $C, D \in \mathbb{Z}/n$. Lad $a \in C$ og $b \in D$. Vi definerer*

$$C + D \stackrel{def}{=} [a+b]_n$$

og

$$C \cdot D \stackrel{def}{=} [ab]_n.$$

Denne definition er potentielt problematisk. Det er nemlig ikke klart at $C + D$ og $C \cdot D$ er **veldefinerede**, da det der står på højresiden afhænger af de valgte repræsentanter a og b. Men hvad hvis man valgte *andre* repræsentanter for C og D? Kunne man så risikere at få et andet resultat når man udregner $C + D$ og $C \cdot D$?

Hvis dette problem opstod, så ville ovenstående ikke være en definition af aritmetiske operationer på restklasserne, men i stedet en definition af operationer på repræsentanterne, hvilket ville være væsentligt mindre interessant. Heldigvis er dette ikke tilfældet, som følgende sætning viser.

Sætning 5.4.2 *De aritmetiske operationer $+$ og $\cdot$ på $\mathbb{Z}/n$ er veldefinerede. Dvs., hvis $C, D \in \mathbb{Z}/n$ og $a, a' \in C$ og $b, b' \in D$ da gælder*

$$[a + b]_n = [a' + b']_n$$

og

$$[ab]_n = [a'b']_n.$$

Med andre ord: Højresiderne i foregående definition er uafhængige af valget af repræsentanter for C og D.

Bevis. Hvis $a, a' \in C$ og $b, b' \in D$ da følger fra Proposition 5.3.2 at $[a]_n = C = [a']_n$ og $[b]_n = D = [b']_n$. Fra Korollar 5.3.6 følger så at $[a + b]_n = [a' + b']_n$ og $[ab]_n = [a'b']_n$. □

Følgende proposition er en indlysende, men vigtig, konsekvens af definitionen af $+$ og $\cdot$ på $\mathbb{Z}/n$.

Proposition 5.4.3 *Lad $n \in \mathbb{N}$ og $a, b \in \mathbb{Z}$. Da gælder*

$$[a]_n + [b]_n = [a + b]_n$$

og

$$[a]_n \cdot [b]_n = [ab]_n.$$

Bevis. Følger direkte af definitionen da $a \in [a]_n$ og $b \in [b]_n$. □

Vi kigger nu igen på vores eksempel fra begyndelsen af kapitlet:

EKSEMPEL. Det oplyses at 1. januar 2018 var en mandag. Brug regning med restklasser til at finde ud af hvilken ugedag 1. januar 2000 var.

Løsning. Vi bruger restklasserne $[0]_7, [1]_7, \ldots, [6]_7$ til at repræsentere hhv. mandag, tirsdag,..., søndag. Da 1. januar 2018 var en mandag repræsenteres denne dag altså af $[0]_7$.

Som vi fandt ud af i eksemplet fra begyndelsen af kapitlet, så er der gået

$$13 \cdot 365 + 5 \cdot 366$$

dage fra 1. januar 2000 til 1. januar 2018. Derfor repræsenterer

$$[-13 \cdot 365 - 5 \cdot 366]_7$$

ugedagen, som 1. januar 2000 faldt på. Ved at bruge Proposition 5.4.3 får vi

$$\begin{aligned}[-13 \cdot 365 - 5 \cdot 366]_7 &= [-13]_7 \cdot [365]_7 + [-5]_7 \cdot [366]_7 \\ &= [1]_7 \cdot [1]_7 + [2]_7 \cdot [2]_7 \\ &= [1 \cdot 1]_7 + [2 \cdot 2]_7 \\ &= [1]_7 + [4]_7 \\ &= [5]_7.\end{aligned}$$

Da $[5]_7$ repræsenterer lørdag følger det, at 1. januar 2000 var en lørdag.

Øvelse 29 *Fuldmåne indtræder med (cirka) 29,5 dages mellemrum. Fuldmåne i september 2018 sker tirsdag d. 25. september.*

På hvilken ugedage vil der være fuldmåne i september 2019?

Hint: *Argumentér for at* $12 \cdot 29,5 = 6 \cdot 59$ *dage efter 25. september 2018 er en dag i september 2019. Brug derefter regning med restklasser modulo 7 til at repræsentere ugedagene, som i foregående eksempel.*

Regneregler (love) for $+$ *og* $\cdot$ *på* $\mathbb{Z}/n$*, og reglernes navne*

Vi afslutter vores diskussion af modulær aritmetik med følgende to sætning om regneregler for regning med restklasser vha. af operationerne $+$ (addition) og $\cdot$ (multiplikation) på $\mathbb{Z}/n$.

Den første sætning viser at regning med restklasserne i $\mathbb{Z}/n$ opfylder mange af de samme abstrakte regneregler som $+$ og $\cdot$ på $\mathbb{Z}$ gør. Den anden sætning viser, at hvis n yderligere er et *primtal*, så opfylder $\mathbb{Z}/n$ mange af de samme abstrakte regneregler som $+$ og $\cdot$ på $\mathbb{R}$, $\mathbb{Q}$ og $\mathbb{C}$ gør.

Det er uhyre vigtigt at man lærer navnene på regnereglerne. Af historiske grunde kaldes nogle af regnereglerne for "love".

Sætning 5.4.4 *Lad* $n \in \mathbb{N}$ *være givet, lad* $x, y, z \in \mathbb{Z}/n$ *være arbitrære. Da gælder følgende regneregler for* $+$ *og* $\cdot$ *på* $\mathbb{Z}/n$*:*

1. **Den associative lov for addition på** $\mathbb{Z}/n$*: Der gælder* $(x + y) + z = x + (y + z)$.
2. $[0]_n$ *er* **neutralt element** *for* $+$*, dvs.*
$$x + [0]_n = [0]_n + x = x.$$
3. **Eksistens af additiv invers***: Der findes et entydigt element i* $\mathbb{Z}/n$*, betegnet* $-x$*, sådan at*
$$x + -x = -x + x = [0]_n.$$
(Elementet $-x$ *afhænger af* x*.)*
4. **Den associative lov for multiplikation på** $\mathbb{Z}/n$*: Der gælder*
$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

5. $[1]_n$ *er* **neutralt element** *for* $\cdot$*, dvs.* $x \cdot [1]_n = [1]_n \cdot x = x$.

6. **Den kommutativ lov for addition:** *Der gælder*

$$x + y = y + x.$$

7. **De distributive love***: Der gælder*

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

og

$$(y + z) \cdot x = y \cdot x + z \cdot x.$$

8. **Den kommutativ lov for multiplikation:** *Der gælder*

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

Bemærkning 5.4.5 *Det er let at tro at Sætning 5.4.4 er fuldkommen triviel og ikke kræver bevis, fordi de nedskrevne regler og love jo er sande for* almindelig *addition og multiplikation af* almindelige *tal.* **At tro dette er en stor fejl***. Restklasser er ikke tal, og derfor er der a priori (på forhånd) ikke nogen grund til at tro at de opfylder samme lovmæssigheder som addition og multiplikation af tal. Foregående sætning siger at de i vidt omfang gør, men det kræver altså bevis!*

Bevis for sætning 5.4.4. Vi giver bevis for 1 og 3 ovenfor, og overlader resten som en øvelse.

1) Lad $a, b, c \in \mathbb{Z}$ være sådan at $x = [a]_n$, $y = [b]_n$ og $z = [c]_n$. Da gælder

$$\begin{aligned}(x + y) + z &= ([a]_n + [b]_n) + [c]_n \\ &= [a + b]_n + [c]_n \\ &= [(a + b) + c]_n \\ &= [a + (b + c)]_n \\ &= [a]_n + [b + c]_n \\ &= [a]_n + ([b]_n + [c]_n) \\ &= x + (y + z).\end{aligned}$$

Bemærk at ovenfor bruges Proposition 5.4.3 til at opnå det 2., 3., 5. og 6. lighedstegn, mens det 4. lighedstegn følger fordi addition på $\mathbb{Z}$ i sig selv opfylder den associative lov. (Overvej!)

3) Lad $a \in \mathbb{Z}$ være sådan at $x = [a]_n$. Lad $-x = [-a]_n$. Da gælder

$$x + -x = [a]_n + [-a]_n = [a - a]_n = [0]_n.$$

På lignende vis ses at $-x + x = [0]_n$. □

Øvelse 30 *Bevis resten af Sætning 5.4.4.*

Sætning 5.4.6 *Lad $n \in \mathbb{N}$ være et* **primtal**. *Da gælder følgende yderligere lovmæssighed: Hvis $z \in \mathbb{Z}/n$, og $z \neq [0]_n$, da findes et entydigt bestemt element $z^{-1} \in \mathbb{Z}/n$ sådan at*

$$z \cdot z^{-1} = z^{-1} \cdot z = [1]_n.$$

Med andre ord: Hvis n er et primtal, da har ethvert $z \in \mathbb{Z} \setminus \{[0]_n\}$ en **multiplikativ invers**.

Bevis. Lad $a \in \mathbb{Z}$ sådan at $x = [a]_n$. Da $x \neq [0]_n$ gælder at n ikke går op i a. (Overvej nøje. Hvis $n|a$, hvad er $[a]_n$ så?). Da n er primtal følger at $\mathrm{sfd}(a, n) = 1$. I følge Bezouts Lemma findes derfor $x, y \in \mathbb{Z}$ sådan at $1 = xn + ya$. Lad $z^{-1} = [y]_n$. Da gælder

$$\begin{aligned} z^{-1} \cdot z = [y]_n[a]_n = [ya]_n = [1 - xn]_n = [1]_n + [-xn]_n \\ = [1]_n + [0]_n = [1]_n, \end{aligned}$$

som ønsket. (Undervejs har vi omskrevet $1 = xn + ya$ til $ya = 1 - xn$, og vi har brugt at $[-xn]_n = [0]_n$, hvilket følger f. eks. fra Lemma 5.2.2.) Til slut bemærkes at $z \cdot z^{-1} = [1]_n$ følger fra en fuldstændig lignende udregning. □

Øvelse 31 *I foregående bevis skulle vi arbejde ganske hårdt for at finde en kandidat til hvad z^{-1} skulle være. Hvorfor kan man ikke bare tage $[\frac{1}{a}]_n$?*

Øvelse 32 *Vis at forudsætningen i Sætning 5.4.6 om at n skal være et primtal ikke uden videre kan fjernes.*

Hint: Kig f. eks. på $\mathbb{Z}/4$, og betragt elementet $[2]_4$.

Øvelse 33 *Bevis følgende "optimale" version af Sætning 5.4.6: Lad $n \in \mathbb{N}$ og $a \in \mathbb{Z}$. Da har $[a]_n$ en multiplikativ invers i $\mathbb{Z}/n$ hvis og kun hvis $\mathrm{sfd}(a, n) = 1$ (mao. a og n er indbyrdes primiske).*

Afsluttende bemærkning: Ringe og legemer

De to foregående sætninger viser, at $\mathbb{Z}/n$, når denne udstyres med regneoperationerne $+$ og $\cdot$ som blev defineret ovenfor i begyndelsen af afsnit 5.4, har en algebraisk struktur der i høj grad ligner talsystemerne $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ eller $\mathbb{C}$. Hvis n er et primtal så ligner $\mathbb{Z}/n$ faktisk mere $\mathbb{Q}$, $\mathbb{R}$ eller $\mathbb{C}$ end $\mathbb{Z}$, i følge foregående sætning.

Senere i kurset skal vi kort se på abstrakte algebraiske strukturer som opfylder 1) – 7) i Sætning 5.4.4. En sådan algebraiske struktur kaldes en **ring**. En algebraisk struktur der opfylder 1) – 8) i Sætning 5.4.4 kaldes en **kommutativ ring**. Hvis en algebraisk struktur opfylder 1)– 8) i Sætning 5.4.4 og *desuden* opfylder Sætning 5.4.6, så kalder man den for et *legeme* (Tysk: Körber. Engelsk: Field.)

Med henvisning til hvad der kommer senere kan vi altså omformulere de foregående to sætninger som følger:

Sætning 5.4.7 *Lad $n \in \mathbb{N}$. Da er $\mathbb{Z}/n$ en kommutativ ring når den udstyres med regneoperationerne $+$ og $\cdot$ som defineret i begyndelsen af afsnit 5.4 ovenfor. Hvis n er et primtal, så er $\mathbb{Z}/n$ et legeme (og omvendt: Hvis $\mathbb{Z}/n$ er et legeme da er n et primtal.)*

6
Mere mængdelære

Thales fra Milet (ca. 635–546 f.v.t.) sagde: Alt er vand. Vores tids matematikere siger: Alt er mængder. Eller rettere: Alle matematiske objekter er mængder. Mængdelæren anses nemlig af de fleste for at være matematikkens grundlag, dvs. en universel teori for matematik, en teori som omgiver al anden matematik.[1]

I dette kapitel bygger vi videre på de elementære mængdebegreber som vi allerede har indført i kapitel 1.

Vi tager synspunktet "alt er mængder" helt alvorligt. Hvis x er en mængde og $y \in x$, så er y også en mængde, for *alt er mængder*. Dette føles nok lidt mærkeligt i starten, for hvis nu vi tager mængden naturlige tal $\mathbb{N}$, og $y \in \mathbb{N}$, så vil vi jo nok mene at y er et tal, og ikke en mængde. Dette er dog en misforståelse: I moderne matematik er alt mængder, og derfor er ethvert $y \in \mathbb{N}$ en mængde *som naturligt også fortolkes som et tal*. Tallet 2 er f. eks. mængden $\{\emptyset, \{\emptyset\}\}$; dette vender vi tilbage til senere.

[1] Mængdelæren, og idéen om at mængdelæren er matematikkens grundlag, er ret ny. Det er Cantor der fra ca. 1870 og frem indfører mængdelæren, og fra ca. 1900 er mange af tidens store matematikere blevet overbevist om at mængdelæren er den rigtige grundlagsteori. Det er dog først fra omkring 1930 at mængdelærens grundprincipper, *aksiomerne*, er helt på plads.

Inden vi for alvor går igang minder vi læseren om at der for mængder A og B gælder:

1. $A = B$ er ensbetydende med $(\forall x) x \in A \iff x \in B$;

2. $A \subseteq B$ er ensbetydende med $(\forall x) x \in A \implies x \in B$;

3. fra 1 og 2 fås derfor: $A = B \iff A \subseteq B \wedge B \subseteq A$

Punkt 3 giver anledning til en almindelig måde at bevise at to mængder er lig med hinanden: Man viser de to inklusioner.

