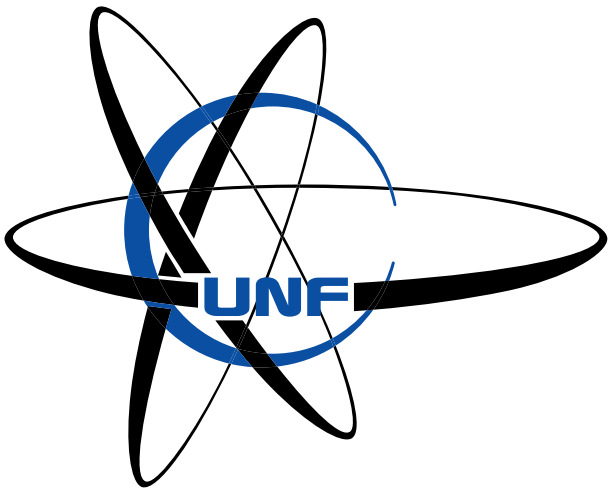


UNF Matematik Camp 2022

Faglige:

Bjørk Jackson Jakobsen (hjælper)	bjj@unf.dk
Trine Rynord (hjælper)	tr@unf.dk
Rasmus Frigaard Lemvig	rle@unf.dk
Karl Bernhard Nielsen	karn@unf.dk
Erik Søndergård Gimsing (ansvarlig)	esg@unf.dk
Marie Stuhr Kaltoft (TEXnisk ansvarlig)	mark@unf.dk
Nanna Wiberg Nielsen	nwn@unf.dk
Anna Mai Østergård	moe@unf.dk
Anne-Kristine Haunsvig	akha@unf.dk
Mathias Weirsøe Klitgaard	mwk@unf.dk

Ungdommens Naturvidenskabelige Forening

Kompendium til UNF Matematik Camp 2022

Kompendiet er skrevet af Erik Søndergaard Gimsing, Marie Stuhr Kaltoft, Rasmus Frigaard Lemvig, Karl Bernhard Nielsen, Anne-Kristine Haunsvig, Mathias Weirsøe Klitgaard, Anna Mai Østergård, Nanna Wiberg Nielsen, Bjørk Jackson Jakobsen og Trine Rynord.

Layout: Esben Skovhus Ditlefsen på forarbejde af Niels Jakob Søe Loft og Mick Althoff Kristensen.

Opsætning/TEXnisk ansvarlig: Marie Stuhr Kaltoft.

Indholdsfortegnelse

Symbolliste

Faglig Introduktion

$\{\cdots\}$	Mængde.
$f\colon A \to B$	Afbildning/funktion.
$f(A)$	Billedet af f.
f^{-1}	Invers funktion.
$f^{-1}(S)$	Urbilledet af S, hvor $f\colon A \to B$ og $S \subseteq B$.
$\subseteq$	Delmængde af.
$\setminus$	Differensmaengde.
$\emptyset$	Den tomme mængde.
$\cap$	Fællesmængde.
$\cup$	Foreningsmænde.
$[a,b]$	Intervallet mellem to reelle tal a og b.
$A^{\complement}$	Komplementærmængden af A.
$\mathcal{P}(A)$	Potensmængden af en mængde A.
$\mathbb{N}$	Naturlige tal.
$\mathbb{Q}$	Rationale tal.
$\mathbb{R}$	Reelle tal.
$\mathbb{Z}$	Hele tal.
X	Universalmængden.
$\in$	Element i.
$\notin$	Ikke element i.
$\neg$	Ikke.

$\Rightarrow$	Implikationspil.
$\Leftrightarrow$	Biimplikationspil.
$\lightning$	Modstrid.
sfd	Største fælles divisor.
mfm	Mindste fælles multiplum.
$\exists$	Der eksisterer.
$\exists!$	Der eksisterer én.
$\forall$	For alle.

Sandsynlighedsteori

$\binom{n}{r}$	Binomialkoefficient. Udtales "n vælg r".
$x + y$	En binomial.
$n!$	Fakultet. Kort måde at skrive $n \cdot (n-1) \cdots 2 \cdot 1$.
$\lim_{N \to \infty}$	Grænseværdi, når N går mod uendelig.
$\sum$	Sumtegn.
S	Udfaldsrum.
A	Udfald/begivenhed.
$A \cup B$	Foreningen af to udfald.
P	En sandsynlighed
$X \colon S \to \mathbb{R}$	Stokastisk variabel.
$P(A \mid B)$	Betinget sandsynlighed for A givet B.
$(X \in B)$	Urbilledet $X^{-1}(B)$.
p_X	Tæthedsfunktion, $p_X = P(X = x)$.
PMF	Forkortelse for tæthedsfunktion.
EX	Middelværdien af X.
$E\left(X^k\right)$	Det $k$te moment.
VX	Variansen af X.

$F(x) = P(X \leq x)$	Fordelingsfunktion.
$H_{n,\alpha}$	Generaliserede harmoniske tal.
$m(t)$	Momentfrembringende funktion.

Gruppeteori

φ	Udtales "phi". Et græsk bogstav. Ofte brugt om en afbildning, især om isomorfier.
$(G,\star)$	En gruppe med kompositionen $\star$. G er mængden som gruppen er defineret over.
$\star$	Kompositionsregel.
$\langle a \rangle$	Undergruppen af G, som er frembragt af a.
e	Neutralelementet.
g^{-1}	Den inverse til g.
$\lvert g \rvert$	Ordenen af elementet g.
$\lvert G \rvert$	Ordenen af gruppen G.
$f(G)$	Billedet af f - mængden af elementer, der bliver ramt, når vi anvender f på G.
$\mathbb{Z}/n\mathbb{Z}$	Den additive gruppe af de n restklasser modulo n.
$[a]_n$	Restklassen for a modulo n. Altså heltal b, der kan skrives på formen $b = a + n \cdot k$, hvor k også er et heltal.
$(\mathbb{Z}/p\mathbb{Z})^\times$	Den multiplikative gruppe af de p restklasser modulo p uden $[0]_p$. p er her et primtal.
S_n	Permutationsgruppen af n elementer.
D_{2n}	Diedergruppen af orden $2n$.

σ	Udtales "sigma". Et græsk bogstav. Ofte brugt om en permutation.
τ	Udtales "tau". Et græsk bogstav. Ofte brugt om en permutation.
Z_n	Den cykliske gruppe af orden n.

Knudeteori

D	Kæde- eller knudediagram.
$\langle D \rangle$	Kauffman parentes.
$K1$, $K2$, $K3$	Kauffman aksiomerne.
K	Knude.
C	Kæde komponent.
c	Krydsning.
L	Kæde.
$R1$, $R2$, $R3$	Reidemeister træk.
sD	Tilstanden af et diagram D.
$\|sD\|$	Antallet af komponenter i diagrammet sD.
$\|s\|$	Værdien af en tilstand s.
b	Fletning.
e	Triviel fletning.
σ_i	Frembringer af fletning gruppen.
B_n	n-fletning gruppen.
p_{ij}	Frembringer af den ægte fletning gruppe.
P_n	n-ægte fletning gruppen.
k	Antallet af kanter på en overflade.
Σ	Overflade.
Σ_D	Seifert overfladen af et diagram D.

	Negativ udjævning.
	Positiv udjævning.

	Højre krydsning.
	Venstre krydsning.
L_+, L_-, L_0	Skein diagrammer af L.
	Ikke-knuden.

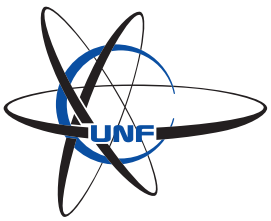
$V(L)$	Jones polynomium.
$\mathbb{Z}[X_1,\ldots,X_N]$	Laurent polynomium.
$M(f)$	Største potens af et polynomium f.
$m(f)$	Laveste potens af et polynomium f.
$\text{sign}(c)$	Fortegnet af krydsning.
$\text{span}(f)$	Spændet af polynomium f.
$s(c)$	Tilstanden af en krydsning.
$w(D)$	Vridning.
$\chi(\Sigma)$	Eulerkarakteristik af en overflade.
$b(L)$	Fletning indekset af en kæde.
$g(K)$	Genus af en knude.
$g(\Sigma)$	Genus af en overflade.

$\simeq$	Ækvivalent med.
$\sqcup$	Disjunkt forening.
rL	Modsætningen af L.
mL	Spejlbilledet af L.
$\#$	Knudesum.
$[x,y]$	Kommutator.

Kombinatorisk Spilteori

0	Nulspillet. Spillet, hvor ingen kan trække.
$\star$	Spillet, hvor begge spillere kan trække til 0. Udtales "stjerne".
$\mathcal{G}^V$	Mængden af spil, som Venstre kan trække til.

$\mathcal{G}^H$	Mængden af spil, som Højre kan trække til.
$\mathcal{V}$	Mængden af spil, hvor Venstre altid vinder.
$\mathcal{H}$	Mængden af spil, hvor Højre altid vinder.
$\mathcal{F}$	Mængden af spil, hvor første spiller vinder.
$\mathcal{A}$	Mængden af spil, hvor anden spiller vinder.
$G + H$	Sumspillet af G og H.
$-G$	Negationen af spillet G, så $G+(-G)$ er et nulspil.
$G = H$	Lighed mellem spil, så $G - H$ er et nulspil.
$G > H$	$G - H$ er et positivt spil.
$G < H$	$G - H$ er et negativt spil.
$G \parallel H$	$G - H$ er et uldent spil.
$G \geq H$	Venstre vinder $G - H$, når Højre starter.
$G \leq H$	Højre vinder $G - H$, når Venstre starter.
$G \triangleright H$	Venstre vinder $G - H$, når Venstre starter.
$G \triangleleft H$	Højre vinder $G - H$, når Højre starter.
$\uparrow$	Spillet $\{0\|\star\}$. Udtales "pil op".
$\downarrow$	Negationen af $\uparrow$.



0 Faglig Introduktion

I dette introduktions kapitel kigger vi på nogle centrale begreber for højere matematik. Vi kigger på begreberne *mindste fælles divisor, største fælles multiplum, mængder, mængdeoperationer, udsagn, beviser* og *funktioner*.

1 Talteori

Vi starter med et mini-kapitel om talteori. Vi arbejder i dette kapitel kun med de positive heltal $1, 2, 3, ...$ også kendt som de *naturlige tal*, hvilket skrives med symbolet $\mathbb{N}$.

Vi taler i talteori om, at et tal kan dele et andet tal. Dette betyder, at man kan dividere et tal med et andet. F.eks. deler tallet 3 tallet 12, fordi $12/3 = 4$, som er et naturligt tal. Derimod deler tallet 3 ikke 11, fordi $11/3 = 3{,}75$, som ikke er et naturligt tal. Vi har nu bogens første definition.

Definition 1.1.

1. Et tal a *deler* b skrevet $a|b$ hvis $b = a \cdot n$ hvor a, b, n alle er naturlige tal.

2. Lad a, b, d være naturlige tal. Da er d en *fælles divisor* for a og b hvis $d|a$ og $d|b$.

3. Lad a og b være naturlige tal. Den *største fælles divisor* for a og b, skrevet $\text{sfd}(a, b)$, er den største divisor, som a og b har tilfælles.

Eksempel 1.2. Tallet 12 har divisorerne 1, 2, 3, 4, 6 og 12 da disse tal er de eneste der dividere 12. Tallet 30 har divisorerne 1, 2, 3, 5, 6, 10, 15 og 30. Tallene 30 og 12 har dermed de fælles divisorer 1, 2, 3, 6. Den største af disse fælles divisorer er 6, dermed er $\text{sfd}(12, 30) = 6$. ∘

Den sidste ting vi vil tage med i dette afsnit er *mindste fælles multiplum*.

Definition 1.3. Lad a og b være naturlige tal. Da er det *mindste fælles multiplum* af a og b, skrevet $\text{mfm}(a, b)$, det mindste tal d, hvor $a|d$, og $b|d$. Eksempelvis er $\text{mfm}(6, 15) = 30$ da både 6 og 15 deler 30, men ingen tal mindre end 30 kan deles af både 6 og 15.

2 Mængder

En *mængde* er en samling af *elementer*. Vi skriver oftest mængder i tuborgparenteser $\{\cdots\}$. Mængden af talene 7, 9 og 13 kan dermed skrives som

$$\{7, 9, 13\}.$$

Elementer behøves ikke nødvendigvis at være tal. Eksempelvis kan man også have mængden af danske universiteter

$$\{\text{AAU}, \text{AU}, \text{CBS}, \text{DTU}, \text{ITU}, \text{KU}, \text{RUC}, \text{SDU}\}.$$

Et element kan højst være i en mængde én gang. Så eksempelvis vil

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

ikke være gyldig, da 3 skrives to gange, men mængden

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

vil være en gyldig mængde.

Nogle mængder bruges ofte og har dermed deres eget symbol. I kender fra kapitlet før $\mathbb{N}$ som symbolet for de *naturlige tal*

$$\mathbb{N} = \{1, 2, 3, ...\}.$$

I kender måske også $\mathbb{Z}$, som symbolet for alle heltal

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

En anden vigtig mængde er den *tomme mængde* $\emptyset$, som er mængden uden nogle elementer

$$\emptyset = \{\}.$$

Andre vigtige mængder er mængden af alle brøker også kaldt de *rationale tal*, der betegnes med symbolet $\mathbb{Q}$, og mængden af alle kommatal, også kaldt de *reelle tal*, som betegnes med symbolet $\mathbb{R}$.

Lad os introducere nogle nye symboler. Det første symbol $\in$ betyder "er element i". Eksempelvis betyder

$$2 \in \mathbb{N},$$

at 2 er et element i de naturlige tal. Med andre ord er 2 et naturligt tal. Derimod betyder

$$-1 \notin \mathbb{N},$$

at -1 ikke er et element i de naturlige tal. Dette er sandt, da $\mathbb{N}$ er mængden af alle positive heltal, og -1 er et negativt tal.

Det andet symbol er $|$, der betyder "hvorom der gælder", "således at" eller lignende. Eksempelvis betyder

$$\left\{ n^2 \mid n \in \mathbb{N} \right\},$$

mængden af tal opløftet i anden, hvorom der gælder, at det opløftede tal er et naturligt tal. Med andre ord mængden af kvadrattal

$$\{1, 4, 9, 16, 25, \dots\}.$$

Et andet eksempel er mængden af lige tal som kan skives som

$$\{2n \mid n \in \mathbb{Z}\}.$$

Prøv at læse denne mængde højt og overbevis dig selv om, hvorfor denne mængde er mængden af alle lige tal.

Nogle gange er alle elementer i en mængde indenholdt i en anden mængde. Eksempelvis indeholder heltallen $\mathbb{Z}$ alle de naturlige tal $\mathbb{N}$. Dette betyder at $\mathbb{N}$ er en delmængde af $\mathbb{Z}$, der skrives

$$\mathbb{N} \subseteq \mathbb{Z}.$$

Et andet eksempel er

$$\{1, 2\} \subseteq \{1, 2, 3, 4\},$$

fordi at alle elementerne i den første mængde $\{1, 2\}$ også er elementer i den anden mængde $\{1, 2, 3, 4\}$. Andre eksempler er

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

$$\{1, 2, 3\} \subseteq \{1, 2, 3\}$$

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

Prøve at overvej hvorfor $\emptyset$ er en delmængde (er der nogen elementer i $\emptyset$ der *ikke* ligger i $\{1, 2, 3\}$?). Vi siger at to mængder A og B er lig hinanden, hvis $A \subseteq B$, og $B \subseteq A$. Dette skriver vi som $A = B$.

3 Mængdeoperationer

Nu har vi styr på hvad en mængde er, men vi vil også godt kunne regne med dem. Lad A og B være to vilkårlige mængder. Da betyder

- $A \cup B$ *foreningsmængden* af A og B, eller med andre ord "mængden af alle elementer, der findes i enten A eller B". Eksempelvis

$$\{1,2,3,4\} \cup \{3,4,5\} = \{1,2,3,4,5\}.$$

- $A \cap B$ *fællesmængden* af A og B, eller med andre ord "mængden af de elementer der både er i A og i B". Eksempelvis

$$\{1,2,3,4\} \cap \{3,4,5\} = \{3,4\}.$$

- $A \setminus B$ er *differensmængden* af A og B, det vil sige alle de elementer i B som ikke ligger i A. Eksempelvis

$$\{1,2,3,4\} \setminus \{3,4,5\} = \{1,2\}$$

- $\mathcal{P}(A)$ eller 2^A *potensmængden* af A er mængden af alle delmængder af A. Eksempelvis

$$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$$

En sidste vigtig mængde operation er *komplementærmængden*. Lad X være en mængde (ofte kaldet *universalmængden*) og lad $A \subseteq X$. Da er komplementærmængden til A, kaldt $A^{\complement}$ det samme som differensmængden af X og A. Altså er

$$A^{\complement} = X \setminus A.$$

4 Beviser

Vi vil i dette afsnit gennemgå tre typer beviser. Det første type bevis er *direkte bevis*, som i vil have set før. Det andet type bevis er et *modstridsbevis*. Det tredje type bevis er *bevis ved induktion*, som de færreste af jer vil have stødt på. Lad os først definere matematiske udsagn.

Definition 4.1. Et *udsagn* er en sætning, som enten er sand eller falsk.

Eksempel 4.2. Eksempler på udsagn er:

- $1 + 1 = 2$
- Månen er lilla
- $x > 4$
- $2 \leq x^2 - 3$
- Det regner
- $7 \cdot 17 = 331$

Bemærk at nogle udsagn er sande, så som $1 + 1 = 2$, nogle er falske, så som $7 \cdot 17 = 331$, og nogle udsagn afhænger af variable, så som $x > 4$, der er sand for nogle men ikke alle x. ∘

Hvis p_1,p_2,...,p_n og q er udsagn, siger vi at q sluttes af p_1,p_2,...,p_n, hvis når alle udsagnene p_1,p_2,...,p_n er sande, så er q også sand.

Eksempel 4.3. Hvis p_1 er at x er et lige tal, p_2 er at x er delelig med 3 og q er at x er delelig med 6, så sluttes q af p_1 og p_2. Dette er tilfældet da lige tal, der er delelig med 3, også er delelig med 6. ∘

Et matematisk bevis er i sin enkelthed en slutning af q fra p_1,p_2,...,p_n, hvor alle udsagnene p_1,p_2,...,p_n er *aksiomer*, antagelser eller tidligere beviste udsagn.

Bemærkning 4.4. Et *aksiom* er et udsagn, som er så banalt, at matematikkere ikke kan bevise dem, men må antage dem som sande. Den første til at beskrive nogle aksiomer var Euklid fra Alexandria, der blandt andet beskrev aksiomet "hvis $a = c$ og $b = c$ så er $a = b$".

Definition 4.5. Et *direkte bevis* er et bevis, hvor vi i stedet for at vise, at p_1,p_2,...,p_n medfører q, så viser vi, at p_1 medfører p_2 medfører ... medfører p_n medfører q.

Medfører kan også skrives med en *implikationspil* $\Rightarrow$. Hvis p_1 medfører p_2 og p_2 medfører p_1 kan det angives med en *biimplikationspil* $\Leftrightarrow$.

Eksempel 4.6. Som eksempel, lad os bevise at kvadratet på et lige tal er lige.

Bevis. Lad vores første udsagn være vores antagelse at x er lige. Altså

$$x = 2n.$$

Dette medføre

$$x^2 = (2n)^2 = 2^2n^2,$$

som medføre at

$$x^2 = 2(2n^2),$$

og da $2n^2$ er et heltal må $2(2n^2)$ være et lige tal. □

I matematikkens verden vil vi gerne have, at der ikke eksistere modstrid. Altså udsagn der både er sande og falske på samme tid. Dette betyder at man kan bruge en bevisform der hedder *modstridsbevis*, hvor man viser at et udsagn ikke kan være sandt og dermed må udsagnets modsætning være sand.

Definition 4.7. Et *modstridsbevis* er et bevis, hvor man viser, at et udsagn er sandt ved at vise, at udsagnets modsætning fører til modstrid. Man afslutter typisk et modstridsbevis med ↯.

Eksempel 4.8. Jeg vil gerne bevise at jeg ikke er en fisk.

Antag for modstrid at jeg er en fisk.

Hvis jeg er en fisk, har jeg gæller.

Hvis jeg har gæller, kan jeg kun indtage ilt i vand.

Men jeg indtager ilt på land.

Dermed må min antagelse om at være en fisk være forkert, og jeg er dermed ikke en fisk. ∘

Eksempel 4.9. Som et eksempel vil vi bevise at $\sqrt{2}$ er irrational.

Bevis. Antag for modstrid, at $\sqrt{2}$ ikke er irrational. Altså at $\sqrt{2}$ kan skrives, som en uforkortelig brøk $\frac{p}{q}$. Da må

$$\left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2} = 2.$$

Dermed må

$$p^2 = 2 \cdot q^2,$$

da er p^2 et lige tal og derfor må p altså også være et lige tal. Da p er lige må det kunne skrives på formen $2 \cdot m$ og dermed må

$$p^2 = (2 \cdot m)^2 = 4 \cdot m^2 = 2 \cdot q^2,$$

og dermed må

$$2 \cdot m^2 = q^2,$$

og q er dermed også et lige tal. Derfor kan q skrives på formen $2 \cdot n$. Men det vil sige, at

$$\sqrt{2} = \frac{p}{q} = \frac{2 \cdot m}{2 \cdot n},$$

som er en forkortelig brøk, hvilket er i strid med vores antagelse om, at $\frac{p}{q}$ er en uforkortelig brøk. Dermed kan $\sqrt{2}$ ikke skrives som en uforkortelig brøk, hvilket er i modstrid med vores antagelse om, at $\sqrt{2}$ er rational. ↯

Den sidste bevisform vi vil gennemgå er induktionsbeviser.

Definition 4.10. Et *induktionsbevis* er et bevis, som følger nedenstående "algoritme".

- Lad $p(n)$ være et udsagn, som indeholder variablen $n \in \mathbb{N}$ (for eksempel $p(n) := n \leq n^2$).
- Vi kalder udsagnet, hvor 1 indsættes på n's plads for induktionsstarten (for eksempel $p(1) := 1 \leq 1^2$).
- Induktionstrinnet er at vise, at hvis $p(m)$ er sand, så er $p(m+1)$ også sand (for eksempel hvis $p(m) := m \leq m^2$, så er $p(m+1) := m+1 \leq (m+1)^2$).
- Hvis vi kan bevise både induktionsstarten og -trinnet, så er $p(n)$ sand for alle $n \in \mathbb{N}$.

På mange måder minder induktionsbeviser om dominobrikker. Forstil dig en række dominobrikker. Så kan man med induktion vise, at hvis man vælter den første brik, vælter alle brikkerne.

Induktionsstarten er at man vælter den første dominobrik. Induktionsskridtet er at vise at hvis en brik vælter, så vælter den næste brik også.

Med dette vist ved vi nu at alle brikkerne vælter fordi vi vælter den første (induktionsstarten), og fordi den første brik er væltet vælter den anden brik også (induktionsskridtet), og fordi den anden brik er væltet vælter den tredje brik også (induktionsskridtet) og så videre. Altså vælter alle dominobrikkerne.

Eksempel 4.11. Vi vil bevise at summen af de første n ulige tal er n^2.