6.1 Mængdealgebra med de endelige mængdeoperationer

Læseren husker fra kapitel 1 definitionerne af $\cap, \cup, \setminus, \triangle$ og $\times$. Med de logiske tegn kan disse udtrykkes som

$$\begin{aligned} A \cup B &= \{x : x \in A \vee x \in B\}, \\ A \cap B &= \{x : x \in A \wedge x \in B\}, \\ A \setminus B &= \{x : x \in A \wedge x \notin B\}, \\ A \triangle B &= (A \setminus B) \cup (B \setminus A), \\ A \times B &= \{(a,b) : a \in A \wedge b \in B\}. \end{aligned}$$

Vi vil nu kigge lidt nærmere på nogle algebraiske identiteter der er tilknyttet disse. Man bør lære de vigtigste af dem, dvs. de distributive love og de Morgans love, udenad. Andre regneregler kan man som regel selv bevise når behovet opstår, eller slå op.

Sætning 6.1.1 ("De distributive love") *Der gælder for alle mængder A, B og C:*

$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \end{aligned}$$

Vi beviser kun den første identitet og overlader den anden til læseren som en øvelse.

Bevis. Vi viser de to inklusioner.

"$\subseteq$" : Antag at $x \in A \cup (B \cap C)$. Så er $x \in A$ eller $x \in B \cap C$.

Hvis $x \in A$, så er $x \in A \cup B$ og $x \in A \cup C$, så $x \in (A \cup B) \cap (A \cap C)$, som ønsket. Antag derfor at $x \notin A$. Så er $x \in B \cap C$, dvs. $x \in B$ og $x \in C$. Derfor er $x \in A \cup B$ og $x \in A \cup C$, og derfor gælder $x \in (A \cup B) \cap (A \cap C)$, som ønsket.

"$\supseteq$" : Antag $x \in (A \cup B) \cap (A \cup C)$. Så er $x \in A \cup B$ og $x \in A \cup C$.

Hvis $x \in A$ følger naturligvis $x \in A \cup (B \cap C)$, så vi kan antage $x \notin A$. Da $x \in A \cap B$ og $x \notin A$ gælder så $x \in B$. Ligeledes ses at $x \in C$ gælder. Vi har nu vist at $x \in B \cap C$, og derfor også at $x \in A \cup (B \cap C)$, som ønsket. □

Sætning 6.1.2 ("De Morgans love") *Lad A, B, og C være mængder. Da gælder*

$$\begin{aligned} A \setminus (B \cap C) &= (A \setminus B) \cup (A \setminus C) \\ A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C) \end{aligned}$$

Øvelse 34 *Bevis den foregående sætning. Det kan f. eks. gøres ved at vise "to inklusioner" som vi gjorde med de distributive love.*

6.2 Funktioner (abstrakt, mængdeteoretisk defineret)

Vi indfører nu, som tidligere lovet, det abstrakte, mængdeteoretiske funktionsbegreb. I næste kapitel går vi i dybden med funktionsbegrebet, her giver vi blot definitionen og et par eksempler.

Tidligere sagde vi blot at en funktion $f : A \to B$ er en "en regel, der til ethvert $x \in A$ knytter et og kun et element $f(x) \in B$", men nu indfører vi funktioner rigtigt og stringent.[2]

Definition 6.2.1 *En* funktion[3] *fra en mængde A til en mængde B er en mængde $f \subseteq A \times B$ sådan at følgende er opfyldt:*

1. *For ethvert $x \in A$ findes $y \in B$ så at $(x, y) \in f$;*
2. *Hvis $(x, y) \in f$ og $(x, y') \in f$ da er $y = y'$.*

Med andre ord: For ethvert $x \in A$ er der ét og kun ét $y \in B$ sådan $(x, y) \in f$.[4]

Hvis $f \subseteq A \times B$ er en funktion fra A til B, da skriver vi $f : A \to B$, og hvis $x \in A$ da skriver vi $f(x)$ for det entydige $y \in B$ sådan at $(x, y) \in f$. Vi kalder A **domænet** *for f, og B kaldes* **codomænet** *for f.*

Intuitionen bag foregående definition er at vi har valgt at bruge grafen for f, som jo på en naturlig måde er en delmængde af $A \times B$, til at repræsentere f som en mængde. Det virker måske baglæns. Det ændrer dog i praksis meget lidt på hvordan vi tænker på og bruger funktioner i vores matematiske dagligdag.

Fordelen ved vores mængdeteoretiske definition af begrebet "funktion" er at den gør det muligt at tale abstrakt om funktioner. Vores "gamle" funktionsbegreb fra Kapitel 2 sagde at en funktion var noget, der var givet en regel eller en foreskrift, men vores nye begreb kræver intet at den art. Nu er en funktion simpelthen bare en mængde af par, der opfylder det naturlige krav at der er en entydig funktionsværdi til ethvert element i domænet.

EKSEMPLER. 1) Vi er vandt til at give en funktion ved en forskrift, f. eks. $f(x) = x^2 + e^x$. Det er også fint, så længde foreskriften for ethvert x giver en entydig funktionsværdi.

I det nærværende eksempel er funktionen $f(x)$ fra et mængdeteoretisk synspunkt faktisk mængden

$$\{(x, x^2 + e^x) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}.$$

2) Mængden

$$\mathbb{T} = \{(x, y) : x^2 + y^2 = 1\}$$

er ikke nogen funktion. (Hvorfor?)

Notation: Når man skal angive en funktion, så er det ret almindeligt at skrive $f : x \mapsto \ldots$ frem for $f(x) = \ldots$. F. eks. kunne vi ovenfor i det første eksempel have skrevet $f : x \mapsto x^2 + e^x$ i stedet for $f(x) = x^2 + e^x$.

[2] Husk at i moderne matematik er *alt* mængder, så en funktion må også være en mængde. Det er det, vi tidligere har tænkt på som grafen for en funktion som vi nu bruger til at definere *begrebet* funktion.

[3] Nogle gange kaldes en funktion også en afbildning. Ordet funktion er i de sidste 20 år igen blevet det mest brugte ord.

[4] Denne del af definitionen siger, sagt i daglig tale, at der for ethvert $x \in A$ er en entydigt fastlagt funktionsværdi $y \in B$ knyttet til x.

6.3 *n-ært produkt*

Definition 6.3.1 *Lad $n \in \mathbb{N}$. En* n-tupel *er en ordnet liste $(x_1, \ldots, x_n)$ af n matematiske objekter.*[5]

[5] Bemærk at et ordnet par (x_1, x_2) er det samme som en 2-tupel.

Vi generaliserer nu det cartesiske produkt, idet vi indfører produktet af *flere* end 2 mængder.

Definition 6.3.2 *Lad $A_1, A_2, \ldots, A_n$ være $n \geq 2$ mængder. Da defineres produktet af $A_1, A_2, \ldots, A_n$ ved*

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_1 \in A_1 \wedge x_2 \in A_2 \wedge \cdots \wedge x_n \in A_n\},$$

dvs. $A_1 \times A_2 \times \cdots \times A_n$ består af alle n-tupler $(x_1, x_2, \ldots, x_n)$ hvor $x_1 \in A_1$, $x_2 \in A_2$, osv.

Når man tager produktet af den samme mængde n gange skriver man A^n, dvs.

$$A^n = \underbrace{A \times \cdots \times A}_{\text{(n faktorer)}}$$

EKSEMPLER. (a) Som nævnt i Kapitel 1 er $\mathbb{R}^2$ det, vi normalt tænker på som planen. Naturligvis er $\mathbb{R}^3$ derfor det, vi normalt tænker på som det 3-dimensionelle Euklidiske rum, og $\mathbb{R}^n$ er det n-dimensionelle Euklidiske rum.

(b) Mængden $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ kan man tænke på som "gitterpunkterne" i planens 1. kvadrant, dvs. de punkter i planen der har naturlige tal som koordinater.

(c) Mængden $\mathbb{Z} \times \mathbb{Q} \times \mathbb{C}$ er mængden af alle tripler (a, q, z) hvor a er et helt tal, q er et rationalt tal, og z er et komplekst tal.

6.4 *Indicerede familier af mængder*

Tæt forbundet til konceptet relation er et andet koncept, nemlig de indicerede familier af mængder.

Definition 6.4.1 *Lad I være en (som regel ikke-tom) mængde, nedenfor kaldet "indexmængden". En* familie af mængder indiceret af I *er en funktion $i \mapsto X_i$, hvis domæne er I, og hvis codomæne er mængden af mængder $\{X_i : i \in I\}$.*

Man skriver almindeligvis sådan en familie som $(X_i)_{i \in I}$, hvormed man mener at funktionen f er givet ved $f : i \mapsto X_i$.

Eksempler 1) Lad $\mathbb{Q}$, de rationale tal, være vores indeksmængde. Da kan vi danne familien $(X_q)_{q \in \mathbb{Q}}$ af delmængder af $\mathbb{R}$, som er defineret ved

$$X_q = \{x \in \mathbb{R} : x \neq q\}.$$

Bemærk at (for et givent $q \in \mathbb{Q}$) består mængden X_q af de reelle tal, som ikke er lig med q.

2) Lad $n \in \mathbb{N}$. Husk, at for ethvert $a \in \mathbb{Z}$ er $[a]_n$ restklassen af a modulo n, og at restklassen $[a]_n \subseteq \mathbb{Z}$. Dermed er $([a]_n)_{a\in\mathbb{Z}}$ en familie af delmængder af $\mathbb{Z}$, som er parametriseret af $\mathbb{Z}$.

(I en hvis forstand er $([a]_n)_{a\in\mathbb{Z}}$ "overparametriseret", dvs. den samme mængde gentages mange gange med forskellige indeks, idet vi får en familie med de samme mængder ved at kigge blot på $([r]_n)_{0\leq r<n}$. Men den slags "overparametrisering" er helt fint, og ofte endda praktisk.)

3) Lad $\mathbb{T} = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 0\}$, dvs $\mathbb{T}$ er enhedscirklen i planen. Definér for enhver vektor $\vec{v} \in \mathbb{T}$ mængden

$$L_{\vec{v}} = \{(x,y) \in \mathbb{R}^2 : (x,y) \cdot \vec{v} = 0\}.$$

(Her er $\cdot$ prikproduktet, også kaldet skalarproduktet, som I kender fra lineær algebra eller plangeometri.) Da er $(L_{\vec{v}})_{\vec{v}\in\mathbb{T}}$ er familie af delmængde af planen $\mathbb{R}^2$, bestående af alle linjer gennem origo $(0,0)$.

Øvelse 35 *Lad igen $\mathbb{T}$ være enhedscirklen i $\mathbb{R}^2$. Definér for hvert $\vec{v} \in \mathbb{T}$ mængden*

$$H_{\vec{v}} = \{\vec{w} \in \mathbb{R}^2 : \vec{v} \cdot \vec{w} \geq 0\}.$$

(Prikprodukt!) Beskriv geometrisk familien af mængde $(H_{\vec{v}})_{\vec{v}\in\mathbb{T}}$.

6.5 Algebra med indicerede familier af mængder

Vi har tidligere indført forening og fællesmængde af to (og dermed endeligt mange) mængder. For indicerede familier af mængder kan disse to begreber generaliseres som følger:

Definition 6.5.1 *Lad $(X_i)_{i\in I}$ være en indiceret familie af mængder. Da definerer vi*

$$\bigcup_{i\in I} X_i = \{x : (\exists i \in I) x \in X_i\},$$

som kaldes foreningen *af familien $(X_i)_{i\in I}$, og hvis $I \neq \emptyset$ da defineres*

$$\bigcap_{i\in I} X_i = \{x : (\forall i \in I) x \in X_i\},$$

som kaldes fællesmængden *af familien $(X_i)_{i\in I}$.*

Vi tager eksemplerne fra foregående afsnit, og ser hvad der sker når vi anvender forenings- og fællesmængdeoperationerne.

Eksempler. 1) Lad igen $(X_q)_{q\in\mathbb{Q}}$ være familien hvor

$$X_q = \{x \in \mathbb{R} : x \neq q\}.$$

Da er $\bigcup_{q\in\mathbb{Q}} X_q = \mathbb{R}$ (hvorfor?), og $\bigcap_{q\in\mathbb{Q}} X_q$ er mængden af irrationale tal dvs. mængden $\mathbb{R} \setminus \mathbb{Q}$ (hvorfor?).

2) Lad $n \in \mathbb{N}$ og lad $([a]_n)_{a\in\mathbb{Z}}$ være familien af restklasser modulo n. Da er $\bigcup_{a\in\mathbb{Z}}[a]_n = \mathbb{Z}$ og $\bigcap_{a\in\mathbb{Z}}[a]_n = \emptyset$.

3) Lad $(L_{\vec{v}})_{\vec{v}\in\mathbb{T}}$ være defineret som i foregående afsnit, dvs. $L_{\vec{v}}$ er linjen gennem $(0,0)$ som er vinkelret på vektoren $\vec{v}$. Da er $\bigcup_{\vec{v}\in\mathbb{T}} L_{\vec{v}} = \mathbb{R}^2$ og $\bigcap_{\vec{v}\in\mathbb{T}} L_{\vec{v}} = \{(0,0)\}$.

Øvelse 36 *Vælg et af foregående eksempler, og nedskriv et detaljeret argument der viser hvad foreningen og fællesmængden af familien er.*

Øvelse 37 *Definer for hvert $\vec{v} \in \mathbb{T}$ en mængde*

$$H'_{\vec{v}} = \{(x,y) \in \mathbb{R}^2 : (x,y)\cdot\vec{v} \leq 1\}.$$

(Prikprodukt!) Forklar geometrisk hvilken mængde i planen $H'_{\vec{v}}$ er. Find $\bigcup_{\vec{v}\in\mathbb{T}} H'_{\vec{v}}$ og $\bigcap_{\vec{v}\in\mathbb{T}} H'_{\vec{v}}$.

Følgende sætning giver en generalisering af de distributive love og de Morgans love til indicerede familier af mængder.

Lemma 6.5.2 *Lad $(X_i)_{i\in I}$ være en indiceret familie af mængder, og lad A være en given mængde. Da gælder*

$$A \cap (\bigcup_{i\in I} X_i) = \bigcup_{i\in I}(A \cap X_i),$$

og hvis $I \neq \emptyset$ gælder

$$A \cup (\bigcap_{i\in I} X_i) = \bigcap_{i\in I}(A \cup X_i),$$

$$A \setminus (\bigcup_{i\in I} X_i) = \bigcap_{i\in I}(A \setminus X_i),$$

og

$$A \setminus (\bigcap_{i\in I} X_i) = \bigcup_{i\in I}(A \setminus X_i).$$

Bevis. Se sætning 175 og 176 i Lützens bog ("DMM"). □

Øvelse 38 *I foregående sætning giver højresiderne kun mening hvis man forstår hvilke familier af mængder operationerne $\bigcap_{i\in I}$ og $\bigcap_{i\in I}$ anvendes på. Nedskriv disse familier af mængder.*

*6.6 Indicerede familier, hvor indeksmængden er en produktmængde**

Dette er ikke en del af vort pensum, men det er uhyre vigtigt for fremtidige kurser, særligt kurser i målteori og sandsynlighedsteori. Vi nøjes med at diskutere situationen hvor indexmængden $I = I_1 \times I_2$. Situationen hvor indexmængden er et n-ært produkt diskuteres i en øvelse.

Lad $(X_i)_{i\in I}$ være en familie af mængder indiceret af $I = I_1 \times I_2$. Vi antager at $I_1 \neq \emptyset \neq I_2$ for at undgå problemer med anvendelser af $\bigcap$.

Bemærk at ethvert element i I har formen (i,j) hvor $i \in I_1$ og $j \in I_2$. Vælges $i_0 \in I_1$ får vi derfor en familie af mængder $(X_{(i_0,j)})_{j\in I_2}$, og vælges $j_0 \in I_2$ fås en familie af mængder $(X_{(i,j_0)})_{i\in I_1}$.

For ethvert $i \in I_1$ kan vi derfor definere mængderne

$$Y_i = \bigcup_{j\in I_2} X_{(i,j)} \text{ og } Z_i = \bigcap_{j\in I_2} X_{(i,j)}$$

og for ethvert $j \in I_2$ kan vi definere

$$V_j = \bigcup_{i\in I_1} X_{(i,j)} \text{ og } W_j = \bigcap_{i\in I_1} X_{(i,j)}.$$

Vi definerer nu

$$\bigcap_{i\in I_1}\bigcup_{j\in I_2} X_{(i,j)} = \bigcap_{i\in I_1} Y_i \text{ og } \bigcup_{i\in I_1}\bigcap_{j\in I_2} X_{(i,j)} = \bigcup_{i\in I_1} Z_i,$$

og

$$\bigcap_{j\in I_2}\bigcup_{i\in I_1} X_{(i,j)} = \bigcap_{j\in I_2} V_j \text{ og } \bigcup_{j\in I_2}\bigcap_{i\in I_1} X_{(i,j)} = \bigcup_{j\in I_2} W_j,$$

Øvelse 39 *Lad $I = \mathbb{Z}\times\mathbb{Z}$ og lad*

$$X_{i,j} = \{(x,y) \in \mathbb{R}\times\mathbb{R} : (x = i \wedge y = j \wedge j \geq |i|) \vee (j < |i| \wedge x = 0)\}.$$

Find (dvs. beskriv) mængderne

$$\bigcap_{i\in\mathbb{Z}}\bigcup_{j\in\mathbb{Z}} X_{(i,j)},\ \bigcup_{i\in\mathbb{Z}}\bigcap_{j\in\mathbb{Z}} X_{(i,j)},\ \bigcap_{j\in\mathbb{Z}}\bigcup_{i\in\mathbb{Z}} X_{(i,j)},\ \text{og}\ \bigcup_{j\in\mathbb{Z}}\bigcap_{i\in\mathbb{Z}} X_{(i,j)}.$$

(Bemærk at mængderne $X_{(i,j)}$ er delmængder af $\mathbb{R}^2$; at når $j \geq |i|$ så har $X_{(i,j)}$ præcis et element (hvilket?); og at når $j < |i|$ er $X_{i,j} = \{0\}\times\mathbb{R}$.)

Sætning 6.6.1 *Der gælder at*

$$\bigcap_{i\in I_1}\bigcup_{j\in I_2} X_{(i,j)} = \{x : (\forall i \in I_1)(\exists j \in I_2)\ x \in X_{i,j}\},$$

$$\bigcup_{i\in I_1}\bigcap_{j\in I_2} X_{(i,j)} = \{x : (\exists i \in I_1)(\forall j \in I_2)\ x \in X_{i,j}\},$$

$$\bigcap_{j\in I_2}\bigcup_{i\in I_1} X_{(i,j)} = \{x : (\forall j \in I_2)(\exists i \in I_1)\ x \in X_{i,j}\},$$

$$\bigcup_{j\in I_2}\bigcap_{i\in I_1} X_{(i,j)} = \{x : (\exists j \in I_2)(\forall i \in I_1)\ x \in X_{i,j}\}.$$

Øvelse 40 *Bevis foregående sætning. (Man kan f. eks. vise de to inklusioner i hvert tilfælde.)*

Øvelse 41 *Lad $I = I_1 \times I_2$, og lad $(X_i)_{i\in I}$ være en familie af mængder sådan at $X_i \subseteq A$ for alle $i \in I$. I det følgende bruges ^{c} til at indikere komplement med hensyn til A som grundmængde, f. eks. $X_i^c = A \setminus X_i$. Vis at*

$$(\bigcap_{i\in I_1}\bigcup_{j\in I_2} X_{(i,j)})^c = \bigcup_{i\in I_1}\bigcap_{j\in I_2} X_{(i,j)}^c.$$

(Lignende identiteter gælder naturligvis for de 3 andre måder at kombinere $\bigcup$ og $\bigcap$.)

Øvelse 42 *Denne øvelse henvender sig til dem, der har lyst til selv at udvikle lidt teori.*

Lav en general teori om familier af mængder indiceret af produktmængder på formen $I_1 \times I_2 \times \cdots I_k$. Definér rekursivt (på k) operationer af alternerende forening og fællesmængde så som f. eks. $\bigcup\bigcap\bigcup\cdots$. Formulér og bevis en sætning á la Sætning 6.6.1, og generalisér foregående øvelse.

6.7 Potensmængde

Givet en mængde X, da kan man forme mængden[6]

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

dvs. mængden af delmængder af X. Dette kaldes *potensmængden* af X.

[6] Vores misbrug af mængdebyggeren retfærdigøres af det såkaldte *potensmængdeaksiom*.

Bemærk, at det betyder det samme at skrive $A \in \mathcal{P}(X)$ som at skrive $A \subseteq X$. Bemærk også, at der altid gælder at $\emptyset \in P(X)$ og $X \in P(X)$.

Øvelse 43 *Lad $x_1, \ldots, x_n$ være vilkårlige mængder.*

1) Nedskriv $\mathcal{P}(\{x_1, x_2\})$ på listeform.

2) Bevis at mængden $\mathcal{P}(\{x_1, \ldots, x_n\})$ har 2^n elementer. (Hint: Induktion efter n.)

3) Hvor mange elementer har $\mathcal{P}(\emptyset)$?

Bemærkning. Begrebet potensmængde er nyttigt og vigtigt i moderne matematik, men det er også kontroversielt. For hvad er $\mathcal{P}(\mathbb{N})$, f. eks.? Definitionsmæssigt er det bare mængden af delmængder af $\mathbb{N}$, men dermed har vi indført et objekt, der "fanger" totaliteten af alle delmængder af $\mathbb{N}$, uden at have sagt noget om hvilke delmængder af $\mathbb{N}$ der findes. Dette er, ved nærmere eftertanke, en højest mærkværdigt måde at lave matematik på. På længere sigt fører denne uforsigtighed til Cantors *kontinuumsproblem* (også kaldet kontinuumshypotesen).

6.8 Tal som mængder i mængdelæren (ikke del af pensum!)

Alt er mængder. Derfor er tal også mængder. Men hvordan?

Vi starter med at definere at 0 er repræsenteret af den tomme mængde, $\emptyset$. Dette giver god mening: Den tomme mængde er en mængde med 0 elementer.

Definér generelt for en mængde x at $\mathcal{S}(x) = x \cup \{x\}$. Bemærk at elementerne i $\mathcal{S}(x)$ præcis er elementerne i x, samt mængden x selv.

Vi definerer ved rekursion: $1 = \mathcal{S}(0)$, og generelt er $n+1 = \mathcal{S}(n)$.

Man ser hurtigt at

$$1 = \{\emptyset\},$$
$$2 = \{\emptyset, \{\emptyset\}\},$$
$$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},$$

osv.

Men hov, jeg sagde "ved rekursion"... Det giver vel ingen mening uden at jeg allerede har defineret mængden af naturlige tal? Derfor er ovenstående cirkulært.

Korrekt. Man indfører derfor i mængdelæren følgende aksiom:

Aksiom 6.8.1 (Uendelighedsaksiomet) *Der findes en mængde $\mathcal{I}$ sådan at $\emptyset \in \mathcal{I}$ og hvis $x \in \mathcal{I}$ så er $\mathcal{S}(x) \in \mathcal{I}$.*

Mængden $\mathcal{I}$ indeholder alle de mængder, vi gerne vil definere som naturlige tal, og muligvis mange flere mængder. Ved hjælp af potensmængden af $\mathcal{I}$ og mængdebyggeren (ikke helt trivielt) kan man nu isolere præcis delmængden af $\mathcal{I}$ som består af de elementer, der opnås ved at anvende $\mathcal{S}$ gentagende gange, startende med $\emptyset$. Med andre ord, mængden $\mathbb{N}_0$ kan, vha. mængdebyggeren, isoleres ud fra mængden $\mathcal{I}$ i aksiomet.

Derfor findes mængden $\mathbb{N}_0$, og den består præcis af de elementer, som vi ønskede at definere i vores naive, rekursive definition ovenfor.

Det er nemt at definere $\mathbb{Z}$ ud fra $\mathbb{N}_0$:

$$\mathbb{Z} = \{(i,n) \in \{0,1\} \times \mathbb{N}_0 : i = 1 \implies n > 0\}.$$

(Man skal tænke på elementerne på formen $(1,n)$ som værende de negative tal.)

Nu kan $\mathbb{Q}$ defineres som

$$\{(a,b) \in \mathbb{Z} \times \mathbb{N} : \mathrm{sfd}(a,b) = 1\}.$$

Endeligt kan $\mathbb{R}$ defineres som mængden

$$\{A \subseteq \mathbb{Q} : A \neq \emptyset \wedge \mathbb{Q} \setminus A \neq \emptyset \wedge (\forall x, y \in \mathbb{Q})((x \in A \wedge y < x) \implies y \in A)\}.$$

Dette ser spøjst ud, men man skal intuitivt (!) tænke på at hvert A i mængden ovenfor repræsenterer tallet $\sup(A)$. Endelig er

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}.$$

Hermed er alle talmængderne defineret i mængdelæren.

7
Funktioner og afbildninger

Vi følger i dette emne Lützens bog *Diskrete Matematiske Metoder*. Nedenfor findes kun nogle enkelte bemærkninger og øvelser. Det forventes nedenfor at man har læst kapitlet om funktioner og afbildninger i Lützens bog.

Husk fra forelæsningen at en funktion $f : A \to B$ er en mængde $f \subseteq A \times B$ sådan at 1) for alle $x \in A$ findes $y \in B$ så at $(x, y) \in f$ og 2) hvis $(x, y) \in f$ og $(x, y') \in f$ så er $y = y'$. Vi skriver $f(x) = y$ hvis $(x, y) \in f$.

Hvis $f : A \to B$ er en funktion da kaldes A *domænet* (eller *definitionsmængden*) og B kaldes *codomænet* (eller *sekundærmængden*). Det er almindeligt at skrive $\mathrm{dom}(f)$ for domænet af f, og $\mathrm{codom}(f)$ for codomænet af f.

Hvis $C \subseteq A$, så defineres

$$f(C) = \{y \in B : (\exists x \in C) f(x) = y\} = \{f(x) : x \in C\}.$$

Dette kaldes *billedet*[1] af C under f. Billedet af A under f, dvs. $f(A)$, benævnes også $\mathrm{im}(f)$ eller $\mathrm{ran}(f)$, og kaldes *værdimængden*[2] af f.

[1] Engelsk: *image*.

[2] Engelsk: *range*.

Bemærk at når $f : A \to B$ og $C \subseteq A$, så er $f(C) \subseteq B$.

Et begreb, jeg glemte at indføre i forelæsningen er *urbillede*. Hvis $f : A \to B$, og $D \subseteq B$, da defineres

$$f^{-1}(D) = \{x \in A : f(x) \in D\},$$

og denne mængde kaldes *urbilledet*[3] af D. Bemærk at $f^{-1}(D) \subseteq A$, og er defineret selv når f ikke har nogen invers[4].

[3] Engelsk: *pre-image.*

[4] Det er måske forvirrende at f^{-1} bruges i notationen her, men i en lidt anden betydning end invers funktion. Det må man vænne sig til. Nogle forfattere skriver i stedet $f^{\leftarrow}(D)$ for urbilledet af D, men denne notation er ikke så udbredt som $f^{-1}(D)$.

Følgende begreb er uhyre nyttigt, men mangler i Lützens bog:

Definition 7.0.1 *Lad $f : A \to B$ være en funktion, og lad $C \subseteq A$ være en delmængde af A. Da er $f \restriction C$ den funktion $C \to B$ som defineres ved*

$$(f \restriction C)(x) = f(x)$$

for alle $x \in C$. Funktionen $f \restriction C$ kaldes restriktionen[5] *af f til C.*

[5] Andre almindelige notationer for restriktionen er $f|C$ og $f_{|C}$.

Øvelse 44 *Med notation som i foregående definition, vis at $f \restriction C = f \cap C \times B$.*

Med andre ord: Restriktionen af f til C "gør det samme" som f, men er kun defineret på C.

EKSEMPEL. Lad $f : \mathbb{R} \to \mathbb{R}$ være funktionen $f(x) = e^x$. Så er $\mathrm{dom}(f) = \mathbb{R}$, $\mathrm{codom}(f) = \mathbb{R}$, $\mathrm{ran}(f) = (0, \infty)$. Hvis $C = [-1, 1]$ da er $(f \restriction C)(x) = e^x$ for alle $x \in [-1, 1]$, men i modsætning til f er $f \restriction C$ ikke defineret udenfor intervallet $[-1, 1]$.