Bevis. Bevis ved induktion. **Induktionsstart:** Summe af det første ulige tal er 1^2. Dette er sandt, da det første ulige tal er 1, og $1 = 1^2$. **Induktionstrin:** Bemærk at det n'te ulige tal er $2n-1$. Lad os antage at summen af de første n

ulige tal er n^2, altså at $1 + 3 + 5 + ... + (2n - 1) = n^2$, så er summen af de første $n + 1$ ulige tal $n^2 + 2n + 1 = (n + 1)^2$, hvilket var hvad vi skulle vise. □

5 Funktioner

I dette afsnit vil vi gennemgå basalt om afbildninger samt domænet og kodomænet af disse. Vi vil også gennemgå nogle egenskaber afbildninger kan have, herunder injektiv, surjektiv og bijektiv.

En afbildning, svare til det, du ville kalde en funktion. Dog er en en funktion kun en afbildning der er defineret på de reelle tal $\mathbb{R}$, mens ordet afbildning bliver brugt i alle andre tilfælde. Hvilke vil sige af afbildning er det generelle udtryk.

Definition 5.1. En *afbildning* f er en sammenknytning af elementer i to mængder A og B, så $a \in A$ får tildelt et element $f(a) \in B$. Dette bliver noteret således: $f\colon A \to B$, som bliver udtalt som: f er en afbildning fra A til B.

Bemærkning 5.2. En afbildning $f\colon A \to B$ skal give et og kun et $b \in B$ til hvert $a \in A$.

Hvis ens postuleret afbildning ikke opfylder kravende for en afbildning, siger vi at den ikke er veldefineret (dette er et matematisk fagord der betyder i denne sammenhæng: Dette du har beskrevet er ikke afbildning). Et eksempel på en ikke veldefineret afbildning er $f : \mathbb{R} \to \mathbb{R}$ givet ved $f(x) = 1/x$ da der ikke knytter sig nogen værdi til 0. Et andet eksempel kunne være $f : A \to B$ som knytter to forskellige elementer b_1 og b_2 i B til et element $a \in A$, dette er ikke tilladt da man kun må knytte en værdi til a, nemlig $f(a)$.

Definition 5.3. Lad $f : A \to B$ være en afbildning. Mængden A kaldes for *domænet* eller *definitionsmængden* for f og

mængden B kaldes for *kodomænet* eller *værdimængden* for f.

Definition 5.4. Lad $f : A \to B$ være en afbildning. Hvis $f(a) = b$, så siges det, at a bliver afbildet i eller sendt over i b, samt at b bliver ramt af a. Mængden af de elementer $b \in B$ som bliver ramt af elementer fra A kaldes for *billedet af* f. Dette bliver noteret således:

$$\begin{aligned} f(A) =& \{f(a) \in B \mid a \in A\} \\ =& \{b \in B \mid \text{ Der findes et } a \in A \text{ således at } f(a) = b\} \\ =& \{b \in B \mid \exists a \in A : f(a) = b\}. \end{aligned}$$

I stedet for at gå fra domænet til kodomænet med f kan man også gå den anden vej med et urbilledet.

Definition 5.5. Lad A,B være mængder og lad $f \colon A \to B$. Lad endvidere $S \subseteq B$. Da er *urbilledet* af S under f

$$f^{-1}(S) = \{x \in A \mid f(x) \in S\}.$$

Bemærk, at urbilledet er en mængde – ikke en funktion. Det er altså mængden af elementer i domænet, som rammer S.

Eksempel 5.6. Lad $f \colon \mathbb{R} \to \mathbb{R}$ givet ved $f(x) = x^2$.

Da er urbilledet af $\{4\}$ det samme som $\{x \in \mathbb{R} \mid x^2 = 4\} = \{-2, 2\}$.

Da er urbilledet af $[0; 1]$ det samme som $[-1; 1]$ fordi $f([-1; 1]) = [0; 1]$ samt at for alle $x \notin [-1; 1]$ er $f(x) \notin [0; 1]$ ∘

Hvis domænet og kodomænet fremgår af sammenhængen, samt at der ikke er behov for at referere til afbildningen ved navn, vil man kunne benytte denne notation:

$$x \mapsto y$$

Dette læses som: afbildningen, der sender x over i y. Her angiver x et element i domænet og y angiver det element i kodomænet der bliver ramt af x.

Nu vil vi se på afbildningers forskellige egenskaber. Vi kigger på injektivitet, surjektivitet og bijektioner.

Definition 5.7. En afbildning $f : A \to B$ kaldes *injektiv*, også kaldet en-til-en, hvis ethvert $b \in f(A)$ bliver ramt af højst ét $a \in A$

Her skal i bemærke at definitionen på en afbildning og injektiv ikke er det samme. Forskellen ligger i, at en afbildning gerne må sende både a og a' til samme b. Og for at opfylde injektiv definitionen er det kun a eller a' der bliver sendt til b. Da man nogle gange kalder en injektiv afbildning for en-til-en afbildningen, da der er en en-til-en sammenhæng mellem elementerne i A og elementerne i B som rammes af f.

Eksempel 5.8 (Bevis for injektivitet)**.** Lad $f : A \to B$. Når man vil vise, at en afbildning f er injektiv, tager man udgangspunkt i en standart fremgangsmåde.

Antag, at der findes a og a', så $f(a) = f(a')$. Hvis man ud for antagelsen kan vise at $a = a'$, så er afbildningen injektiv. Hvis det ikke kan vises at $a = a'$ altså $a \neq a'$ så vil det føre til en modstrid.

Lad os vise, at afbildningen $f : \mathbb{R} \to \mathbb{R}$, hvor $f(x) = 5x-6$ for alle x i $\mathbb{R}$ er injektive. Derfor antag at der findes x og y, så $f(x) = f(y)$.

$$f(x) = f(y) \Rightarrow 5x - 6 = 5y - 6 \Rightarrow 5x = 5y \Rightarrow x = y$$

Dette giver at f er injektiv. ∘

Definition 5.9. En afbildning $f : A \to B$ kaldes *surjektiv*, hvis ethvert $b \in B$ bliver ramt af et element fra A

Bemærkning 5.10. Det vil sige at en afbildning er surjektiv, hvis billedet af f er lig $B : f(A) = B$

Eksempel 5.11 (Bevis for surjektivitet)**.** Lad $f : A \to B$. Når man vil vise, at f er surjektiv, skal man vise, at der for ethvert $b \in B$ findes $a \in A$, så $f(a) = b$.

Lad os vise, at afbildningen $f : \mathbb{R} \to \mathbb{R}$, hvor $f(x) = 5x-6$ for alle x i $\mathbb{R}$, er surjektiv. Tag derfor $y \in \mathbb{R}$. Lad $x = \frac{y}{5} + \frac{6}{5}$

$$f(x) = g\left(\frac{y}{5} + \frac{6}{5}\right) = 5\left(\frac{y}{5} + \frac{6}{5}\right) - 6 = y + 6 - 6 = y$$

x er her fundet ved løse ligningen $y = 5x - 6$ for y. Surjektiviteten vises dog ved at indsætte det fundne x og vise at det rammer det givne y, uanset, hvordan man har fundet sit x. ∘

Definition 5.12. En afbildning er *bijektiv*, hvis den både er surjektiv og injektiv.

Dette betyder, at når en afbildning fra A til B er bijektiv, så vil der blive dannet par mellem elementerne i de to mængder, således at ethvert element i B er parret med præcist ét element i A. Per definition af en afbildning er hvert element i A også præcis i ét par. En bijektion mellem to mængder er en injektiv og surjektiv korrespondance mellem mængderne.

Eksempel 5.13. Afbildningen $f(x) = 5x-6$ er vist til både at være injektiv og surjektiv, hvilket betyder at den er vist til at være bijektiv. ∘

Sætning 5.14. En afbildning $f : A \to B$ er bijektiv, når der findes $g : B \to A$, så $f(g(b)) = b$ for alle $b \in B$ og $g(f(a)) = a$ for alle $a \in A$. g kaldes for en dobbeltsidet invers til f og bliver noteret således $g = f^{-1}$.

Som den skarpe læser måske har bemærket, så minder notationen for en invers funktion *meget* om notationen for

urbilledet. Man kan ofte kende forskel på de to ved at en invers ofte skrives i forbindelse med et enkelt element, hvor urbilledet altid tages af en mængde. Selvom inversen ikke eksisterer (det gør den nemlig ikke altid!), så kan vi altid tage urbilledet af en mængde.

6 Opgaver

Opgave 6.1:
Bestem

1) $\text{sfd}(12, 15)$

2) $\text{sfd}(6, 4)$

3) $\text{sfd}(6, 30)$

4) $\text{mfm}(3, 10)$

5) $\text{mfm}(12, 4)$

6) $\text{mfm}(14, 6)$

Opgave 6.2:
Fortæl en ven hvad svaret til følgende spørgsmål er:

1) Hvad er en mængde?

2) Hvad er et udsagn?

3) Hvad er et bevis?

4) Hvad er en funktion?

Opgave 6.3:
Afgør om følgende udsagn er sande:

1) $7 \in \mathbb{N}$

2) $7 \in \mathbb{Z}$

3) $7 \in \{2n | n \in \mathbb{Z}\}$

4) $7 \subseteq \mathbb{N}$

5) $\{7\} \subseteq \mathbb{N}$

6) $\emptyset = \{\}$

7) $\{\emptyset\} = \{\}$

Opgave 6.4:
Lad $A = \{1, 2, 3\}$ og $B = \{2, 3, 4\}$. Bestem følgende:

1) Hvad er $A \cup B$?

2) Hvad er $A \cap B$?

3) Hvad er $A \setminus B$?

4) Hvad er $B \setminus A$?

5) Hvad er $P(A)$?

Opgave 6.5:
Lad $A = \mathbb{N}$ og $B = \mathbb{Z}$. Bestem følgende:

1) Hvad er $A \cup B$?

2) Hvad er $A \cap B$?

3) Hvad er $A \setminus B$?

4) Hvad er $B \setminus A$?

5) Hvad er A^C i B?

Opgave 6.6:
For tre vilkårlige mængder A, B, C er det altid tilfældet at $(A \cup B) \cap C = A \cup (B \cap C)$?

Hvis nej, giv et modeksempel.

Opgave 6.7:
Bestem hvilke af følgende mængder er det samme, som den tomme mængde.

1) $\{n \in \mathbb{Z} | n \leq 0\} \cap \mathbb{N}_0$.

2) Mængden af chokolade i denne bog.

3) $\emptyset \cap \mathbb{R}$.

4) $\emptyset \cup \mathbb{R}$.

5) $[0; 1] \cap [3; 8]$.

Opgave 6.8:
Skriv følgende mængder på elementform:

1) $\{x \in \mathbb{R} | x^2 = 2\}$

2) $\{x \in \mathbb{Z} | x^2 = 2\}$

3) $\{x \in \mathbb{Q} | x^2 - 2x = 0\}$

Opgave 6.9:
Afgør om følgende udsagn er sande:

1) $(a+b)^2 = a^2 + b^2$.

2) Der eksistere naturlige tal x og y således at $64 = 3x + 5y$.

3) $x \cdot y$ er ulige hvis og kun hvis x og y er ulige.
(Hint: et ulige tal kan altid stå på formen $2n+1$ og et lige tal på formen $2n$).

4) $x \cdot y$ er lige hvis og kun hvis enten x eller y er lige.

Opgave 6.10:
Følg beviset for at $\sqrt{2}$ er irrational og bevis følgende:

1) $\sqrt{3}$ er irrational.

2) $\sqrt{6}$ er irrational. Overvej, hvorfor beviset ikke virker, hvis man vil vise at $\sqrt{4}$ er irrational.