Øvelse 45 *(a) Bevis følgende sætning:*

Sætning 7.0.2 *Lad $f : A \to B$ og $g : B \to C$ være funktioner. Da gælder*

1. *$g \circ f$ er surjektiv hvis og kun hvis $g \restriction f(A)$ er surjektiv.*
2. *$g \circ f$ er injektiv hvis og kun hvis f er injektiv og $g \restriction f(A)$ er injektiv.*
3. *$g \circ f$ er bijektiv hvis og kun hvis f er injektiv og $g \restriction f(A)$ er bijektiv.*

(b) Brug Sætning 7.0.2 ovenfor til at bevise Sætning 290 og 291 fra Lützens bog ("DMM").

Bemærkning: Sætning 7.0.2 ovenfor skal man tænke på som en bedre, skarpere version af Sætning 290 og 291, som kombinerer de to sætninger i én. Den kan dog kun formuleres når begrebet restriktion er indført.

8
Relationer, specielt ækvivalensrelationer

Vi følger i dette emne Lützens bog *Diskrete Matematiske Metoder*. Nedenfor repeterer vi dog definitionen på en relation og en ækvivalensrelation, og vi giver et eksempel og en stribe øvelser.

Definition 8.0.1 *Lad X være en mængde.*

(A) En relation[1] *på X er en delmængde af $X \times X$. Med andre ord, en mængde R er en relation på X hvis $R \subseteq X \times X$. Specielt er en relation en mængde af ordnede par.*

Hvis $(x, x') \in R$, da skriver vi xRx', og siger "x er R-relateret til x'".

(B) En ækvivalensrelation *på X er en relation E på X der opfylder følgende tre betingelser:*

[1] Det som vi kalder en relation kaldes ofte en *binær* relation i andre tekster.

1. *E er* refleksiv, *dvs.*
$$(\forall x \in X)\ xEx.$$

2. *E er* symmetrisk, *dvs.*
$$(\forall x, x' \in X)\ xEx' \implies x'Ex.$$

3. *E er* transitiv, *dvs.*
$$(\forall x, z, w \in X)\ (xEz \wedge zEw) \implies xEw.$$

Vi minder også læseren om at når E er en ækvivalensrelation på X, og $x \in X$, da kaldes mængden

$$[x]_E = \{y \in X : xEy\}$$

for x's *E-ækvivalensklasse*. Mængden af ækvivalensklasser,

$$X/E = \{[x]_E : x \in X\},$$

kaldes for *kvotientmængden* af X under E.

EKSEMPEL: Lad $n \in \mathbb{N}$. Vi har allerede set i Proposition 5.3.4 at $\equiv_n$ er refleksiv, symmetrisk og transitiv. Bemærk at

$$\equiv_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : n|(a - b)\}.$$

Derfor er $\equiv_n$ en ækvivalensrelation på $\mathbb{Z}$. (Relationen $\equiv_n$ er en *delmængde af* $\mathbb{Z} \times \mathbb{Z}$, derfor er den *en relation på* $\mathbb{Z}$.)

Bemærk at $\equiv_n$-ækvivalensklasserne det samme som restklasserne modulo n. (Overvej!) Bemærk desuden at $\mathbb{Z}/\equiv_n = \mathbb{Z}/n$.

Øvelse 46 *Definer en relation på* $\mathbb{R}$ *ved*

$$x \sim x' \iff (\exists a \in \mathbb{Z})\ x - x' = 2\pi a.$$

0) Nedskriv en definition af $\sim$ *vha. mængdebyggernotation, dvs., find ud af hvad der skal stå i stedet for spørgsmålstegnene inden for de krøllede paranteser sådan at*

$$\sim = \{? \mid ?\}.$$

1) Vis at $\sim$ *er en ækvivalensrelation på* $\mathbb{R}$.
2) Find en naturlig bijektion mellem $\mathbb{R}/\sim$ *og* $\mathbb{T}$.

Hint til 2): *Husk at* $\mathbb{T}$ *er enhedscirklen, dvs.*

$$\mathbb{T} = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\} = \{(\cos(\theta), \sin(\theta)) : \theta \in [0, 2\pi)\}.$$

Øvelse 47 *Definer en relation på* $\mathbb{R} \times \mathbb{R}$ *ved*

$$(x,y)E(x',y') \iff y = y'.$$

0) Nedskriv en definition af E *vha. mængdebyggernotation. Dvs., find ud af hvad der skal stå i stedet for spørgsmålstegnene inden for de krøllede paranteser:*

$$E = \{? \mid ?\}.$$

1) Vis at E *er en ækvivalensrelation på* $\mathbb{R} \times \mathbb{R}$.
2) Find en naturlig bijektion mellem $\mathbb{R}$ *og* $\mathbb{R} \times \mathbb{R}/E$.

Øvelse 48 *Lad* $\tilde{E}$ *være relationen på* $\mathbb{Z} \times \mathbb{N}$ *defineret ved*

$$(n,m)\tilde{E}(n',m') \iff nm' = n'm.$$

0) Nedskriv en definintion af $\tilde{E}$ *vha. mængdebyggernotation.*
1) Vis at $\tilde{E}$ *er en ækvivalensrelation (på* $\mathbb{Z} \times \mathbb{N}$*).*
2) Find en naturlig bijektion mellem $\mathbb{Z} \times \mathbb{N}/\tilde{E}$ *og* $\mathbb{Q}$.

Øvelse 49 *Definer en relation på* $\mathbb{R}$ *ved*

$$xE_v x' \iff x - x' \in \mathbb{Q}.$$

(Denne ækvivalensrelation kaldes Vitalis ækvivalensrelation*.)*
1) Vis at E_v *er en ækvivalensrelation på* $\mathbb{R}$.
2) Find en naturlig surjektion $p : \mathbb{R} \to \mathbb{R}/E_v$.
3) Find en bijektion mellem $\mathbb{R}/E_v$ *og* $\mathbb{R}$. *(Advarsel: Ikke helt let. Du får nok brug for udvalgsaksiomet i en eller anden form, f.eks. til at danne en højreinvers. Derefter kræves stadig lidt kreativitet.)*
4) Kan du finde en **naturlig** bijektion *mellem* $\mathbb{R}/E_v$ *og* $\mathbb{R}$*?*

Hint til 4): *I modsætning til de foregående øvelser vil jeg gætte på at du ikke kan, men det er svært at bevise at der* ikke *findes noget der er "naturligt", for begrebet "naturligt" er upræcist. Vi kan som regel genkende når noget er "naturligt", men hvad betyder det at en funktion ikke er naturlig?*

Men, vi kan dog prøve at undersøge om en bijektion $f : \mathbb{R}/E_v \to \mathbb{R}$ *måske må have nogle meget mærkelige egenskaber, og derfor ikke kan være naturlig. Her er en idé: Hvis* $f : \mathbb{R}/E_v \to \mathbb{R}$ *er en bijektion, så lad* $\hat{f} = f \circ p$*, hvor p kommer fra del 2) ovenfor. Så er* $\hat{f} : \mathbb{R} \to \mathbb{R}$ *en surjektion, som er konstant på hver* E_v *ækvivalensklasse. Start med at vise at* $\hat{f}$ *ikke kan være kontinuert. Ønsker man en større udfordring, så kan man forsøge med: For ethvert interval* $[a, b] \subseteq \mathbb{R}$*, hvor* $a < b$*, gælder at funktionen* $g_{[a,b]} : \mathbb{R} \to \mathbb{R}$

$$g_{[a,b]}(x) = \begin{cases} 1 & \text{hvis } x \in \hat{f}^{-1}([a,b]) \\ 0 & \text{hvis } x \notin \hat{f}^{-1}([a,b]). \end{cases}$$

ikke er Riemann (eller Lebesgue) integrabel over noget lukket interval $[c, d]$*, hvor* $c < d$*.*

9
Permutations

This chapter is in English! The reason for this is very simple: These are the first notes I wrote for DIS back in 2015, at a time when it was still possible for foreign students to request that the whole course was taught in English.

I never got around to translating this part, and as DIS is now running for the last time ever, it has now become pointless to translate it. Besides, it is probably good for you in some way to get used to reading English texts...

The chapter contains a proof of the Theorem 407 and Theorem 413 (Cykelsætningen, the "Cycle decomposition theorem") in Lützens book ("DMM"), but matches the presentation given in the lecture. Recall that a *permutation on* A (in the sense of DMM Chapter 10) simply means a bijection $\sigma : A \to A$ of the set A onto itself.

9.1 Orbits, cycles, and the decomposition theorem

Notation: (1) Given a set A, we let

$$\Sigma(A) = \{\sigma \mid \sigma : A \to A \text{ is a permutation of } A\}$$

be the set of all permutations on A.

(2) The *identity permutation* on A is denoted 1_A (or sometimes Id_A), and is defined by $1_A(x) = x$ for all $x \in A$.

(3) For $n \in \mathbb{N}$, we let $\sigma^0 = 1_A$, and

$$\sigma^n = \underbrace{\sigma \cdots \sigma}_{n \text{ times}},$$

$$\sigma^{-n} = \underbrace{\sigma^{-1} \cdots \sigma^{-1}}_{n \text{ times}}$$

(4) Given $\sigma \in \Sigma(A)$, we let

$$\mathrm{Fix}(\sigma) = \{x \in A : \sigma(x) = x\}$$

be the set of *fixpoints*, and

$$\mathrm{Move}(\sigma) = \{x \in A : \sigma(x) \neq x\}.$$

the set of *moving points* (da.: *flyttepunkter*).

Exercise 50 *Prove: If $x \in \mathrm{Move}(\sigma)$ then $\sigma(x) \in \mathrm{Move}(\sigma)$. (Hint: The contrapositive statement...)*

Recall that two permutations $\sigma, \tau \in \Sigma(A)$ are *disjoint* if $\mathrm{Move}(\sigma) \cap \mathrm{Move}(\tau) = \emptyset$.

Proposition 9.1.1 (Sætning 397) *If $\sigma, \tau \in \Sigma(A)$ are disjoint then $\sigma\tau = \tau\sigma$ (i.e., σ and τ "commute").*

Proof. Let $x \in A$. We must show that $\sigma\tau(x) = \tau\sigma(x)$. This is clear if x is a fixpoint for both σ and τ, and so we may assume that $x \in \mathrm{Move}(\sigma)$ or $x \in \mathrm{Move}(\tau)$. Suppose first $x \in \mathrm{Move}(\sigma)$. Then $x \in \mathrm{Fix}(\tau)$ and so $\sigma\tau(x) = \sigma(x)$. By Exercise 50 we also have $\sigma(x) \in \mathrm{Move}(\sigma)$, whence $\sigma(x) \in \mathrm{Fix}(\tau)$, and so $\tau\sigma(x) = \sigma(x)$. Thus

$$\sigma\tau(x) = \sigma(x) = \tau\sigma(x).$$

This finishes the proof in the case when $x \in \mathrm{Move}(\sigma)$. The proof when $x \in \mathrm{Move}(\tau)$ is, mutatis mutandis[1], the same. □

[1] *Mutatis mutandis* is Latin and means "with the necessary [and obvious] changes".

Warning: The converse to the previous proposition is *false*. For instance, σ always commutes with itself (because $\sigma\sigma = \sigma\sigma$), but σ is never disjoint from itself unless $\sigma = 1_A$.

Orbits. We shall now discuss the notion of *orbits* (da.: *baner*) of a permutation. Our approach is at first quite abstract, as we first define from a given $\sigma \in \Sigma(A)$ an equivalence relation on A.

Let $\sigma \in \Sigma(A)$. Define on A a (binary) relation E_σ by

$$xE_\sigma x' \iff (\exists n \in \mathbb{Z})\ \sigma^n(x) = x'.$$

Proposition 9.1.2 *E_σ is an equivalence relation, called the* **orbit equivalence relation**[2] *of σ.*

[2] Da.: Baneækvivalensrelation

Proof. Since $\sigma^0(x) = 1_A(x) = x$ we have $xE_\sigma x$ for all $x \in A$, whence E_σ is reflexive.

If $xE_\sigma x'$ then by definition there is some $n \in \mathbb{Z}$ such that $\sigma^n(x) = x'$. Then $\sigma^{-n}(x') = x$, which shows that $x'E_\sigma x$. Thus E_σ is symmetric.

Finally, suppose $xE_\sigma y$ and $yE_\sigma z$. Then there is $n, m \in \mathbb{Z}$ such that $\sigma^n(x) = y$ and $\sigma^m(y) = z$. But now

$$z = \sigma^m(y) = \sigma^m(\sigma^n(x)) = \sigma^{m+n}(x)$$

which shows that $xE_\sigma z$. Thus E_σ is transitive. □

Recall that the *E_σ-equivalence class* of $x \in A$ is the set

$$[x]_{E_\sigma} = \{y \in A : xE_\sigma y\}.$$

Definition 9.1.3 *Let $x \in A$ and $\sigma \in \Sigma(A)$. The equivalence class $[x]_{E_\sigma}$ is called the* orbit *of x (under σ). We write $[x]_\sigma$ or B_x for the orbit of x, that is,*

$$[x]_{E_\sigma} = [x]_\sigma = B_x.$$

Proposition 9.1.4 *The orbits form a partition (da.*: klassedeling*) of* A.

Proof. Since the orbits are by definition the E_σ equivalence classes, this follows directly from DMM Sætning 244 applied to E_σ. □

Exercise 51 *Let* $\sigma \in \Sigma(A)$ *and* $x \in A$. *Prove that*

$$[x]_\sigma = \{\sigma^n(x) : n \in \mathbb{Z}\} = \{\ldots, \sigma^{-3}(x), \sigma^{-2}(x), \sigma^{-1}(x), x, \sigma(x), \sigma^2(x), \sigma^3(x) \ldots\}.$$

(This is the definition of orbit that was given in lecture).

The next proposition shows that when A is a finite set then the definition of orbit given in our textbook agrees with the definition of orbit given in Definition 9.1.3 above.

Proposition 9.1.5 *Let* $\sigma \in \Sigma(A)$ *and* $x \in A$, *and suppose* A *is a finite set. Then the orbit* $[x]_\sigma$ *is finite, and there is* $n \in \mathbb{N}$ *such that*

$$[x]_\sigma = \{x, \sigma(x), \ldots, \sigma^{n-1}(x)\},$$

and if n *is the least such* n *then* $\sigma^n(x) = x$.

Proof. First note that since A is finite, every orbit is finite, as clearly $[x]_\sigma \subseteq A$.

Claim: There is $n \in \mathbb{N}$ such that $\sigma^n(x) \in \{x, \sigma(x), \ldots, \sigma^{n-1}(x)\}$.

Proof of Claim: If no such n existed, then the set

$$\{x, \sigma(x), \sigma^2(x), \ldots\}$$

would have to infinite, but since $\{x, \sigma(x), \sigma^2(x), \ldots\} \subseteq A$ this is impossible. $_{\text{Claim.}}\dashv$

Let n be least such that $\sigma^n(x) \in \{x, \sigma(x), \ldots, \sigma^{n-1}(x)\}$. Then $\sigma^n(x) = \sigma^k(x)$ for some $0 \leq k < n$. We can't have $k > 0$ since n was least such that $\sigma^n(x) \in \{x, \sigma(x), \ldots, \sigma^{n-1}(x)\}$. So we must have $k = 0$, which shows that $\sigma^n(x) = x$.

Finally, notice that since $x = \sigma^n(x)$ we have $\sigma^{-1}(x) = \sigma^{n-1}(x)$, whence $\sigma^{-k}(x) = \sigma^{k(n-1)}(x)$, and from this we get that

$$\{\sigma^i(x) : i \in \mathbb{Z}\} \subseteq \{x, \sigma(x), \ldots, \sigma^{n-1}(x)\}.$$

Since the opposite inclusion is also true (trivially), it follows that $[x]_\sigma = \{x, \sigma(x), \ldots, \sigma^{n-1}(x)\}$, as required. □

The following corollary is important to note, despite its being completely obvious from the previous proposition.

Corollary 9.1.6 *With notation as in the previous proposition,* n *is the number elements in the orbit* $[x]_\sigma$ *(that is,* $n = |[x]_\sigma|$*). It follows that* $\sigma^{|[x]_\sigma|}(x) = x$ *for any* $x \in A$.

Cycles and the decomposition theorem. Given a set A and *distinct* elements $a_1, \ldots, a_p \in A$, the corresponding *p-cycle* is the permutation $\gamma \in \Sigma(A)$ defined by

$$\gamma(x) = \begin{cases} x & \text{if } x \notin \{a_1, \ldots, a_p\}, \\ a_{i+1} & \text{if } x = a_i \text{ and } 1 \leq i < p, \\ a_1 & \text{if } x = a_p. \end{cases}$$

Note that if $p > 1$ then $\mathrm{Move}(\gamma) = \{a_1, \ldots, a_p\}$. If $p = 1$ then $\gamma = 1_A$, so $\mathrm{Fix}(\gamma) = A$. The p-cycle γ is denoted in *cycle notation* by $(a_1\ a_2\ \cdots\ a_p)$ (no commas). Notice that the ordering of the elements $a_1, \ldots, a_p$ is important; if we reorder the elements, then the corresponding cycle may be different. For instance, $(a_1\ a_2\ a_3)$ is not the same 3-cycle as $(a_1\ a_3\ a_2)$ (why?). However, the 3-cycles $(a_1\ a_2\ a_3)$ and $(a_2\ a_3\ a_1)$ *are* the same permutation. The latter example is a special case of the next exercise.

Exercise 52 *Let $a_1, \ldots, a_p \in A$ be distinct elements of A, and let $1 \leq i \leq p$. Show that*

$$(a_1\ a_2\ \cdots\ a_p) = (a_i\ a_{i+1}\ \cdots a_p\ a_1\ a_2\ \cdots a_{i-1}).$$

The next exercise is important because it connects cycles and orbits.

Exercise 53 *Let $a_1, \ldots, a_p \in A$ be distinct elements of A, let γ be the corresponding p-cycle, and let $1 \leq i \leq p$. Show that $[a_i]_\gamma = \{a_1, \ldots, a_p\}$, and that if $x \notin \{a_1, \ldots, a_p\}$ then $[x]_\gamma = \{x\}$.*

Definition 9.1.7 *Let A be a finite set, $\sigma \in \Sigma(A)$, $x \in A$, and let $n = |[x]_\sigma|$, so that $[x]_\sigma = \{x, \sigma(x), \ldots, \sigma^{n-1}(x)\}$. By the* n-cycle corresponding to x *(under σ) we mean the cycle*

$$(x\ \sigma(x)\ \cdots\ \sigma^{n-1}(x)),$$

and we denote this by γ_x^σ (or just γ_x if σ is understood from the context).

Proposition 9.1.8 *With notation as in the previous definition, for every $y \in [x]_\sigma$ we have*

$$\gamma_x(y) = \sigma(y).$$

Moreover, $[x]_\sigma = [x]_{\gamma_x}$, and if $y \in [x]_\sigma$ then $\gamma_y = \gamma_x$.

Proof. That $[x]_\sigma = [x]_{\gamma_x}$ is clear from the definition of γ_x. If $y \in [x]_\sigma$ then $y = \sigma^i(x)$ for some $0 \leq i < n$. If $i < n - 1$ then

$$\sigma(y) = \sigma(\sigma^i(x)) = \sigma^{i+1}(x) = \gamma(\sigma^i(x)).$$

If $i = n - 1$ then $\sigma(\sigma^i(x)) = x = \gamma(\sigma^i(x))$.

If $y \in [x]_\sigma$, then $y = \sigma^i(x)$ for some $0 \leq i < n$, and so $\gamma_y = \gamma_x$ follows from Exercise 52. □

Lemma 9.1.9 *Let A be a finite set, let $\sigma \in \Sigma(A)$, and let k be the number of σ-orbits of size > 1, and let $[x_1]_\sigma, \ldots, [x_k]_\sigma$ be those k orbits. Then the cycles $\gamma_{x_1}, \ldots, \gamma_{x_k}$ are pairwise disjoint, and*

$$\sigma = \gamma_{x_1} \ldots \gamma_{x_k}.$$

Proof. It is clear that the cycles $\gamma_{x_1}, \ldots, \gamma_{x_k}$ are disjoint, since $\mathrm{Move}(\gamma_{x_i}) = [x_i]_{\gamma_{x_i}} = [x_i]_\sigma$, where the last equality follows from Proposition 9.1.8.

If x is a fixpoint of σ, then $|[x]_\sigma| = 1$, and so $x \in \mathrm{Fix}(\gamma_{x_i})$ for all γ_{x_i}. Thus

$$\sigma(x) = x = \gamma_{x_1} \ldots \gamma_{x_k}(x).$$

Suppose then x is not a fixpoint of σ. Then x belongs to exactly one $[x_i]_\sigma$ for some $1 \leq i \leq k$. Note that the set $[x_i]_\sigma$ consists of fixpoints for all γ_{x_j}, $j \neq i$, since $\mathrm{Move}(\gamma_{x_i}) = [x_i]_{\gamma_{x_i}} = [x_i]_\sigma$. This together with Proposition 9.1.8 gives

$$\gamma_{x_1} \ldots \gamma_{x_k}(x) = \gamma_{x_i}(x) = \sigma(x),$$

as required. □

Lemma 9.1.10 *Let A be a finite set and let $\sigma \in \Sigma(A)$. Suppose σ is a product of k disjoint cycles $\gamma_1, \ldots, \gamma_k$ of length > 1. Then σ has k orbits of size > 1, and each such orbit $[x]_\sigma$ coincides with the orbit $[x]_{\gamma_i}$ for exactly one $i \leq k$, and it holds for this i that $\gamma_i = \gamma_x^\sigma$.*

Proof. Let $x \in A$, and suppose x is not a fixpoint for σ. Then for some i, x is not a fixpoint for γ_i. Since $[x]_{\gamma_i} = \mathrm{Move}(\gamma_i)$, it follows from the disjointness of the cycles $\gamma_1, \ldots, \gamma_k$ that $\gamma_i(y) = \sigma(y)$ for all $y \in [x]_{\gamma_i}$. From this $[x]_{\gamma_i} = [x]_\sigma$ and $\gamma_i = \gamma_x^\sigma$ follow easily. □

Theorem 9.1.11 (Decomposition theorem, Sætning 407) *Let A be a finite set, $\sigma \in \Sigma(A)$. Then there is a unique set $\{\gamma_1, \ldots, \gamma_k\} \subseteq \Sigma(A)$ of disjoint cycles of length > 1 such that*

$$\sigma = \gamma_1 \cdots \gamma_k.$$

Proof. Lemma 9.1.9 proves the existence of such a set $\{\gamma_1, \ldots, \gamma_k\}$; and Lemma 9.1.10 in turn proves the uniqueness. □

9.2 Opgaver

Opgave 9.2.1 *Lad*

$$A = \{1,2,3\} \times \{1,2,3\}.$$

(Husk er Definition 3.1.1 af det cartesiske produkt.)

Definer en permutation $\sigma \in \Sigma(A)$ ved

$$\sigma(i,j) = \begin{cases} (i+1,j) & \text{hvis } i \in \{1,2\} \\ (1,j) & \text{hvis } i = 3. \end{cases}$$

1) Tegn en tegning af mængden A som en delmængde af planen $\mathbb{R}^2$.

2) Vis at σ har tre baner, nemlig præcis mængderne $\{1\} \times \{1,2,3\}$, $\{2\} \times \{1,2,3\}$ og $\{3\} \times \{1,2,3\}$.

3) Nedskriv de til banerne tilhørende cykler. Vis med pile på din tegning fra 1) hvordan disse cykler "virker" på punkterne i mængden A.

Opgave 9.2.2 *Lad n være givet.*

1) Lav en skitse i planen der "viser" hvordan følgende mængde ser ud:

$$A = \bigcup_{i=1}^{n} \{i\} \times \{1, \ldots, i\}$$

2) Nedskriv definitionen på en permutation af A, der opfylder kravet at der for ethvert $1 \leq i \leq n$ er præcis én bane af længde i. Findes der mere end en permutation af A der opfylder dette krav?

3) Vis, ved at tegne pile på din skitse fra 1) ovenfor, "hvordan" din permutation fra 2) "virker" på punkterne i mængden A.

Opgave 9.2.3 *Lad $n, k \in \mathbb{N}$, hvor $0 \leq k < n$, og betragt mængden $A_n = \mathbb{Z}/n$. Definer en funktion $\sigma_k : A_n \to A_n$ ved $\sigma_k([a]_n) = [a]_n + [k]_n$.*

1) Vis at σ_k er en permutation af A_n (dvs. er en bijektion af A_n på sig selv). Det kan f. eks. gøres ved at finde en invers funktion til σ_k. (Der er faktisk en ret oplagt kandidat til en invers funktion som man nemt kan tjekke virker).

2) Lad nu $n = 20$ og $k = 5$. Nedskriv cyklerne og de tilhørende baner for permutationen σ_k i dette tilfælde.

10
Kombinatorik: To øvelser

Vi følger Lützens DMM i emnet kombinatorik (og dækker kun nogle dele af Lützens kapitel om disse ting). Nedenfor findes to øvelser, der klargør et par detaljer fra forelæsningen.

Øvelse 54 *Lad A være en mængde, $r \in \mathbb{N}$. Lad*

$$\mathbb{P}(n,r) = \{(a_1,\ldots,a_r) \in A^r : (\forall i,j \leq r)\ i \neq j \implies a_i \neq a_j\},$$

og lad

$$\tilde{\mathbb{P}}(n,r) = \{f : \{1,\ldots,r\} \to A : f \text{ er injektiv}\}.$$

1) Vis at $(a_1,\ldots,a_r) \in \mathbb{P}(n,r)$ hvis og kun hvis $(a_1,\ldots,a_r)$ er en r-permutation udtaget fra A, som defineret i Lützens DMM.

2) Vis at funktionen $F : \tilde{\mathbb{P}}(n,r) \to \mathbb{P}(n,r)$ defineret ved

$$F(f) = (f(1),\ldots,f(r))$$

er en bijektion fra $\tilde{\mathbb{P}}(n,r)$ på $\mathbb{P}(n,r)$.

3) Forklar hvorfor foregående viser, at en lige så god (men alternativ) definition af begrebet "en r-permutation udtaget fra A" er at sige, at en r-permutation udtaget fra A er en injektion fra $\{1,\ldots,r\}$ til A.

Øvelse 55 *I forelæsningen indførte jeg som et eksperiment følgende definition: Lad A og B være mængder. En* B-permutation udtaget fra *A (eller mere udførligt,* en B-indiceret permutation udtaget fra *A) er en injektion $f : B \to A$.*

1) Vis at en $\{1,\ldots,r\}$-permutation udtaget fra A er det samme som en r-permutation udtaget fra A.

2) Vis at når A er endelig, da er en A-permutation udtaget fra A det samme som en bijektion af A på sig selv, dvs. det som i DMM kapitel 10 kaldes en permutation af A.

3) Giv et eksempel på at når A er en uendelig mængde, da er en A-permutation udtaget fra A ikke nødvendigvis en permutation af A.

11
Logik og bevisførelse

Matematisk logik er det område af matematik hvori matematisk argumentation og bevisførelse studeres. Logik er derfor "matematik om matematik". Udsagnslogikken, som præsenteres nedenfor, er en simpel model for matematisk argumentation.

Det er vigtigt at forstå at vi her beskriver en *matematisk model* for korrekt matematisk argumentation, ligesom $\mathbb{R}^3$ er en simpel model for det 3-dimensionelle rum vores dagligdag (tilsyneladende) foregår i. Ligesom man i sig selv ikke lærer at bygge et hus eller en bro af at studere geometri, så lærer man heller ikke at lave matematiske beviser af at studere logik. Med det hjælper utvivlsomt.

Vi diskuterer *ikke* prædikatlogik her[1]. Ønsker man en indføring i prædikatlogikken så skal man tage kurset "Introduktion til matematisk logik" på 3. eller 4. studieår.

[1] Udsagnslogikkens store mangel er præcis at den ikke håndterer kvantificering.

11.1 Udsagnslogik

Uformelt er et udsagn noget som "vi siger", som kan tillægges en sandhedsværdi: *sand* eller *falsk*. Et udsagn kaldes også en *påstand*.

Logik handler om forbindelsen mellem udsagn, og om korrekt argumentation: Hvis vi ved, at visse på forhånd givne udsagn er sande eller falske, hvad kan vi så konkludere om andre udsagns sandhedsværdi? I praksis skal logik sikre *konsistens*, dvs. at vores konklusioner ikke strider mod hinanden[2].