Opgave 6.11:
Brug induktion til at bevise følgende:

1) $1 + 2 + ... + n = \frac{n(n+1)}{2}$

2) $1 + 4 + 7 + ... + (3n-2) = \frac{n(3n-1)}{2}$

3) $2 + 6 + 10 + ... + (4n-2) = 2n^2$

Opgave 6.12:
Bevis med induktion, at 4 går op i $5^n - 1$.

Opgave 6.13:
Bestem for hver funktion om de er injektive, surjektive eller bijektive.

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

2) $f : \mathbb{R} \to \mathbb{R}_+$ givet ved $f(x) = x^2$.

3) $f : \mathbb{R}_+ \to \mathbb{R}$ givet ved $f(x) = x^2$.

4) $f : \mathbb{R}_- \to \mathbb{R}_+$ givet ved $f(x) = x^2$.

5) $f : \mathbb{N} \to \mathbb{R}$ givet ved $f(x) = x^2$.

6) $f : \mathbb{Z} \to \mathbb{R}$ givet ved $f(x) = x^2$.

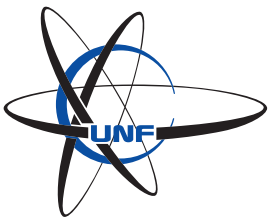
Opgave 6.14:
Lad $f(x) = \sin(x)$. Bestem et domæne og et kodomæne, så f bliver henholdsvis injektiv, surjektiv, bijektiv og ingen af delene.

Opgave 6.15:
Lad $f : \mathbb{R} \to \mathbb{R}$. Giv eksempler på f, så f er henholdsvis injektiv, surjektiv, bijektiv og ingen af delene.

Opgave 6.16:
Lad $f : \mathbb{R} \to \mathbb{R}$ være defineret ved $f(x) = \cos(x)$.

1) Bestem mængderne $f(\mathbb{R}_+)$ og $f(\mathbb{R}_-)$.

2) Bestem urbilledet af $[0; 1]$.



Sandsynlighedsteori 1

1 Summer og sandsynligheder

I dette kapitel skal vi studere sandsynlighedsteori. Måske kan man lidt cirkulært sige, at sandsynlighedsteori er det matematiske studie af sandsynlighed. Man kan tænke på det, som studiet af udfald af eksperimenter og hvilke udfald, vi forventer, vil ske oftest. I kapitlet kommer vi ind på, hvordan matematikere definerer sandsynlighed, og vi skal arbejde med såkaldte stokastiske variable, som bruges til at beskrive diverse udfald. Til slut vil vi anvende de forskellige teknikker i forløbet på diverse kortspil og terningespil. Inden vi springer ud i sandsynlighedsteorien skal vi have nogle ting på plads, nemlig summer og kombinatorik.

Summer

Definition 1.1. Lad $a_1, a_2, \ldots, a_n$ være reelle tal. Da kan vi skrive summen $a_1 + a_2 + \cdots + a_n$ som

$$\sum_{i=1}^{n} a_i.$$

Hvis vi har uendeligt mange tal $a_1, a_2, \ldots$ indekseret (nummereret) ved de naturlige tal $\mathbb{N}$, så skriver vi

$$\sum_{i=1}^{\infty} a_i \quad \text{eller} \quad \sum_{n=1}^{\infty} a_n.$$

Vi kalder dette for en *uendelig sum* eller en *række*.

Bemærkning 1.2. Senere kommer vi også til at se mange eksempler på summer, som er indekseret ved alle heltal større end eller lig 0, $\mathbb{N}_0$. Konceptet er præcis det samme som, når summen er indekseret ved $\mathbb{N}$.

Eksempel 1.3. Lad os se på summen

$$\sum_{i=1}^{10} i.$$

Dette er summen $1+2+3+4+5+6+7+8+9+10$. Vi udregner dette til 55. ∘

Eksempel 1.4. Lad os se på den uendelige sum

$$\sum_{n=1}^{\infty} n,$$

dvs. $1+2+3+\ldots$. Denne sum bliver klart uendeligt stor, så vi skriver

$$\sum_{n=1}^{\infty} n = \infty.$$

Hvis en række er lig uendelig, siger vi, at rækken *divergerer*. ∘

Det er ikke altid tilfældet, at en uendelig sum af positive tal bliver uendelig. Nogle gange kan summen *konvergere* til et tal. Man kan tænke på det, som at hvert led nærmer sig 0 tilstrækkeligt hurtigt, så selvom man lægger uendeligt mange ting sammen, bliver summen endelig.

Eksempel 1.5. Det viser sig, at

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Dvs. vi har $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}$. At vise dette kræver teknikker fra matematisk analyse, som vi ikke kommer ind på her. Man skal dog ikke tro, at blot fordi leddene i summen nærmer sig 0, når n bliver større, at summen så vil blive endelig. F.eks. viser det sig, at

$$\sum_{n=1}^{\infty} \frac{1}{n} = \infty.$$

Rækken $1 + \frac{1}{2} + \frac{1}{3} + \ldots$ kaldes *den harmoniske række*. ∘

Lad os, som det sidste inden vi springer ud i sandsynligheder, se på nogle nyttige eksempler på rækker, som ikke er lig uendelig. Først ser vi på *geometriske rækker*.

Definition 1.6. Lad x være et reelt tal. Summen

$$\sum_{n=0}^{N} x^n$$

kaldes en *geometrisk sum*. Rækken

$$\sum_{n=0}^{\infty} x^n$$

kaldes den *geometriske række*.

Hvis du kender til grænseværdier, kan du bemærke, at

$$\lim_{N\to\infty} \sum_{n=0}^{N} x^n = \sum_{n=0}^{\infty} x^n.$$

Summerne $\sum_{n=0}^{N} x^n$ kaldes *afsnitssummerne* for den geometriske række $\sum_{n=0}^{\infty} x^n$. Det viser sig, at man nemt kan udregne disse afsnitssummer, hvilket lemmaet herunder illustrerer.

Lemma 1.7. For et reelt tal $x \neq 1$ har vi, at

$$\sum_{n=0}^{N} x^n = \frac{1 - x^{N+1}}{1 - x}.$$

Bevis. Vi fører beviset ved induktion over N. For $N = 1$ har vi, at

$$\sum_{n=0}^{N} x^n = x^0 + x^1 = 1 + x = \frac{(1+x)(1-x)}{1-x} = \frac{1-x^2}{1-x},$$

hvilket stemmer overens med formlen i lemmaet. Bemærk, at vi har lov til at dividere med $1 - x$, da $x \neq 1$, så $1 - x \neq 0$. Dette viser induktionsstarten.

Antag, at $N > 1$, og at formlen gælder for $N - 1$. Vi har da, at

$$\begin{aligned}\sum_{n=0}^{N} x^n &= x^N + \sum_{n=0}^{N-1} x^n = x^N + \frac{1-x^N}{1-x} \\ &= \frac{x^N(1-x)}{1-x} + \frac{1-x^N}{1-x} = \frac{x^N(1-x)+1-x^N}{1-x} \\ &= \frac{x^N - x^{N+1} + 1 - x^N}{1-x} = \frac{1-x^{N+1}}{1-x},\end{aligned}$$

som ønsket. Dette viser induktionsskridtet. Ifølge induktionsprincippet kan vi konkludere, at formlen gælder for alle $N \in \mathbb{N}$. □

Eksempel 1.8. Lad os udregne summen af de første 100 tal i følgen $1, \frac{1}{10}, \frac{1}{100}, \ldots$. Summen er

$$\sum_{n=0}^{100} \left(\frac{1}{10}\right)^n = \frac{1 - \left(\frac{1}{10}\right)^{101}}{1 - \frac{1}{10}} \approx 1{,}1111.$$

∘

Vi kan bruge Lemma 1.7 til at vise følgende nyttige resultat for geometriske rækker.

Sætning 1.9. Lad x være et reelt tal med $|x| < 1$. Da er

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

Bevis. Bemærk, at fordi $|x| < 1$, da vil x^n komme tættere og tættere på 0, når n vokser. I symboler kan vi skrive, at $\lim_{n\to\infty} x^n = 0$. Dermed får vi per Lemma 1.7, at

$$\sum_{n=0}^{\infty} x^n = \lim_{N\to\infty} \sum_{n=0}^{N} x^n = \lim_{N\to\infty} \frac{1-x^{N+1}}{1-x} = \frac{1}{1-x},$$

som ønsket. □

Eksempel 1.10. Lad os udregne den uendelige sum $1 + \frac{1}{2} + \frac{1}{4} + \ldots$. Vi ser, at denne række er den geometriske række

$$\sum_{n=0}^{\infty} \left(\frac{1}{2}\right)^n.$$

Da $\left|\frac{1}{2}\right| = \frac{1}{2} < 1$, så kan vi anvende Sætning 1.9 og få

$$\sum_{n=0}^{\infty} \left(\frac{1}{2}\right)^n = \frac{1}{1-\frac{1}{2}} = 2.$$

∘

Lad os til slut se på eksponentialfunktionen.

Eksempel 1.11. Eksponentialfunktionen evalueret i et punkt x kan opskrives som en række, nemlig

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$

hvor $n!$ betegner *fakultetsfunktionen*, $n! = n \cdot (n-1) \cdot \cdots \cdot 1$. F.eks. er $3! = 6$ og $4! = 24$. Vi har som konvention, at $0! = 1$. ∘

Ovenstående række for eksponentialfunktionen (som er et eksempel på en såkaldt *Taylorrække*) kommer til at dukke op senere i forløbet, hvor vi skal studere Poisson-fordelingen.

Kombinatorik: At tælle i matematik

For at regne sandsynligheder er det vigtigt at kende det totale antal udfald, som et eksperiment kan have. Alle kan regne ud, at hvis en terning har 6 sider, så er der 6 mulige udfald, men hvad så når det at tælle bliver mere komplekst? Vi starter med at kigge på produktreglen.

Sætning 1.12 (Produktreglen)**.** Hvis eksperiment A har n_1 forskellige udfald, eksperiment B har n_2 forskellige udfald og udfaldene er uafhængige, så vil antallet af udfald for eksperiment $A \cup B$ være $n_1 \cdot n_2$.

Vi ser, at dette kan udvides til flere eksperimenter end to. I tilfældet med tre eksperimenter, A, B og C, har vi, at der er henholdsvis n_1, n_2 og n_3 mulige udfald. Da kan vi observere, at eksperiment $D = A \cup B$ har $n_4 = n_1 n_2$ mulige udfald, og da vil eksperiment $E = C \cup D$ have $n_5 = n_4 n_3 = n_1 n_2 n_3$ mulige udfald. Ved at bruge samme fremgangsmåde kan dette vises for et arbitrært antal eksperimenter.

Eksempel 1.13. Vi kaster 5 seks-sidede terninger. Hvor mange udfald har dette eksperiment? Eftersom hver terning er uafhængig af de andre, så kan vi anvende produktreglen. Hvert kast har 6 mulige udfald, og der er 5 terninger. Derfor har vi

$$6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 = 6^5 = 7776$$

mulige udfald. Det følger, at sandsynligheden for at slå 5 en'ere er $\frac{1}{7776}$. ∘

Eksempel 1.14. Vi kaster nu en tyve-sidet terning, 2 syv-sidede terninger og 1 fem-sidet terning. Hvor mange udfald har dette eksperiment? Igen er hver terning uafhængig af de andre, så vi kan anvende produktreglen. Vi har

$$20 \cdot 2 \cdot 7 \cdot 5 = 1400$$

mulige udfald. ∘

Den næste grundsten i at tælle er additionsreglen.

Sætning 1.15 (Additionsreglen)**.** Lad eksperiment A have n_1 udfald og eksperiment B have n_2 udfald. Hvis eksperimenterne er uafhængige, så er der $n_1 + n_2$ udfald for $A \cup B$.

Ligesom før kan vi udvide denne sætning til arbitrært mange eksperimenter.