[2] Mangel på konsistens ser man ofte i dårlige film eller bøger, hvor de oplysninger vi gives fører til modstridende konklusioner, og historien bliver dermed utroværdig.

Eksempler på konkrete udsagn er "$5 = 2$" eller "Wozniacki vandt Wimbledon i 2016", som når de fortolkes på den mest oplagte måde er falske. Men fortolker vi i stedet 2 og 5 kan som restklasser modulo 3, dvs. som $[2]_3$ og $[5]_3$, og her er ligningen $5 = 2$ faktisk sand; og man kan også forestille sig at Wozniacki var navnet på en fiktiv person i en roman, og så kunne det jo godt være sandt *inden for romanens historie* at denne person vandt Wimbledon i 2016. Et konkret udsagns sandhedsværdi kan derfor (ofte!) være afhængig af den *kontekst* det fortolkes i.

I den teori vi præsenterer nu **findes konkrete udsagn ikke**. I stedet repræsenteres konkrete udsagn abstrakt i vores teori med *udsagnsva-*

riable, $P_1, P_2, P_3 \ldots$, osv. Disse udsagnsvariable kan gives en af to værdier: Sand eller Falsk, som vi repræsenter med hhv. 1 og 0.

Det er som sagt forbindelsen mellem udsagn der interesserer os. Disse forbindelser repræsenteres ved **konnektivsymbolerne**

$$\neg \quad \vee \quad \wedge \quad \Longrightarrow \quad \Longleftrightarrow$$

der henholdsvis kaldes *negation, disjunktion, konjunktion, implikation* og *biimplikation*, og repræsenterer "ikke", "eller", "og", "medfører" og "hvis og kun hvis".

I vores teori findes konkrete udsagn som sagt ikke (de repræsenteres jo symbolsk af udsagnsvariable). Vores teori har kun såkaldt *formelle udsagn*, som vi nu definerer.[3]

[3] Et formelt udsagn kaldes ofte også for en "*Udsagnsform*", hvilket er et godt ord, da det (korrekt) antyder at det er den syntaktiske form som er det væsentlige ved et formelt udsagn.

Definition 11.1.1

1. *Alle udsagnsvariable er formelle udsagn.*
2. *Hvis α og β formelle udsagn, da er følgende også formelle udsagn:*
$$\neg\alpha, (\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \implies \beta) \text{ og } (\alpha \iff \beta).$$
3. *Intet er et formelt udsagn* medmindre *1 og 2 ovenfor kræver det*[4]*, og specielt består alle formelle udsagn endeligt mange symboler.*

[4] Bemærk at betingelse 3 specielt medfører, at et formelt udsagn α som ikke indeholder nogen konnektiver er en udsagnsvariabel. For hvis α ikke indeholder nogen konnektiver, så er det ikke betingelse 2 der kræver at α er et formelt udsagn. Så må det være 1 der kræver det. Ergo er α en udsagnsvariabel.

Uformelt siger definitionen: Formelle udsagn er det, der kan opbygges fra de udsagnsvariable ved at bruge konnektiverne endeligt mange gange som 2 foreskriver. Definitionen er rekursiv, idet definitionen først erklærer i betingelse 1. at alle udsagnsvariable er formelle udsagn, og derefter i betingelse 2. erklærer hvordan nye formelle udsagn kan dannes ud fra gamle. Betingelse 3 udsiger blot, at formelle udsagn ikke kan dannes på andre måder end ved at bruge 1. og 2. i definitionen. Vi har medtaget parenteser i vort symbolsprog, for at sikre entydig læselighed af formelle udsagn.

Man bliver hurtigt træt af at sige 'formelle". Derfor vil vi i det følgende ofte blot skrive *udsagn* når vi egentlig mener *formelle udsagn*.

Bemærk at parenteserne er vigtige for at udsagnene kan læses entydigt: F.eks. er $P_1 \vee P_2 \implies P_7$ ikke et formelt udsagn, for der mangler parenteser[5]. Derimod er $(P_1 \vee (P_2 \implies P_7))$ og $((P_1 \vee P_2) \implies P_7)$ formelle udsagn. (Uformelt droppes den yderste parentes i et sammensat udsagn dog ofte, da de ikke er vigtige for læseligheden.)

[5] Man kan dog indføre en "prioritering" af konnektiverne som kan spare os for at sætte så mange paranteser, se DMM side ??

Udsagn (formelle!), som dannes ved hjælp af 2. i definitionen ovenfor kaldes *sammensatte udsagn*.

Definition 11.1.2 *Sandhedsværdien af de sammensatte udsagn er fastlagt ved følgende* **sandhedstabel**[6] *(1 er "sand", 0 er "falsk"):*

[6] En sandhedstabel kaldes også en *sandhedstavle*. Vi bruger begge ord i flæng.

α	β	$\neg\alpha$	$(\alpha \wedge \beta)$	$(\alpha \vee \beta)$	$(\alpha \implies \beta)$	$(\alpha \iff \beta)$
1	*1*	*0*	*1*	*1*	*1*	*1*
1	*0*	*0*	*0*	*1*	*0*	*0*
0	*1*	*1*	*0*	*1*	*1*	*0*
0	*0*	*1*	*0*	*0*	*1*	*1*

Bemærk at implikationen $\alpha \implies \beta$ er sand *medmindre* forudsætningen ("antecedenten") α er sand, men β ("konsekventen") er falsk. Dette reflekterer, at $\alpha \implies \beta$ udtrykker et *betinget* udsagn: *Hvis* α så β. Derfor giver det mening at når α ikke er sand, så giver $\alpha \implies \beta$ ingen information om β.

Bemærk også at sandhedstabellen faktisk er en rekursiv definition, idet den kun fastlægger sandhedsværdien af udsagnene i de sidste 5 kolonner, hvis man allerede kender sandhedsværdien af udsagnene i de to første kolonner.

Sætning 11.1.3 *Lad γ være et formelt udsagn. Antag at sandhedsværdien af samtlige i γ indgående udsagnsvariable er fastlagt. Da er sandhedsværdien af γ entydigt fastlagt ud fra sandhedstavlen ovenfor.*

Bevis. Hvis γ er en udsagnsvariabel er der intet at bevise (hvorfor?!). Derfor kan vi antage at γ er et sammensat udsagn.

Vi beviser sætningen ved fuldstændig induktion efter $n \in \mathbb{N}$ i følgende prædikat, $P(n)$: *Hvis γ er et formelt sammensat udsagn med n konnektiver og hvori sandhedsværdien af alle de indgående udsagnsvariable er kendt, da er γ's sandhedsværdi (entydigt) fastlagt af sandhedstabellen*.

(Bemærk at 3 i definitionen af formelt udsagn netop sikrer, at der højest indgår endeligt mange konnektiver i et formelt udsagn.)

Induktionsstart: Hvis γ er et sammensat udsagn med ét konnektiv, da må der findes der udsagnsvariable P_i og P_j således at γ er et af følgende udsagn:

$$\neg P_i, (P_i \wedge P_j), (P_i \vee P_j), (P_i \implies P_j) \text{ eller } (P_i \iff P_j).$$

Da det er antaget at sandhedsværdien af de i γ indgående udsagnsvariable kendt, er sandhedsværdien af γ nu (entydigt) fastlagt ud fra sandhedstabelen. Derfor er $P(1)$ sandt.

Induktionstrin: Antag nu at $P(i)$ er sand for alle $i \leq n$. Lad γ være et udsagn hvori der indgår $n+1$ konnektiver, og hvor vi kender sandhedsværdien af alle indgående udsagnsvariable. I følge definitionen af formelt udsagn må der findes formelle udsagn α og β således at γ er præcis[7] et af følgende udsagn:

$$\neg\alpha, (\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \implies \beta) \text{ eller } (\alpha \iff \beta).$$

[7] Hvis man er meget pedantisk bør man faktisk bevise dette (dvs. "præcis").

Da γ har $n+1$ konnektiver må α og β have højest n konnektiver til sammen (overvej). Da $P(i)$ er sand for alle $i \leq n$ følger det at sandhedsværdien af α og β er fastlagt når sandhedsværdien af alle de i γ, og derfor i α og β, indgående udsagnsvariable er kendt. Men når sandhedsværdien af α og β er kendt, da fastligger sandhedstabelen jo entydigt sandhedsværdien af de sammensatte udsagn $\neg\alpha$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \implies \beta)$ og $(\alpha \iff \beta)$, og derfor af γ, som jo er præcis et af disse. □

I praksis siger sætningen at vi kan finde et formelt udsagns mulige sandhedsværdier ved at lave en sandhedstabel. Følgende illustrerer dette samt andre pointer i den foregående tekst.

EKSEMPEL. Lars Løkke Rasmussen har engang sagt i TV Avisen: "Hvis Venstre har vundet valget, jamen så er det da klart, at hvis jeg bliver statsminister, så har Venstre vundet valget. Sådan er det."

Er det, Lars Løkke Rasmussen siger her, sandt?

Løsning: Vi kan bruge P_1 til at repræsentere "Venstre har vundet valget" og P_2 til at repræsentere "Lars Løkke Rasmussen bliver statsminister". Hr. Rasmussens påstand er derfor: $(P_1 \implies (P_2 \implies P_1))$. Vi bruger definitionen af sandhedsværdien af $\implies$ ovenfor til at lave en sandhedstabel:

P_1	P_2	$(P_2 \implies P_1)$	$(P_1 \implies (P_2 \implies P_1))$
1	1	1	1
1	0	1	1
0	1	0	1
0	0	1	1

(For at få den sidste kolonne har vi brugt sandhedstavlen for $\alpha \implies \beta$ på 1. og 3. kolonne.)

Vi ser heraf at $(P_1 \implies (P_2 \implies P_1))$ er sandt ligegyldig hvad sandhedsværdien af P_1 og P_2 er.

Definition 11.1.4 *1) Et udsagn som er sandt ligegyldig hvilken værdi som de indgående udsagnsvariable gives kaldes en* **tautologi**.

2) Et udsagn som er falskt ligegyldig hvilken værdi som de indgående udsagnsvariable gives kaldes en **modstrid** *(eller en* absurditet*).*

3) Vi siger to udsagn α og β er **logisk ækvivalente**, *skrevet*[8] *$\alpha \equiv \beta$, hvis $(\alpha \iff \beta)$ er en tautologi. Sagt på en anden måde: α og β er logisk ækvivalente hvis deres sandhedsværdier er identiske, ligegyldig hvilken sandhedsværdi de indgående udsagnsvariable gives.*

[8] Advarsel: $\alpha \equiv \beta$ er *ikke* et formelt udsagn! Symbolet $\equiv$ bruges til at udtrykke en *relation* mellem formelle udsagn.

Det foregående eksempel viser at $(P_1 \implies (P_2 \implies P_1))$ er en tautologi.

Notation: I det følgende dropper vi nogen gange at skrive *den yderste parentes* i et formelt udsagn, medmindre dette gør læsningen af udsagnet tvetydigt. Parenteser *inde* i et formelt udsagn kan dog meget sjældent droppes, da dette kan forstyrre læsningen af udsagnet (e.g., $\alpha \wedge \beta \implies \alpha$ kan læses på to tilsyneladende helt forskellige måder, nemlig som $(\alpha \wedge \beta) \implies \alpha$ og som $\alpha \wedge (\beta \implies \alpha)$).

Øvelse 56 *Lad α, β og γ være udsagn. Vis, enten ved at lave en sand-*

hedstabel eller ved at argumentere, at følgende udsagn er tautologier:

$$\begin{aligned}
&i.\ (\alpha \implies (\alpha \vee \beta))\\
&ii.\ (\alpha \wedge \beta) \implies \alpha\\
&iii.\ (\alpha \wedge (\alpha \implies \beta)) \implies \beta\\
&iv.\ ((\alpha \vee \beta) \wedge (\neg\alpha \vee \gamma)) \implies (\beta \vee \gamma)\\
&v.\ ((\alpha \iff \beta) \implies (\alpha \implies \beta))
\end{aligned}$$

"Logisk huskeseddel". Følgende er en liste af nyttige logiske ækvivalenser og deres tilhørende tautologier[9]. I listen står α, β og γ for vilkårlige formelle udsagn; yderste parenteser droppes for overskuelighedens skyld.

[9] Sammenlign med Sætning 50 i DMM

	Logisk ækvivalens	**Tilhørende tautologi**
1.	$\neg\neg\alpha \equiv \alpha$	$\neg\neg\alpha \iff \alpha$
2.	$\alpha \wedge \beta \equiv \beta \wedge \alpha$	$(\alpha \wedge \beta) \iff (\beta \wedge \alpha)$
3.	$\alpha \vee \beta \equiv \beta \vee \alpha$	$(\alpha \vee \beta) \iff (\beta \vee \alpha)$
4.	$(\alpha \wedge \beta) \wedge \gamma \equiv \alpha \wedge (\beta \wedge \gamma)$	$((\alpha \wedge \beta) \wedge \gamma) \iff (\alpha \wedge (\beta \wedge \gamma))$
5.	$(\alpha \vee \beta) \vee \gamma \equiv \alpha \vee (\beta \vee \gamma)$	$((\alpha \vee \beta) \vee \gamma) \iff (\alpha \vee (\beta \vee \gamma))$
6.	$\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$	$(\alpha \vee (\beta \wedge \gamma)) \iff ((\alpha \vee \beta) \wedge (\alpha \vee \gamma))$
7.	$\alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$	$(\alpha \wedge (\beta \vee \gamma)) \iff ((\alpha \wedge \beta) \vee (\alpha \wedge \gamma))$
8.	$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$	$\neg(\alpha \wedge \beta) \iff (\neg\alpha \vee \neg\beta)$
9.	$\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$	$\neg(\alpha \vee \beta) \iff (\neg\alpha \wedge \neg\beta)$
10.	$\alpha \implies \beta \equiv \neg\alpha \vee \beta$	$(\alpha \implies \beta) \iff (\neg\alpha \vee \beta)$
11.	$\alpha \implies \beta \equiv \neg\beta \implies \neg\alpha$	$(\alpha \implies \beta) \iff (\neg\beta \implies \neg\alpha)$
12.	$\alpha \iff \beta \equiv (\alpha \implies \beta) \wedge (\beta \implies \alpha)$	$(\alpha \iff \beta) \iff ((\alpha \implies \beta) \wedge (\beta \implies \alpha))$

Bemærkning. På grund af ækvivalenserne 4 og 5 dropper man ofte at sætte parenteser (bortset måske fra de yderste) i lister af konjunktioner og disjunktioner, f. eks. $\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n$. Ækvivalenserne 6 og 7 kaldes nogen gange de *distributive love* for $\vee$ og $\wedge$, og ækvivalenserne 8 og 9 kaldes ofte *De Morgans love*. Alle ækvivalenserne ovenfor kan naturligvis eftervises ved at lave en sandhedstavle.

EKSEMPEL. Vis at

$$\alpha \implies (\beta \implies (\alpha \wedge \beta))$$

er en tautologi ved at omforme den til en kendt tautologi vha. de logiske ækvivalenser ovenfor.

Løsning:

$$\begin{aligned}
\alpha \implies (\beta \implies (\alpha \wedge \beta)) &\equiv \neg(\beta \implies (\alpha \wedge \beta)) \implies \neg\alpha\\
&\equiv \neg(\neg\beta \vee (\alpha \wedge \beta)) \implies \neg\alpha\\
&\equiv (\neg\neg\beta \wedge \neg(\alpha \wedge \beta)) \implies \neg\alpha\\
&\equiv (\beta \wedge (\neg\alpha \vee \neg\beta)) \implies \neg\alpha\\
&\equiv (\beta \wedge (\beta \implies \neg\alpha)) \implies \neg\alpha
\end{aligned}$$

Her har vi omformet ved at først bruge ækvivalensen 11, så 10, så 9, så 8 og 1, så 3 og 10.

Da den sidste linje er en tautologi i følge Øvelse 56 *iii.* er det nu vist at det udsagn vi startede er en tautologi.

Bemærkning. Alle tautologier er selvfølgelig logisk ækvivalente (overvej!), men det kræver ofte lidt kreativitet at omforme en tautologi til en anden (hvis det da overhovedet kan lade sig gøre).

Øvelse 57 *Vis at*

$$(\alpha \wedge \beta) \implies \gamma \equiv \alpha \implies (\beta \implies \gamma)$$

EKSEMPEL. Vis at

$$(\alpha \implies (\beta \vee \gamma)) \implies ((\alpha \vee \beta \vee \gamma) \implies (\beta \vee \gamma))$$

er en tautologi.

Løsning. Fra den foregående øvelse samt ækvivalens 11 har vi

$$\begin{aligned}&(\alpha \implies (\beta \vee \gamma)) \implies ((\alpha \vee \beta \vee \gamma) \implies (\beta \vee \gamma))\\ &\equiv ((\neg\alpha \vee (\beta \vee \gamma)) \wedge (\alpha \vee (\beta \vee \gamma))) \implies (\beta \vee \gamma).\end{aligned}$$

Men den nederstelinje er bare tautologien iv i forklædning, så ovenstående er en tautologi.

11.2 Beviser i udsagnslogikken

Definition 11.2.1 *Et udsagn α kaldes en (tautologisk)* **konsekvens**[10] *af $\{\gamma_1, \ldots, \gamma_m\}$, hvor $m \in \mathbb{N}_0$, hvis der gælder at α er altid er sand når $\gamma_1, \ldots, \gamma_m$ er sande.*

[10] DMM bruger terminologien "gyldig slutning af α fra $\gamma_1, \ldots, \gamma_m$" for det vi har kaldt en konsekvens. Det er såmænd fint nok, men det er forkert når DMM sidestiller dette med begrebet *deduktion*. En deduktion er nemlig noget andet, og vi definerer begrebet deduktion (korrekt) nedenfor.

Øvelse 58 *Bevis at hvis $m \geq 1$ da er α er en tautologisk konsekvens af $\{\gamma_1, \ldots, \gamma_m\}$ hvis og kun hvis*

$$(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies \alpha$$

er en tautologi, og hvis $m = 0$ da er α er en tautologisk konsekvens af $\{\gamma_1, \ldots, \gamma_m\} = \emptyset$ hvis og kun hvis α er en tautologi.

Om $(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies \alpha$ er en tautologi kan naturligvis tjekkes ved at lave en sandhedstavle, men når matematikere vil vide om et udsagn er en konsekvens af andre udsagn, så laver de *beviser*, ikke sandhedstavler. Man siger, at matematikere benytter *den deduktive metode*.

Et bevis er, løst sagt, en endelig liste af udsagn, der starter med vores antagelser, og (forhåbentlig) slutter med vores ønskede konklusion. Beviset bevæger sig frem ad ved at vi undervejs udleder delkonklusioner fra vores antagelser, og det vi allerede har bevist tidligere.

For at beviset skal bevæge sig frem ad har vi altså brug for en måde at drage konklusioner på, en *slutningsregel*. I disse noter hæfter vi

os ved den i matematikken mest brugte slutningsregel, kaldet **Modus Ponens**:

$$\frac{\alpha \qquad \alpha \implies \beta}{\beta}$$

Dette læses som følger: For vilkårlige α og β gælder, at man fra α og $\alpha \implies \beta$ kan slutte (konkludere) β.

Definition 11.2.2 *Lad α og $\gamma_1, \ldots, \gamma_m$ være $m \geq 0$ formelle udsagn*[11]. *En* **deduktion**[12] *af α fra $\gamma_1, \ldots, \gamma_m$ er en endelig liste*

$$\begin{array}{l} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{array}$$

af udsagn sådan at

1. *det sidste udsagn α_n er udsagnet α, som skulle bevises;*
2. *hvert α_i er enten*
   - *(a) en af antagelserne $\gamma_1, \ldots, \gamma_m$; eller*
   - *(b) en i forvejen kendt tautologi; eller*
   - *(c) opnået ved at bruge Modus Ponens på foregående linjer, dvs. findes $j, k < i$ således α_k er det formelle udsagn $\alpha_j \implies \alpha_i$.*

Hvis der findes en deduktion for α fra $\gamma_1, \ldots, \gamma_m$, så skriver vi

$$\gamma_1, \ldots, \gamma_m \vdash \alpha.$$

[11] Vi tillader at $m = 0$, hvilket svarer til at der ikke er nogen γ_i'er.

[12] Man kunne også kalde en deduktion for et bevis, men for at skelne formelle beviser i udsagnslogikken fra beviser andetsteds foretrækker vi ordet deduktion.

Bemærkning. Ovenfor kaldes $\alpha_1, \ldots, \alpha_n$ *linjerne* i deduktionen. Deduktionens *længde* er antallet af linjer (ovenfor n).

Vi giver nu to eksempler på deduktioner. Det andet eksempel viser sig også at være nyttigt senere i kurset.

EKSEMPEL. Vis at

$$\gamma_1, \gamma_2 \vdash \gamma_1 \wedge \gamma_2$$

Løsning: Vi har fra tidligere tautologien

$$\gamma_1 \implies (\gamma_2 \implies (\gamma_1 \wedge \gamma_2)).$$

Derfor kan vi lave følgende deduktion fra $\{\gamma_1, \gamma_2\}$:

$$\begin{array}{l} \gamma_1 \\ \gamma_2 \\ \gamma_1 \implies (\gamma_2 \implies (\gamma_1 \wedge \gamma_2)) \\ \gamma_2 \implies (\gamma_1 \wedge \gamma_2) \\ \gamma_1 \wedge \gamma_2. \end{array}$$

Forklaring: De to første linjer i deduktionen er vores antagelser. Den tredie linje er den ovenfor nævnte tautologi. Den fjerde linje fremkommer ved at bruge Modus Ponens på linje 1 og linje 3. Den 5. linje fremkommer ved at bruge Modus Ponens på linje 2 og linje 4.

Øvelse 59 *Generalisér foregående eksempel ved at vise at*

$$\gamma_1, \ldots, \gamma_n \vdash \gamma_1 \wedge \cdots \wedge \gamma_n.$$

EKSEMPEL. Vis at

$$(\alpha \implies (\beta \vee \gamma)) \vdash ((\alpha \vee \beta \vee \gamma) \implies (\beta \vee \gamma))$$

Løsning. Vi har tidligere set at

$$(\alpha \implies (\beta \vee \gamma)) \implies ((\alpha \vee \beta \vee \gamma) \implies (\beta \vee \gamma))$$

er en tautologi. Derfor har vi følgende deduktion:

$$\begin{array}{l} \alpha \implies (\beta \vee \gamma) \\ (\alpha \implies (\beta \vee \gamma)) \implies ((\alpha \vee \beta \vee \gamma) \implies (\beta \vee \gamma)) \\ ((\alpha \vee \beta \vee \gamma) \implies (\beta \vee \gamma)) \end{array}$$

som viser det ønskede.

Øvelse 60 *Vis at*

$$(\alpha \implies (\beta \vee \gamma)) \vdash (\alpha \vee \beta \vee \gamma) \iff (\beta \vee \gamma).$$

Hint: Man skal lave en deduktion der ender med det ønskede udsagn. Kombinér det foregående eksempel og tautologien i. fra Øvelse 56.

Vi vil ikke bevise følgende (vigtige) sætning i forelæsningerne i dette kursus, men den er rar at kende. Den siger, essentielt, at et udsagn α er en konsekvens af andre udsagn $\gamma_1, \ldots, \gamma_m$ hvis og kun hvis der findes en deduktion af α fra $\gamma_1, \ldots, \gamma_m$.

Sætning 11.2.3 (Udsagnslogikkens fuldstændighed, endelig version) *Hvis α og $\gamma_1, \ldots, \gamma_m$ er formelle udsagn, og hvor $m \in \mathbb{N}_0$, da gælder $\gamma_1, \ldots, \gamma_m \vdash \alpha$ hvis og kun hvis α er en konsekvens af $\gamma_1, \ldots, \gamma_m$.*

Bevis.[13] Antag først at α er en konsekvens af $\gamma_1, \ldots, \gamma_m$ og $m > 0$. Så er $(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies \alpha$ er en tautologi. Lad

$$\begin{array}{l} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{array}$$

[13] Beviset indgår ikke i pensum! Dog skal det siges, at hvis man kan forstå dette bevis, så har man også forstået alle grundbegreberne i udsagnslogikken virkelig godt, så det er nok værd at prøve kræfter med.

være en deduktion af $\gamma_1 \wedge \cdots \wedge \gamma_m$ fra $\gamma_1, \ldots, \gamma_m$ (som findes pga. Øvelse 59). Derfor er

$$\begin{array}{l} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \\ (\gamma_1 \wedge \cdots \wedge \gamma_m) \implies \alpha \\ \alpha \end{array}$$

en deduktion af α fra $\gamma_1, \ldots, \gamma_m$. Så vi har vist at $\gamma_1, \ldots, \gamma_m \vdash \alpha$.

Tilfældet $m = 0$ er trivielt (overvej!).

For den modsatte retning beviser vi ved fuldstændig induktion (efter n) følgende påstand, $P(n)$: Hvis der er en deduktion med n linjer af α fra $\gamma_1, \ldots, \gamma_m$, så er $(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies \alpha$ en tautologi.

Basistrin, $n = 1$: Hvis α har en deduktion med kun en linje fra $\gamma_1, \ldots, \gamma_m$ som må α være en tautologi eller α må være en af udsagnene $\gamma_1, \ldots, \gamma_m$. Men så er $(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies \alpha$ en tautologi (overvej).

Induktionstrin: Antag påstanden holder for n, og lad α være et udsagn der har en deduktion fra $\gamma_1, \ldots, \gamma_m$ med $n+1$ linjer,

$$\begin{array}{l} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n+1}. \end{array}$$

Hvis α er en tautologi, eller α er et af udsagnene $\gamma_1, \ldots, \gamma_m$, så følger som i basistrinnet at $(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies \alpha$ er en tautologi.

Antag derfor at α opnås ved at bruge Modus Ponens på tidligere linjer, α_i og α_k, hvor $i, k \leq n$, og hvor α_k er $\alpha_i \implies \alpha$. Fra induktionsantagelsen er $(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies \alpha_i$ og $(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies \alpha_k$ tautologier. Da α_k er udsagnet $(\alpha_i \implies \alpha)$ følger at

$$(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies (\alpha_i \implies \alpha)$$

er en tautologi. Herfra ses at

$$(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies \alpha$$

er en tautologi, idet der gælder at hvis $(\gamma_1 \wedge \cdots \wedge \gamma_m)$ er sand, da er α_i og $\alpha_i \implies \alpha$ sande, og dermed følger at α er sand. (Lav eventuelt en sandhedstavle hvis ikke den foregående sætning overbeviste dig.)□

11.3 Bevistyper

Vi diskuterer nu forskellige bevistyper som man ofte møder i matematik ud fra deres baggrund i udsagnslogikken. Med henblik på at give simple

eksempler på de forskellige bevistyper indfører vi følgende definition fra elementær talteori.

Definition 11.3.1 *Lad $n, q \in \mathbb{N}$. Vi siger at n er et* **multiplum** *af q hvis der findes $m \in \mathbb{N}$ sådan at $n = qm$.*

Et multiplum af 2 *kaldes et* **lige** *tal.*

Bevismetoden "direkte bevis"

Skematisk kan et direkte bevis beskrives som følger:

Problem: Vi antager $\gamma_1, \ldots, \gamma_m$ holder, og ønsker at bevise at $\beta \implies \alpha$.

Løsning: Vi antager $\gamma_1, \ldots, \gamma_m$ *og* β holder, og beviser α.

Baggrunden for at denne metode virker er følgende Sætning.

Sætning 11.3.2 (Deduktionsteoremet) *Lad α, β og $\gamma_1, \ldots, \gamma_m$ være formelle udsagn. Da gælder: Hvis*

$$\gamma_1, \ldots, \gamma_m, \beta \vdash \alpha$$

så

$$\gamma_1, \ldots, \gamma_m \vdash \beta \implies \alpha.$$

Bevis. Vi udnytter Fuldstændighedssætningen: Hvis $\gamma_1, \ldots, \gamma_m, \beta \vdash \alpha$, så er

$$(\gamma_1 \wedge \cdots \wedge \gamma_m \wedge \beta) \implies \alpha$$

en tautologi. Fra Øvelse 57 er dette udsagn logisk ækvivalent med

$$(\gamma_1 \wedge \cdots \wedge \gamma_m) \implies (\beta \implies \alpha),$$

som derfor er en tautologi. Derfor er $(\beta \implies \alpha)$ en konsekvens af $\gamma_1, \ldots, \gamma_m$, og Fuldstændighedssætningen giver derfor at

$$\gamma_1, \ldots, \gamma_m \vdash \beta \implies \alpha.$$

som ønsket. □

EKSEMPEL PÅ ET DIREKTE BEVIS. Bevis at hvis n er et lige (naturligt) tal så er n^2 også lige.