Eksempel 1.16. Der skal vælges én på matcamp fra enten deltagerne eller fra arrangør-holdet. Der er 50 deltagere og 25 arrangører. Hvor mange muligheder er der for at vælge denne person? Eftersom arrangører ikke er deltagere på MatCamp kan vi anvende additionsreglen. Der er

$$50 + 25 = 75$$

mulige personer, som kan blive valgt. ∘

Sætning 1.17 (Dueslagsprincippet/skuffeprincippet)**.** Hvis N objekter bliver placeret i k skuffer, er der mindst én skuffe med $\left\lceil \frac{N}{k} \right\rceil$, hvor $\lceil \frac{N}{k} \rceil$ er det mindste heltal større end eller lig $\frac{N}{k}$.

Bevis. For $k \geq N$ er det klart, da mindst én skuffe har et objekt. Hvis N er 0, er der ingen skuffer med objekter, så det holder også der. Vi kigger derfor på tilfældet, hvor $k < N$. Placér k af de N objekter i hver sin skuffe. Hvis der er k objekter, som ikke er blevet lagt i skuffer, forsæt da som før, indtil der er n objekter tilbage, hvor $0 \leq n < k$. Hvis $n = 0$, så har har alle skuffer $\frac{N}{k}$ objekter i sig. Desuden kan vi ikke fordele det sådan, at ingen skuffer vil have færre objekter i sig. Derfor holder dueslagsprincippet for $n = 0$. Hvis $n > 0$, tilføjer vi objekter, og vi kan ikke tilføje dem sådan, at mindst en skuffe ikke får mindst et objekt yderligere.

Derfor holder dueslagsprincippet også for $n > 0$. Vi har dermed været igennem alle muligheder for dueslagsprincippet, og beviset er færdigt. □

Selvom det virker simpelt, bliver dueslagsprincippet brugt meget i kombinatorik.

Eksempel 1.18. Fra et almindeligt spil kort bliver 21 kort taget ud, da vil mindst $\left\lceil \frac{21}{4} \right\rceil = \lceil 5{,}25 \rceil = 6$ være af samme kulør. ○

Vi kan også bruge dueslagsprincippet til at finde ud af det mindste antal af en specifik type objekt, der er i en specifik skuffe.

Eksempel 1.19. Vi er interesserede i at vide, hvor mange kort N vi skal trække fra et almindeligt spil kort for at være sikre på at have mindst 5 kort af én kulør.
Vi kan nu lade hver kulør være en skuffe, så vi har 4 skuffer. Når vi trækker et kort, placerer vi altså kortet i den skuffe, som svarer til kortets kulør. Vi ved fra dueslagsprincippet, at mindst én skuffe vil have $\left\lceil \frac{N}{4} \right\rceil$ kort, og eftersom kuløren, vi ønsker, er arbitrær, og vi ønsker 5 kort af samme kulør, skal vi finde N således, at $\left\lceil \frac{N}{4} \right\rceil \geq 5$. For $N \leq 16$ vil $\left\lceil \frac{N}{4} \right\rceil \leq 4$. Det følger derfor, at det mindste tal, som opfylder vores kriterium, er $N = 17$, eftersom $\left\lceil \frac{17}{4} \right\rceil = \lceil 4{,}25 \rceil = 5$. Der skal derfor trækkes mindst 17 kort, før vi kan være sikre på at have 5 kort af samme kulør. ○

Dueslagsprincippet kan også anvendes mere avanceret, hvor man først skal være smart med sine valg af skuffer.

Eksempel 1.20. 45 mennesker har valgt at spille kort med et almindeligt spil kort. De skal alle have mindst ét kort for at kunne spille. Vi kan vise, at der vil være en sekvens af spillere, hvor præcis 37 kort er blevet delt ud.

Lad n_i være det antal kort, der er blevet delt ud til og med den i'te person. Vi kigger nu på den stigende sekvens $n_1, n_2, \ldots, n_{45}$, hvor $1 \leq n_i \leq 52$. Vi konstruerer nu en ny sekvens ud fra den ovenstående, $n_1 + 37$,$n_2 + 37, \ldots$,$n_{45} + 37$ hvor $38 \leq n_i + 37 \leq 89$. Hvis vi kigger på sekvensen af alle disse heltal, altså n_1,$n_2, \ldots$,n_{45},$n_1 + 37$,$n_2 + 37, \ldots$,$n_{45} + 37$ hvor $1 \leq n_i \leq 89$, så ser vi at der er 90 tal, der alle er mindre end 90. Da fortæller dueslagsprincippet os, at to af tallene i listen må være ens. Det vil sige, at der eksisterer et par i,$j \in \mathbb{N}$, så $n_i = n_j + 37$. Da har vi, at der fra person $j + 1$ til person i bliver delt præcis 37 kort ud. ∘

Definition 1.21 (r-Permutation)**.** En r-permutation for en samling af unikke objekter er en ordnet rækkefølge af r objekter.

Permutationer bliver brugt, når rækkefølgen af objekterne har betydning.

Eksempel 1.22. Der er 5 personer, Anna, Bo, Christoffer, Dorte og Egon, som kan vinde en førsteplads eller andenplads i en konkurrence. Her skal vi finde en 2-permutation. Det kunne f.eks. være Anna og Dorte eller Dorte og Anna. ∘

Sætning 1.23 (Antal permutationer)**.** Lad $n \in \mathbb{N}$ og lad $1 \leq r \leq n$. Da vil antallet af r-permutationer for samlingen af n objekter være givet ved

$$P(n,r) = n(n-1)(n-2) \cdot \cdots \cdot (n-(r-1)).$$

Bevis. Vi ønsker at anvende produktreglen. Vi observerer, at der vil være n måder at vælge det første objekt. Nu hvor det er valgt, så er der $n - 1$ måder at vælge det næste objekt. Sådan forsættes der, indtil vi skal vælge det sidste objekt, hvor der er $n - (r - 1)$ objekter tilbage. Eftersom alle disse udvælgelser er uafhængige af hinanden, kan vi anvende

produktreglen, som giver $n(n-1)\cdot\cdots\cdot(n-(r-1))$ muligheder. □

Dette kan være lidt træls at regne på en lommeregner, så vi bruger oftest følgende korollar

Korollar 1.24 (Første version)**.** Lad $n \in \mathbb{N}$ og lad $1 \leq r \leq n$. Da vil

$$P(n,r) = \frac{n!}{(n-r)!}.$$

Bevis. Se Opgave 5.20. □

Vi observerer desuden, at for $r = 0$ har vi, at

$$P(n,0) = \frac{n!}{n!} = 1.$$

Dette giver god mening, da der er præcis én måde at ordne nul elementer, den tomme mængde. Vi kan derfor udvide Korollar 1.24 til nedenstående.

Korollar 1.25 (Fuld version)**.** Lad $n \in \mathbb{N}$ og lad $0 \leq r \leq n$. Da vil

$$P(n,r) = \frac{n!}{(n-r)!}.$$

Hvad gør vi så, når rækkefølgen på objekterne er ligegyldig, som i Lotto, hvor man bare skal have de korrekte tal? Her kigger vi på kombinationer.

Definition 1.26 (r-Kombination)**.** En r-kombination for en samling af n unikke objekter er en uordnet rækkefølge af r objekter.

Eksempel 1.27. Lad A være en mængde, da vil en delmængde være en r-kombination for mængden. ∘

For kombinationer skriver vi $\binom{n}{r}$ som læses "n vælg r".

Sætning 1.28 (Antal kombinationer)**.** Lad $n \in \mathbb{N}$ og lad $0 \leq r \leq n$. Da har vi, at

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Bevis. Vi observerer, at antallet af r-permutationer, $P(n,r)$, for en samling kan findes ved først at finde alle kombinationer af samlingen, og derefter finde alle ordninger af de kombinationer. Da disse to udfald ikke påvirker hinanden, kan vi bruge produktreglen. Vi har dermed, at

$$P(n,r) = \binom{n}{r} \cdot P(r,r) \iff \binom{n}{r} = \frac{P(n,r)}{P(r,r)}.$$

Ved at bruge Korollar 1.25 har vi, at

$$\binom{n}{r} = \frac{P(n,r)}{P(r,r)} = \frac{\frac{n!}{(n-r)!}}{\frac{r!}{(r-r)!}} = \frac{n!(r-r)!}{r!(n-r)!} = \frac{n!}{r!(n-r)!},$$

idet $0! = 1$. □

Eksempel 1.29. Hvor mange forskellige hænder af 3 kort kan man få fra et almindeligt spil kort? Hvad med hænder af 49 kort?
Siden to hænder er ens uanset rækkefølgen af kortene, bruger vi kombinationer. Vi bruger Sætning 1.28 og får

$$\binom{52}{3} = \frac{52!}{3!49!} = 22.100 = \frac{52!}{49!3!} = \binom{52}{49}.$$

Vi ser her, at de to spørgsmål har samme svar. ∘

Eksemplet kunne tyde på, at der er symmetri for kombinationer. Dette leder os til næste korollar

Korollar 1.30. Lad $n,r \in \mathbb{N}_0$ og $r \leq n$. Da har vi $\binom{n}{r} = \binom{n}{n-r}$.

Bevis. Se Opgave 5.20. □

Kombinationer har flere egenskaber, som er gode at have i praksis. En sådan egenskab er Pascals identitet.

Sætning 1.31 (Pascals identitet/trekant)**.** Lad $n, k \in \mathbb{N}$ og lad $n \geq k$. Da har vi, at

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Bevis. Vi kigger på højresiden:

$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} \\ &= \frac{n!}{(k-1)!(n+1-k)!} + \frac{n!}{k!(n-k)!}.\end{aligned}$$

Forskellen på $k!$ og $(k-1)!$ er kun en faktor k, og forskellen på $(n+1-k)!$ og $(n-k)!$ er kun en faktor $(n+1-k)$. Vi har derfor, at

$$\begin{aligned}\frac{n!}{(k-1)!(n+1-k)!} + \frac{n!}{k!(n-k)!} &= \frac{n!k + n!(n+1-k)}{k!(n+1-k)!} \\ &= \frac{n!(n+1)}{k!(n+1-k)!} \\ &= \binom{n+1}{k}.\end{aligned}$$

□

Pascals identitet kan visualiseres som en trekant, hvor hvert tal er summen af de to tal oven over:

$$
\begin{array}{ll}
n=0 & \binom{0}{0} \\
n=1 & \binom{1}{0} \quad \binom{1}{1} \\
n=2 & \binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2} \\
n=3 & \binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3} \\
n=4 & \binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4} \\
n=5 & \binom{5}{0} \quad \binom{5}{1} \quad \binom{5}{2} \quad \binom{5}{3} \quad \binom{5}{4} \quad \binom{5}{5} \\
n=6 & \binom{6}{0} \quad \binom{6}{1} \quad \binom{6}{2} \quad \binom{6}{3} \quad \binom{6}{4} \quad \binom{6}{5} \quad \binom{6}{6}
\end{array}
$$

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}
$$

Den øverste trekant er kombinationerne, og den nederste trekant er værdien af den tilsvarende kombination. Vi illustrerer dette med et eksempel.

Eksempel 1.32. Vi har ingen lommeregner og ønsker at regne nogle kombinationer. Vi ved fra sætning 1.31, at vi kan finde $\binom{6}{3}$ ved i stedet at finde $\binom{5}{2} + \binom{5}{3}$. Korollar 1.30 siger også, at $\binom{5}{2} = \binom{5}{3}$. Vi har da, at

$$\binom{5}{3} = \frac{5!}{2!3!} = \frac{5 \cdot 4}{2} = 10,$$

og dermed er

$$\binom{6}{3} = \binom{5}{2} + \binom{5}{3} = 10 + 10 = 20.$$

$\circ$

En anden god egenskab, som kombinationer har, er, hvordan de bliver brugt sammen med *binomialer*. En binomial er et udtryk, hvor to variable er summeret, f.eks $x + y$.