Løsning. Bemærk at vi ønsker at vise en implikation. Deduktionsteoremet siger at vi kan antage at n er lige, og arbejde derfra. Da kan n skrives som $n = 2m$. Derfor er

$$n^2 = (2m)^2 = 2m2m = 2(m2m),$$

hvilket viser at n^2 er lige, som ønsket.

Bemærkning. Ovenstående eksempel på et direkte bevis ligger jo ret langt fra at være et formelt bevis, men kan nok godt med nogen umage

gøres gøres formelt. Antagelserne $\gamma_1, \ldots, \gamma_m$ ville da være regnereglerne som vi ved er sande for de naturlige tal (og som jo bliver brugt i udregningen ovenfor). I praksis laver matematikere stort set aldrig formelle beviser, men i princippet skal ethvert matematisk bevis kunne laves om til et formelt bevis. Med andre ord: Selvom i ikke nedskriver formelle beviser i matematikken, så skal detaljegraden i vores beviser være høj nok til, at man routinemæssigt kunne omformulere beviset til et formelt bevis.

Øvelse 61 *Vis at den modsatte retning i forrige sætning også gælder: Hvis*

$$\gamma_1, \ldots, \gamma_m \vdash \beta \implies \alpha$$

så

$$\gamma_1, \ldots, \gamma_m, \beta \vdash \alpha$$

Hint: En mulighed er at bruge Sætning 11.2.3, men det er lidt snyd. Det er bedre at indse at en $\beta \implies \alpha$ fra $\{\gamma_1, \ldots, \gamma_m\}$ kan "forlænges" til en deduktion af α fra $\{\gamma_1, \ldots, \gamma_m, \beta\}$.

Bevismetoden "Kontraposition".

Skematisk kan et bevis ved kontraposition beskrives som følger:

Problem: Vi antager $\gamma_1, \ldots, \gamma_m$ holder, og ønsker at bevise at $\beta \implies \alpha$.

Løsning: Vi antager $\gamma_1, \ldots, \gamma_m$ *og* $\neg\alpha$ holder, og beviser $\neg\beta$.

Baggrunden for at denne metode virker er følgende.

Lemma 11.3.3 (Kontraposition) *Lad α, β og $\gamma_1, \ldots, \gamma_m$ være formelle udsagn. Da gælder: Hvis*

$$\gamma_1, \ldots, \gamma_m, \neg\alpha \vdash \neg\beta$$

så

$$\gamma_1, \ldots, \gamma_m \vdash \beta \implies \alpha.$$

Øvelse 62 *Vis den foregående sætning. Hint: Brug deduktionsteoremet sammen med tautologien $(\neg\alpha \implies \neg\beta) \implies (\beta \implies \alpha)$.*

EKSEMPEL PÅ ET BEVIS VED KONTRAPOSITION. Lad n være et helt tal. Vis at hvis n ikke er lige, så er $n+2$ ikke lige.

Løsning:[14] Antag at $n+2$ er lige, dvs. der findes m så $n+2 = 2m$. Så følger at

$$n = 2m - 2 = 2(m-1).$$

Derfor følger at n er lige. □

[14] Bemærk at da både antecedenten ("n er ikke lige") og konklusionen ("$n+2$ er ikke lige") ligger problemet selv op til at man bruger kontraposition.

Bevismetoden "Bevis ved modstrid"

Skematisk kan et bevis ved modstrid beskrives som følger:

Problem: Vi antager $\gamma_1, \ldots, \gamma_m$ holder, og ønsker at bevise at α.

Løsning: Vi antager $\gamma_1, \ldots, \gamma_m$ *og* $\neg\alpha$ holder, og beviser $\beta \wedge \neg\beta$ for et eller andet udsagn β.

Baggrunden for at denne metode virker er følgende.

Lemma 11.3.4 (Bevis ved modstrid, "Reductio ad absurdum") *Lad α, β og $\gamma_1, \ldots, \gamma_m$ være formelle udsagn. Da gælder: Hvis*

$$\gamma_1, \ldots, \gamma_m, \neg\alpha \vdash \beta \wedge \neg\beta$$

så

$$\gamma_1, \ldots, \gamma_m \vdash \alpha.$$

Bevis. Fra sætningen om kontraposition følger at

$$\gamma_1, \ldots, \gamma_m \vdash (\neg(\beta \wedge \neg\beta) \implies \alpha).$$

Da $\neg(\beta \wedge \neg\beta)$ er en tautologi kan en deduktion fra $\gamma_1, \ldots, \gamma_m$ af $(\neg(\beta \wedge \neg\beta) \implies \alpha)$ forlænges med linjerne

$$\neg(\beta \wedge \neg\beta)$$
$$\alpha$$

og derfor findes en deduktion af α fra $\gamma_1, \ldots, \gamma_m$, som ønsket. (Den sidste linje, som er α, opnås ved Modus Ponens; overvej!)

EKSEMPEL PÅ ET BEVIS VED MODSTRID. Lad n være et naturligt tal. Vis at $2n + 1$ ikke er lige.

Løsning: Antag at $2n + 1$ er lige. Så findes $m \in \mathbb{N}$ så at $2n + 1 = 2m$. Derfor følger at

$$1 = 2m - 2n = 2(m - n).$$

Derfor er $m - n > 0$ (idet $1 > 0$), og da $m - n$ er et helt tal gælder så at $m - n \geq 1$. Men så får vi

$$2 \leq 2(m - n) = 1,$$

hvilket er en modstrid.[15] □

[15] Vi har anstrengt os for at give et bevis, der kun bygger på nogen meget enkle regneregler. De fleste vil nok synes det er oplagt at 1 ikke er et multiplum af 2, og derfor at allerede linje 3 i beviset er en modstrid.

Metoden "Modeksempel"

Denne metode skiller sig lidt ud fra de andre, for her ønsker vi at vise at noget *ikke* kan bevises ud fra givne antagelser. Strukturen er som følger:

Problem: Vi ønsker at vise at man *ikke* kan bevise α fra $\gamma_1, \ldots, \gamma_m$, dvs.

$$\gamma_1, \ldots, \gamma_m \nvdash \alpha.$$

Løsning: Vi finder en tildeling af sandhedsværdier til de udsagnsvariable som gør $\gamma_1, \ldots, \gamma_m$ sande, men samtidig gør α falsk.

Øvelse 63 *Brug Fuldstændighedssætningen til at begrunde metoden "Modeksempel".*

Bevismetoderne "Opdeling i tilfælde" og "Kædebevis"

Der er to yderligere metoder, der bruges ofte i beviser: Opdeling i tilfælde, og Kædebevis (også kaldet "kædeslutning" eller "hypotetisk syllogisme"). Vi fremhæver disse, ikke blot fordi de er nyttige, men også fordi de hver især indeholder en fælde, som er nem at falde i, og som ofte er årsag til fejl i beviser, også blandt matematikere på højeste niveau.

Opdeling i tilfælde. Metoden er så naturlig at læseren helt sikkert har anvendt den mange gange tidligere. Skematisk kan metoden beskrives som følger:

Problem: Vi antager $\gamma_1, \ldots, \gamma_m$ og ønsker at bevise β.
Løsning: Vi finder et udsagn δ som giver en naturlig opdeling af beviset: Hvis vi antager $\gamma_1, \ldots, \gamma_m$ og δ så kan vi bevise β, *og* hvis vi antager $\gamma_1, \ldots, \gamma_m$ og $\neg\delta$ så kan vi bevise β.

Metodens gyldighed er baseret på følgende:

Sætning 11.3.5 (Opdeling i to tilfælde) *Lad $\gamma_1, \ldots, \gamma_m$, β, og δ være udsagn. Hvis*

$$\gamma_1, \ldots, \gamma_m, \delta \vdash \beta$$

og

$$\gamma_1, \ldots, \gamma_m, \neg\delta \vdash \beta$$

da gælder

$$\gamma_1, \ldots, \gamma_m \vdash \beta$$

Vi overlader beviset til læseren. Man kan naturligvis også formulere en sætning med opdeling i flere end to tilfælde.

EKSEMPEL PÅ ET BEVIS VED OPDELING I TILFÆLDE. Lad $m, n \in \mathbb{N}_0$. Vis at hvis $mn = 0$ så er $m = 0$ eller $n = 0$.

Løsning. Tilfælde 1: $m = 0$. Så er der intet at bevise.

Tilfælde 2: $m \neq 0$. Så er $m \geq 1$. Da $n \geq 0$ følger at $mn \geq n$. Da $mn = 0$ følger at $0 \geq n$, og derfor at $n = 0$, idet $n \in \mathbb{N}_0$ er forudsat.[16] □

[16] Jeg har forsøgt at give et bevis der bruger så få egenskaber ved $\mathbb{N}_0$ som muligt.

Advarsel: Her er en typisk måde, som opdeling i tilfælde bringer folk på afveje: Først finder man et δ, som er en god kandidat til at opdele beviset efter: Når man antager δ, så følger β, som ønsket. Nu antager man så $\neg\delta$, men det viser sig at man har brug for et udsagn, η, som er lidt stærkere end $\neg\delta$, for at bevise β i dette tilfælde. Men da η

er stærkere end $\neg\delta$, så er $\neg\eta$ *svagere* end δ. Desværre glemmer folk, eller sjusker med, at gå tilbage og bevise at β følger fra $\neg\eta$. Sagt på en anden måde: De har glemt at redegøre for tilfældet $(\neg\delta \wedge \neg\eta)$.

Kædebevis. Kædebevis, som også kaldes hypotetisk syllogisme, kan uformelt symboliseres som følger:

$$\begin{aligned} \gamma &\implies \alpha \\ \alpha &\implies \beta \\ \therefore \gamma &\implies \beta \end{aligned}$$

Skematisk kan metoden beskrives som følger:

Problem: Vi antager $\gamma_1, \ldots, \gamma_m$ og ønsker at bevise β.
Løsning: Vi finder et udsagn α og beviser α fra $\gamma_1, \ldots, \gamma_m$, og derefter beviser vi β fra $\gamma_1, \ldots, \gamma_m$ og α.

Følgende sætning viser at metoden virker.

Sætning 11.3.6 (Kædebevis) *Lad $\gamma_1, \ldots, \gamma_m$, β, og α være udsagn. Hvis*

$$\gamma_1, \ldots, \gamma_m \vdash \alpha$$

og

$$\gamma_1, \ldots, \gamma_m, \alpha \vdash \beta$$

da gælder

$$\gamma_1, \ldots, \gamma_m \vdash \beta$$

Vi overlader til læseren at bevise denne sætning.

Metoden er uhyre vigtig, særligt i lange beviser og i matematisk forskning, da den gør det muligt at ligge en *plan* for et bevis: Trin 1: Bevis α. Trin 2: Antag α og bevis β. Man kan naturligvis også formulere en mere generel sætning med opdeling i flere end to trin.

EKSEMPEL PÅ ET KÆDEBEVIS. Bevis, at hvis n er et multiplum af både 2 og 3, da er n et multiplum af 6.

Løsning: Vi bryder beviset ned i to trin, hvor Trin 2 giver den ønskede konklusion. Trin 1 opnår et mellemresultat, der bruges i beviset for trin 2.

Trin 1: Hvis $3q$ er lige da er q lige.

Bevis for Trin 1. Da $3q$ er lige kan vi finde m så at $3q = 2m$. Da $1 = 3 - 2$ har vi

$$q = 1q = (3-2)q = 3q - 2q = 2m - 2q = 2(m-q).$$

Dette viser at q er et multiplum af 2, så derfor er q lige.

Trin 2: Hvis n er et multiplum af både 2 og 3 da er n et multiplum af 6.

Bevis for Trin 2. Da n er et multiplum af 3 kan det skrives som $n = 3q$. Da n er et multiplum af 2 er n lige, så det følger fra Trin 1 at q er lige, dvs. $q = 2p$ for et $p \in \mathbb{N}$. Derfor har vi

$$n = 3q = 3 \cdot 2p = 6p,$$

hvilket viser at n er et multiplum af 6. □[17]

[17] Læseren opmuntres til at at overveje hvad der ville ske hvis vi i stedet for 2, 3 og 6 ovenfor havde brugt 4, 6 og 24 (f. eks.).

Advarsel: Ligesom opdeling i tilfælde, så bringer også kædeslutning undertiden folk på afveje. Typisk sker der det, at man finder et α sådan at man fra α kan bevise β. Det er en god start, men nu viser det sig at man fra $\gamma_1, \ldots, \gamma_m$ kun kan bevise α', som er et svagere udsagn end α. Uden videre omhu overbeviser man sig selv om at "stort set det samme bevis for β ud fra α stadig virker hvis α erstattes med α'". Desværre er det præcis her man får lavet en fejl, idet beviset for β fra α ikke kan modificeres til at bevise β fra α', men det ville man kun have opdaget ved at være meget omhyggelig.

Som sagt: selv store matematikere i den internationale forsknings højeste luftlag falder fra tid til anden i disse fælder. Det giver meget røde ører hos synderen hvis beviset er nået ud til offentligheden før fejlen findes. Ved at være opmærksom på farerne kan man dog udvise den nødvendige omhu, og undgå selv at falde i.

Bemærkning. Ovenstående bevismetoder er langt de mest almindelige, men det er ikke alle. I opgaverne i slutningen af kapitlet kan man finde eksempler på andre bevismetoder.

Øvelse 64 *Der er endnu en bevismetode som vi bruger hele tiden, men som folk aldrig nævner. Det er bevis ved ækvivalens. Den kan skematisk beskrives som følger:*

Problem: *Vi antager $\gamma_1, \ldots, \gamma_m$, og ønsker at bevise β.*
Løsning: *Vi finder et udsagn α og beviser fra $\gamma_1, \ldots, \gamma_m$ udsagnene $\alpha \iff \beta$ og α.*

Nedskriv en sætning der retfærdiggør denne metode.

Bemærkning: Et meget ofte brugt særtilfælde af foregående øvelses bevismetode er når $\alpha \iff \beta$ er en tautologi. Det har vi faktisk gjort allerede flere gange ovenfor!