Sætning 1.33 (Binomialsætningen)**.** Lad x og y være variable, og lad $n \in \mathbb{N}$. Da har vi, at

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j.$$

Bevis. Vi vil her lave et induktionsbevis. For $n = 1$ er det sandt, at

$$\sum_{j=0}^{1} \binom{n}{j} x^{n-j} y^j = x + y.$$

For $n = 2$ har vi, at

$$\begin{aligned}\sum_{j=0}^{2} \binom{n}{j} x^{n-j} y^j &= \binom{2}{0} x^{2-0} y^0 + \binom{2}{1} x^{2-1} y^1 + \binom{2}{2} x^{2-2} y^2 \\ &= x^2 + y^2 + 2xy.\end{aligned}$$

Induktionsantagelsen er, at

$$\sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = (x+y)^n.$$

Vi vil nu vise, at sætningen gælder for $(x+y)^{n+1}$. Observér, at

$$(x+y)^{n+1} = (x+y)(x+y)^n.$$

Vi kan nu bruge vores induktionsantagelse på $(x+y)^n$. Vi har, at

$$\begin{aligned}(x+y)(x+y)^n &= (x+y) \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j \\ &= (x+y) \left(\binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n} y^n \right).\end{aligned}$$

Vi ganger nu x og y ind i parentesen, hvilket giver

$$x^{n+1} + \binom{n}{1}x^n y + \cdots + \binom{n}{n}xy^n + x^n y \\ + \binom{n}{1}x^{n-1}y^2 + \cdots + \binom{n}{n}y^{n+1}.$$

Vi kan nu flytte de variable, der er lig hinanden, uden for parentes. Det er alle led forskellig fra det første og det sidste. Vi har altså, at

$$x^{n+1} + \left(1 + \binom{n}{1}\right)x^n y + \ldots \\ + \left(\binom{n}{k-1} + \binom{n}{k}\right)x^{n-k+1}y^k + \cdots + \left(\binom{n}{n-1} + 1\right)x^1 y^n \\ + y^{n+1}.$$

Ved at anvende Pascals identitet, Sætning 1.31, får vi, at

$$x^{n+1} + \binom{n+1}{1}x^n y + \cdots + \binom{n+1}{n}xy^n + y^{n+1} \\ = \sum_{j=0}^{n+1}\binom{n+1}{j}x^{n+1-j}y^j.$$

Vi har derfor, at

$$\sum_{j=0}^{n+1}\binom{n+1}{j}x^{n+1-j}y^j = (x+y)^{n+1},$$

og per induktion gælder derfor, at

$$(x+y)^n = \sum_{j=0}^{n}\binom{n}{j}x^{n-j}y^j$$

for alle $n \in \mathbb{N}$, som ønsket. □

Der er mange anvendelser af denne sætning. Vi gennemgår nu nogle af dem.

Korollar 1.34. Lad $n \in \mathbb{N}$. Da har vi, at

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n,$$
$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0.$$

Bevis. Ved at bruge binomialsætningen får vi, at

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^{n} \binom{n}{k},$$
$$0^n = (1-1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} (-1)^k = \sum_{k=0}^{n} \binom{n}{k} (-1)^k.$$

□

Der er også andre anvendelser af binomialsætningen.

Eksempel 1.35. Hvad er koefficienten for $x^{17}y^{13}$ i udvidelsen af $(x+y)^{30}$? Vi bruger binomialsætningen og ser, at

$$(x+y)^{30} = \sum_{j=0}^{n} \binom{30}{j} x^{30-j} y^j.$$

For leddet med x^{17} skal $j = 13$. Koefficienten bliver

$$\binom{30}{13} = 119.759.850.$$

○

Hvad er sandsynlighed?

Vi kan nu definere, hvad en matematiker mener med sandsynlighed. Efter definitionen giver vi en forklaring af, hvorfor aksiomerne for sandsynlighed er, som de er.

Definition 1.36. Et *udfaldsrum* S for et eksperiment er en mængde og en delmængde A af S kaldes et *udfald* eller en *begivenhed*. En *sandsynlighed* P er en funktion, som tager en delmængde i S og tildeler denne en værdi i intervallet $[0, 1]$. P opfylder følgende to regler/aksiomer:

1. $P(\emptyset) = 0$ og $P(S) = 1$.
2. Hvis $A_1, A_2, \ldots$ er parvist disjunkte begivenheder (dvs. $A_i \cap A_j = \emptyset$ for alle $i \neq j$) har vi

$$P\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} P(A_n).$$

Hvad står der i ovenstående definition? Alle udfald af eksperimentet er indeholdt i S. Dermed kan man tænke på sandsynligheden $P(S)$ som sandsynligheden for, at *noget* sker. Men der sker altid noget, og derfor er $P(S) = 1$. På samme måde må $P(\emptyset) = 0$, eftersom sandsynligheden for, at ingenting sker, må være 0. Regel to siger, at hvis en samling af begivenheder ikke overlapper noget sted, da må sandsynligheden for, at mindst én af dem finder sted, kunne findes som summen af sandsynligheden for hver begivenhed. Dette stemmer godt overens med vores intuition. Sandsynligheden for at slå et eller to på en terning må være sandsynligheden for at slå et lagt til sandsynligheden for at slå to (da man jo ikke kan slå både et og to på ét terningekast).

Bemærk, at P antager værdier mellem 0 og 1. Man kan tænke på 0 som 0% sandsynlighed og 1 som 100% sandsynlighed for, at en begivenhed finder sted.

Eksempel 1.37. Lad os illustrere definitionen af sandsynlighed med noget velkendt, nemlig en sekssidet terning. Her er $S = \{1, 2, 3, 4, 5, 6\}$ vores udfaldsrum. Vi antager, at terningen er fair, så alle øjne har samme sandsynlighed ved et kast med terningen. $A = \{2\} \subseteq S$ er begivenheden, at vi

slår 2 med terningen. Vi har, at $P(A) = \frac{1}{6}$. $B = \{1, 3, 4\}$ er begivenheden, at vi slår 1, 3 eller 4 med terningen. Vi har klart, at $P(B) = \frac{1}{2}$. Bemærk, at $A \cap B = \emptyset$, så regel nummer to i definitionen siger, at sandsynligheden for at slå enten 1, 2, 3 eller 4 er

$$P(\{1, 2, 3, 4\}) = P(A \cup B) = P(A) + P(B) = \frac{1}{6} + \frac{1}{2} = \frac{4}{6},$$

hvilket vi også ville forvente. ∘

Ud fra de to regler i definitionen af sandsynlighed kan vi udlede flere regler, som er smarte i mange sammenhænge.

Sætning 1.38. En sandsynlighed P har følgende egenskaber for to begivenheder A og B:

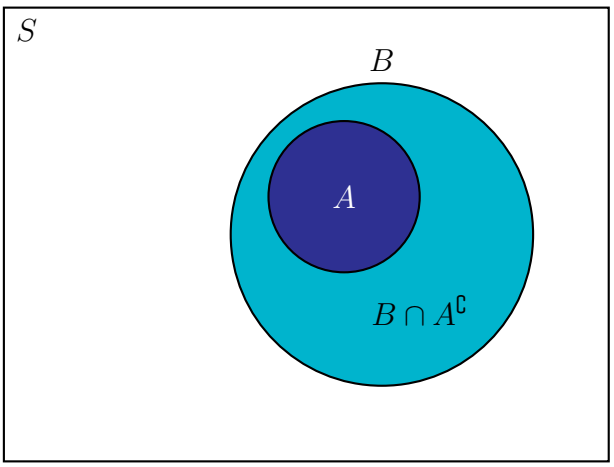
1. $P(A^{\complement}) = 1 - P(A)$.

2. Hvis $A \subseteq B$, da er $P(A) \leq P(B)$.

3. $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

Bevis. 1. Bemærk, at $A \cap A^{\complement} = \emptyset$ og $A \cup A^{\complement} = S$. Dermed giver regel 1 og 2, at $1 = P(S) = P(A \cup A^{\complement}) = P(A) + P(A^{\complement})$. Trækker vi $P(A)$ fra på begge sider, fås $P(A^{\complement}) = 1 - P(A)$.

2. Hvis $A \subseteq B$, kan vi skrive $B = (B \cap A^{\complement}) \cup A$. Se Venn-diagrammet herunder:

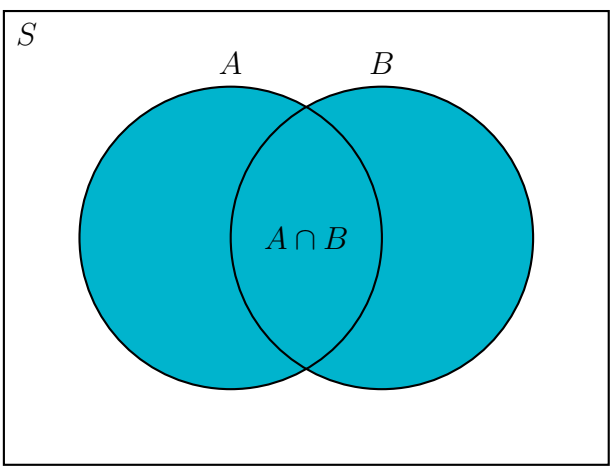


Eftersom A og $B \cap A^{\complement}$ er disjunkte, giver regel 2:

$$P(B) = P((B \cap A^{\complement}) \cup A) = P(B \cap A^{\complement}) + P(A),$$

og da $P(B \cap A^{\complement}) \geq 0$ (husk at sandsynligheder er ikke-negative), må vi have $P(A) \leq P(B)$.

3. Venn-diagrammet herunder er smart at have i tankerne:



$A \cup B$ er det, som er farvet turkis på figuren. Vi kan skrive $A \cup B = A \cup (B \cap A^{\complement})$, hvor den anden forening

er disjunkt. Dermed fås

$$P(A \cup B) = P(A) + P(B \cap A^{\complement}).$$

Vi kan skrive B som en disjunkt forening $B = (A \cap B) \cup (B \cap A^{\complement})$, og dermed giver den anden regel, at

$$P(A \cap B) + P(B \cap A^{\complement}) = P(B).$$

Dvs. $P(B \cap A^{\complement}) = P(B) - P(A \cap B)$. Indsætter vi dette i udtrykket fra før, får vi, at

$$P(A \cup B) = P(A) + P(B) - P(A \cap B),$$

som var det, der skulle vises.

□

De tre resultater i forrige sætning er særdeles nyttige. De er lettere at huske, hvis man har intuition for, hvad de siger. Den første regel siger, at sandsynligheden for, at begivenhed A ikke finder sted er $1 - P(A)$. Det vil vi også forvente i praksis. Sandsynligheden for at slå en sekser på en sekssidet terning er $\frac{1}{6}$, så sandsynligheden for ikke at slå en sekser må være $\frac{5}{6} = 1 - \frac{1}{6}$. Regel nummer to siger, at en begivenhed, som indeholder en mindre begivenhed, har større sandsynlighed for at ske. Igen stemmer det overens med vores intuition. Sandsynligheden for at slå 1, 2 eller 3 med en terning er større end sandsynligheden for at slå 1 eller 2. For at se, hvorfor den sidste regel gælder, kan det være smart at se det tilhørende Venn-diagram i beviset. For at finde sandsynligheden for, at A eller B finder sted (dvs. $P(A \cup B)$), kan vi lægge $P(A)$ og $P(B)$ sammen. Problemet er bare, at vi tæller $P(A \cap B)$ to gange, så vi skal trække $P(A \cap B)$ fra for at få den rigtige sandsynlighed. Lad os tage nogle eksempler på anvendelser af disse regler.

Eksempel 1.39. Antag, at vi har en sekssidet terning, som vi slår to gange. Hvad er sandsynligheden for at slå to forskellige øjne? Lad A være begivenheden, at man får forskellige øjne på hvert kast. Da er $A^{\complement}$ begivenheden, at man slår det samme på de to kast. Udfaldsrummet er $S = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$, som har $6 \cdot 6 = 36$ elementer, og $A^{\complement} = \{(1,1),(2,2),\ldots,(6,6)\}$ har seks elementer. Alle udfald er lige sandsynlige, så $P(A^{\complement}) = \frac{6}{36} = \frac{1}{6}$. Dermed er

$$P(A) = 1 - P(A^{\complement}) = 1 - \frac{1}{6} = \frac{5}{6}.$$

$\circ$

Eksempel 1.40. Antag, at vi spiller bingo, altså vi trækker lod om et tal mellem 1 og 99 (inklusiv 1 og 99). Alle tal har samme sandsynlighed for at blive trukket. Hvad er sandsynligheden for at trække et tal deleligt med 3 eller 5? Vi har klart $S = \{1,2,\ldots,99\}$. Lad A være begivenheden, at tallet, vi har trukket lod om, er deleligt med 3, dvs. $A = \{3,6,9,\ldots,96,99\}$. Lad B være begivenheden, at tallet er deleligt med 5, dvs. $B = \{5,10,\ldots,90,95\}$. Vi ser, at A har 33 elementer, og at B har 19 elementer. $A \cup B$ er da begivenheden, at tallet er deleligt med 3 eller 5. Vi ser, at $A \cap B = \{15,30,45,60,75,90\}$ har 6 elementer. Sandsynligheden for, at tallet er deleligt med 3 eller 5 bliver da:

$$\begin{aligned} P(A \cup B) &= P(A) + P(B) - P(A \cap B) = \frac{33}{99} + \frac{19}{99} - \frac{6}{99} \\ &= \frac{46}{99} \approx 0{,}46. \end{aligned}$$

$\circ$

Lad os til slut give et resultat, der bruges ofte i videregående sandsynlighedsteori, nemlig Booles ulighed.

Lemma 1.41 (Booles ulighed)**.** Lad $A_1, A_2, \ldots$ være begivenheder. Da har vi

$$P\left(\bigcup_{n=1}^{\infty} A_n\right) \leq \sum_{n=1}^{\infty} P(A_n).$$

Bevis. Ideen er ud fra $A_1, A_2, \ldots$ (hvor vi ikke ved, om de er parvist disjunkte) at konstruere en ny følge af begivenheder, som vi ved er parvist disjunkte, og hvor foreningen af dem er lig $\bigcup_{n=1}^{\infty} A_n$. Lad $B_1 = A_1$, $B_2 = A_2 \setminus A_1$, $B_3 = A_3 \setminus (A_1 \cup A_2)$ osv. I ord kan man sige, at B_n er konstrueret ved at at tage A_n og fjerne alt i $A_1, A_2, \ldots, A_{n-1}$. Det er klart, at $B_1, B_2, \ldots$ er en følge af parvist disjunkte mængder. Men samtidig må

$$\bigcup_{n=1}^{\infty} B_n = \bigcup_{n=1}^{\infty} A_n,$$

hvilket vi viser. Da $B_n \subseteq A_n$ for alle n, har vi klart, at inklusionen $\subseteq$ gælder. Lad nu $x \in \bigcup_{n=1}^{\infty} A_n$. Da ligger x i en af mængderne i foreningen, lad os sige $x \in A_N$. Hvis $x \in B_N$, må x være i foreningen til venstre, og vi er færdige. Hvis $x \notin B_N$ betyder det, at x ligger i én af $A_{N-1}, A_{N-2}, \ldots, A_1$. Hermed kan vi gentage argumentet (formelt med induktion), indtil vi måske når A_1. Men $A_1 = B_1$, og uanset hvad ligger x i $\bigcup_{n=1}^{\infty} B_n$. $B_n \subseteq A_n$ giver $P(B_n) \leq P(A_n)$ for alle n, og regel nummer 2 for sandsynligheder giver

$$P\left(\bigcup_{n=1}^{\infty} A_n\right) = P\left(\bigcup_{n=1}^{\infty} B_n\right) = \sum_{n=1}^{\infty} P(B_n) \leq \sum_{n=1}^{\infty} P(A_n),$$

hvilket var det, der skulle vises. □

Booles ulighed skal fortolkes som, at hvis vi naivt lægger sandsynligheden for en masse begivenheder sammen, så kommer vi generelt til at tælle for meget med. Det gør vi nemlig, hvis der er overlap mellem begivenhederne. Bemærk, at hvis begivenhederne er parvist disjunkte, er uligheden i lemmaet en lighed per definitionen af en sandsynlighed.

Betinget og uafhængig sandsynlighed

Betinget sandsynlighed handler om at regne sandsynligheder ud fra nuværende viden i stedet for den rene sandsynlighed. Hvis man kaster en sekssidet terning, vil sandsynligheden for at slå 1 være $\frac{1}{6}$, men hvis du allerede ved, at tallet er 3 eller mindre, kan slaget kun have været, 1, 2, eller 3. Derfor ville sandsynligheden ændre sig til $\frac{1}{3}$. Den første sandsynlighed er den ubetingede sandsynlighed, hvor den anden er betinget på, at man ved noget om den situation, man er i.

Definition 1.42 (Betinget sandsynlighed)**.** Givet to eksperimenter A, B, da vil deres *betingede sandsynlighed* være

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)},$$

når $P(B) \neq 0$. $P(A|B)$ læses som A givet B.

Eksempel 1.43. Lad os kigge på eksemplet givet tidligere. Vi vil finde sandsynligheden for at slå 1, hvis vi har slået 3 eller mindre. Vi definerer A som at være begivenheden at slå 1 og definerer B som begivenheden at slå 3 eller mindre. Vi starter med at finde $A \cap B$. Siden det at slå 1 og det at slå 3 eller mindre indeholder 1 har vi $A \subset B$, dvs. $A \cap B = A$. Vi mangler derfor kun at finde sandsynlighederne. Vi har, at $P(A \cap B) = P(A) = \frac{1}{6}$ og $P(B) = \frac{1}{2}$. Vi kan nu anvende definition 1.42

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{1}{6}}{\frac{1}{2}} = \frac{1}{3}.$$

Så vi ser, at vores intuition før var korrekt. ∘

Hvad gør vi så, når vores eksperimenter ikke har noget med hinanden at gøre? Hvis vi ville regne sandsynligheden for, at det regner i morgen, givet at jeg havde spist en leverpostejsmad til frokost, så ville den sandsynlighed ikke være forskellig fra den ubetingede sandsynlighed for regn.

Definition 1.44 (Uafhængighed)**.** To eksperimenter siges at være uafhængige, hvis en af følgende ækvivalente betingelser gælder:

1. $P(A|B) = P(A)$
2. $P(B|A) = P(B)$
3. $P(A \cap B) = P(A)P(B)$

Hvis dette ikke er tilfældet, er A og B afhængige eksperimenter.

Den sidste egenskab er meget god i praksis, når man skal regne sandsynligheder.

Eksempel 1.45. Vi kigger igen på vores eksperiment med terninger, hvor A er det at slå 1, og B er det at slå 3 eller under. Vi ser med det samme, at de er afhængige, da $P(A|B) = \frac{1}{3} \neq \frac{1}{6} = P(A)$. Men hvad hvis vi ændrede det lidt, sådan at A bliver det at slå 1 eller 6, og B er det samme. Er de nu uafhængige?
Vi observerer

$$A \cap B = \{1,6\} \cap \{1,2,3\} = \{1\} \implies P(A \cap B) = P(\{1\}) = \frac{1}{6}.$$

Vi observerer yderligere, at

$$P(A) \cdot P(B) = \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6} = P(A \cap B).$$

Fra definition 1.44 fås, at A og B er uafhængige eksperimenter. ∘

2 Diskrete stokastiske variable

Stokastiske variable giver en mere overskuelig måde at beskrive eksperimenter. Vi kunne f.eks. være interesseret i, hvor

mange gange vi får krone ved fem kast med en mønt. Her kunne vi definere A_0 til at være begivenheden, at vi får krone nul gange, A_1 at vi får krone én gang osv. Men allerede ved et simpelt eksempel som det her bliver det uoverskueligt. Vi kunne i stedet lade X betegne antal krone ved de fem kast. Dette er en rolle (blandt mange andre!), en stokastisk variabel kan spille.

Definition 2.1. Lad S være et udfaldsrum. En *stokastisk variabel* X er en funktion $X\colon S \to \mathbb{R}$. Med andre ord tager X elementer i udfaldsrummet og tildeler dem en reel værdi. En stokastisk variabel kaldes *diskret*, hvis der eksisterer en liste $a_1, a_2, \ldots$ sådan at X har sandsynlighed 1 for at antage en af værdierne $a_1, a_2, \ldots$.

Vi skal i dette forløb kun arbejde med diskrete stokastiske variable. Der findes også såkaldte *kontinuerte* stokastiske variable, men for at arbejde med disse, skal man have en del forudsætninger inden for infinitesimalregning.

Eksempel 2.2. Antag, at vi flipper en mønt to gange, hvor hvert kast giver plat eller krone. Hvis P betegner plat og K krone, da er udfaldsrummet $S = \{PP, PK, KP, KK\}$. Lad X betegne antal gange, vi slår krone. Da er X en stokastisk variabel med:

$$X(PP) = 0, \quad X(PK) = X(KP) = 1, \quad X(KK) = 2.$$

∘

Vi er som regel interesseret i sandsynligheden for, at en stokastisk variabel antager en bestemt værdi. F.eks. ser vi, at sandsynligheden for, at $X = 2$ i forrige eksempel er $\frac{1}{4}$.

Definition 2.3. Lad B være en delmængde af $\mathbb{R}$ og X en stokastisk variabel. Da betegner vi *urbilledet* $X^{-1}(B)$ med

$f^{-1}(S)$. Hvis $B = \{x\}$ for et element $x \in \mathbb{R}$ skriver vi blot $(X = x)$ for $X^{-1}(B)$.

Selvom $(X \in B)$ blot er en omskrivning af urbilledet som introduceret i den faglige intro, så er det en rigtig smart notation. Som sandsynlighedsteoretikere vil vi altid skrive $(X \in B)$ eller $(X = x)$ i stedet for $X^{-1}(B)$ eller $X^{-1}(\{x\})$, fordi $(X \in B)$ og $(X = x)$ bedre illustrerer, hvad vi er interesseret i. $(X = x)$ er alle udfald $s \in S$, hvor $X(s) = x$, eller sagt endnu kortere: Alle udfald, hvor X er lig x.

Eksempel 2.4. Lad X være den stokastiske variabel fra forrige eksempel. Da er

$$P(X = 0) = \frac{1}{4}, \quad P(X = 1) = \frac{1}{2}, \quad P(X = 2) = \frac{1}{4}.$$

∘

I forrige eksempel beskrev vi sandsynlighederne for alle begivenhederne $X = x$ for $x \in \mathbb{R}$. Vi har beskrevet det, der kaldes for en *tæthedsfunktion* for en stokastisk variabel.

Definition 2.5. For en stokastisk variabel X kaldes funktionen $p_X \colon \mathbb{R} \to \mathbb{R}$ givet ved $p_X(x) = P(X = x)$ for *tæthedsfunktionen* for X. De punkter $x \in \mathbb{R}$, hvor $p_X(x) > 0$, kaldes for *støtten* for X.

Vi vil til tider kalde en tæthedsfunktion for en *PMF*, som er en forkortelse for det engelske *probability mass function*.

Eksempel 2.6. Den stokastiske variabel fra forrige eksempel har PMF

$$p_X(x) = P(X = x) = \begin{cases} \frac{1}{4}, & \text{hvis } x = 0, 2 \\ \frac{1}{2}, & \text{hvis } x = 1 \\ 0, & \text{ellers} \end{cases}$$

∘

Hvis vi har tæthedsfunktionen for en stokastisk variabel, har vi al den information, vi kan ønske os. Derfor vil man som regel angive tæthedsfunktionen, når man skal specificere en stokastisk variabel.

Eksempel 2.7. Lad os antage, at vi slår med to sekssidede terninger. Lad X betegne summen af de to kast. For at bestemme tæthedsfunktionen for X skal vi udregne alle punktsandsynligheder. Her er det smart at lave en tabel:

Tabel 1.1: Værdien af X til de forskellige udfald af de to terningekast.

Terning 1 \2	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

Alle 36 mulige udfald har samme sandsynlighed, så vi aflæser

$$
\begin{aligned}
P(X=2) = P(X=12) &= \frac{1}{36}, \\
P(X=3) = P(X=11) &= \frac{2}{36}, \\
P(X=4) = P(X=10) &= \frac{3}{36}, \\
P(X=5) = P(X=9) &= \frac{4}{36}, \\
P(X=6) = P(X=8) &= \frac{5}{36}, \\
P(X=7) &= \frac{6}{36},
\end{aligned}
$$

eller vi kunne skrive:

$$p_X(x) = \begin{cases} \frac{1}{36}, & \text{hvis } x = 2, 12 \\ \frac{2}{36}, & \text{hvis } x = 3, 11 \\ \frac{3}{36}, & \text{hvis } x = 4, 10 \\ \frac{4}{36}, & \text{hvis } x = 5, 9 \\ \frac{5}{36}, & \text{hvis } x = 6, 8 \\ \frac{6}{36}, & \text{hvis } x = 7 \\ 0, & \text{ellers} \end{cases}$$

∘

Bemærk, at vi i begge eksempler fra før har, at tæthedsfunktionen summerer til 1. Sagt matematisk, hvis $x_1, x_2, \ldots$ er støtten for X, da er $\sum_{i=1}^{\infty} p_X(x_i) = 1$. Dette gælder generelt for tæthedsfunktioner.

Proposition 2.8. Lad X være en stokastisk variabel med støtten $x_1, x_2, \ldots$. Tæthedsfunktionen opfylder, at $p_X(x_i) > 0$ og $p_X(x) = 0$, hvis x ikke er blandt $x_i$erne, samt at $\sum_{i=1}^{\infty} p_X(x_i) = 1$.

Bevis. Den første betingelse holder, fordi sandsynligheder ikke er negative. Den anden egenskab holder, fordi X skal antage en værdi (husk, at en stokastisk variabel er en funktion!), og begivenhederne $(X = x_i)$ er disjunkte, så

$$\sum_{i=1}^{\infty} p_X(x_i) = P\left(\bigcup_{i=1}^{\infty} (X = x_i)\right) = 1.$$

□

Ligesom at to begivenheder kan være uafhængige, kan to (eller flere) stokastiske variable også være det.

Definition 2.9. Lad X og Y være diskrete stokastiske variable på samme udfaldsrum S. Da er X og Y *uafhængige*,

hvis det for alle x i støtten for X og alle y i støtten for Y gælder, at

$$P(X = x, Y = y) = P(X = x)P(Y = y)$$

Hvis to stokastiske variable ikke er uafhængige, kaldes de *afhængige*. Denne definition generaliseres let til et vilkårligt endeligt antal stokastiske variable. $X_1, X_2, \ldots, X_n$ siges at være uafhængige, hvis

$$\begin{aligned} &P(X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n) \\ &\quad = P(X_1 = x_1)P(X_2 = x_1) \cdots P(X_n = x_n) \end{aligned}$$

for alle x_i i støtten for X_i for $i = 1, \ldots, n$.

Vi antager i mange tilfælde, at to variable er uafhængige. F.eks. antager vi det implicit, når vi kaster med en terning flere gange ved at sige, at hvert terningkast ikke afhænger af de andre.

Middelværdi og varians

Vi skal nu introducere nogle nyttige størrelser, man kan tilknytte stokastiske variable. Først introducerer vi middelværdien og viser nogle egenskaber for denne.

Definition 2.10. Lad X være en stokastisk variabel, som antager værdierne $x_1, x_2, \ldots$ med positiv sandsynlighed. Hvis

$$\sum_{i=1}^{\infty} |x_i| P(X = x_i) < \infty$$

definerer vi *middelværdien* EX til at være

$$EX = \sum_{i=1}^{\infty} x_i P(X = x_i)$$

E kommer fra det engelske *expectation*.

Man kan tænke på middelværdien som et vægtet gennemsnit. I har (næsten) sikkert udregnet middelværdier før. Bemærk, at middelværdien altid eksisterer for en stokastisk variabel med endelig støtte.

Eksempel 2.11. Lad X være den stokastiske variabel defineret som antal øjne ved et kast med en sekssidet terning. Da er

$$\begin{aligned} EX &= \sum_{i=1}^{6} i \cdot P(X = i) = \sum_{i=1}^{6} i \cdot \frac{1}{6} \\ &= \frac{1}{6}(1+2+3+4+5+6) \\ &= \frac{21}{6} = \frac{7}{2} \end{aligned}$$

Man kan fortolke dette som, at hvis vi slår med en terning, vil den gennemsnitlige værdi af vores kast være 3,5. ∘

Det kan også hænde, at middelværdien ikke eksisterer for en stokastisk variabel, som det følgende eksempel viser.

Eksempel 2.12. Definér den stokastiske variabel X ved $X(x) = x^3$ for alle $x \in \mathbb{R}$. Antag, at $P(X = n) = \frac{6}{\pi^2 n^2}$ for alle $n \in \mathbb{N}$ og $P(X = x) = 0$ for $x \notin \mathbb{N}$. Dermed er tætheden for X givet ved

$$p_X(x) = \begin{cases} \frac{6}{\pi^2 x^2}, & \text{hvis } x \in \mathbb{N} \\ 0, & \text{ellers} \end{cases}.$$

Lad os for god orden skyld tjekke, at denne tæthed faktisk er en tæthed. $p_X(x)$ er altid ikke-negativ, og vi har

$$\sum_{x \in \mathbb{R}} p_X(x) = \sum_{n=1}^{\infty} p_X(n) = \sum_{n=1}^{\infty} \frac{6}{\pi^2 n^2} = \frac{6}{\pi^2} \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{6}{\pi^2} \frac{\pi^2}{6} = 1.$$

Vi kan nu udregne

$$\sum_{x \in \mathbb{R}} |x| \cdot P(X = x) = \sum_{n=1}^{\infty} n \cdot \frac{6}{\pi^2 n^2} = \frac{6}{\pi^2} \sum_{n=1}^{\infty} \frac{1}{n} = \infty,$$

hvor vi har brugt eksempel 1.5. Dermed eksisterer middelværdien for X ikke. ∘

Forrige eksempel kan sagtens virke kunstigt konstrueret, og det er ikke helt forkert. De eksempler på stokastiske variable, vi er interesserede i, har altid middelværdi. En af de vigtigste egenskaber for middelværdi er *linearitet*.

Sætning 2.13 (Linearitet for middelværdi)**.** Lad X og Y være stokastiske variable på samme udfaldsrum med middelværdi. Da er

$$E(X+Y) = EX + EY, \quad \text{og} \quad E(cX) = cEX.$$

for alle reelle tal c.

For at vise dennne sætning, viser vi følgende hjælperesultat, der giver en alternativ måde at beregne middelværdier.

Lemma 2.14. Lad X være en diskret stokastisk variabel med middelværdi. Da er

$$EX = \sum_{s \in S} X(s)P(\{s\}).$$

Bevis. Middelværdien EX er per definition lig summen af alle $x \cdot P(X = x)$, hvor x gennemløber alle reelle tal x i støtten for X. Mængden $(X = x)$ er alle de $s \in S$, hvor $X(s) = x$. Dermed er

$$P(X = x) = \sum_{\substack{s \in S \\ X(s)=x}} P(\{s\}),$$

per den anden regel for sandsynligheder, thi alle etpunktsmængderne $\{s\}$ selvfølgelig er disjunkte. Da vi summerer over de s, hvor $X(s) = x$, får vi da

$$xP(X = x) = \sum_{\substack{s \in S \\ X(s)=x}} X(s)P(\{s\}).$$

Bemærk, at begivenhederne $\{s \in S \mid X(s) = x\}$ er disjunkte. Lader vi x gennemløbe alle mulige værdier $x_1, x_2, \ldots$ for X, får vi

$$\begin{aligned} EX &= \sum_{i=1}^{\infty} x_i P(X = x_i) = \sum_{i=1}^{\infty} \sum_{\substack{s \in S \\ X(s)=x_i}} X(s) P(\{s\}) \\ &= \sum_{s \in S} X(s) P(\{s\}) \end{aligned}$$

som ønsket. □

Definitionen af middelværdi siger, at vi udregner EX ved at tage det vægtede gennemsnit, hvor summen gennemløber mulige værdier for X. Dette svarer til at udregne middelværdien ved at gruppere de $s \in S$ sammen, hvor $X(s) = x$. Lemmaet siger, at vi kan udregne middelværdien ved ikke at gruppere og i stedet regne med hver punktsandsynlighed. Med dette hjælperesultat er sætning 2.13 nem at bevise:

Bevis for sætning 2.13. Vi har

$$\begin{aligned} EX + EY &= \sum_{s \in S} X(s) P(\{s\}) + \sum_{s \in S} Y(s) P(\{s\}) \\ &= \sum_{s \in S} (X(s) + Y(s)) P(\{s\}) = E(X + Y) \end{aligned}$$

og for alle konstanter $c \in \mathbb{R}$:

$$E(cX) = \sum_{s \in S} cX(s) P(\{s\}) = c \sum_{s \in S} X(s) P(\{s\}) = cEX.$$

□

Eksempel 2.15. Lad os slå med en sekssidet terning seks gange. Lad X_1 betegne antal øjne i første kast, X_2 antal øjne i andet kast og så videre. Hvad er middelværdien af det samlede antal øjne i de seks kast? Vi har $EX_1 = EX_2 = \cdots = EX_6 = 3.5$ fra eksempel 2.11. Dermed har vi

$$E(X_1 + \cdots + X_6) = 6 \cdot 3.5 = 21.$$

○

Eksempel 2.16. Lad X være en stokastisk variabel med $P(X = c) = 1$. X er altså med sandsynlighed 1 lig en konstant $c \in \mathbb{R}$. Da er tætheden givet ved

$$p_X(x) = \begin{cases} 1, & \text{hvis } x = c \\ 0, & \text{ellers} \end{cases}$$

og middelværdien er

$$EX = c \cdot P(X = c) = c.$$

○

Eksempel 2.17. Lad X være en stokastisk variabel med middelværdi. Da er $Y = X - EX$ igen en stokastisk variabel med middelværdi

$$EY = E(X - EX) = EX - E(EX) = EX - EX = 0$$

per linearitet. En stokastisk variabel med middelværdi 0 kaldes nogle gange en *centraliseret* stokastisk variabel. ○

En anden nyttig egenskab for middelværdier indgår, når vi betragter produktet af uafhængige stokastiske variable.

Proposition 2.18. Lad X og Y være diskrete stokastiske variable på samme udfaldsrum. Hvis X og Y er uafhængige, gælder at $EXY = EXEY$.

Bevis. Lad $x_1, x_2, \ldots$ være støtten for X og $y_1, y_2, \ldots$ være støtten for Y. Det er klart, at alle produkter af formen $x_i y_j$

for $i, j = 1, 2, \ldots$ må være støtten for XY. Dermed har vi

$$\begin{aligned} EXY &= \sum_{i,j=1}^{\infty} x_i y_j P(XY = x_i y_j) \\ &= \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} x_i y_j P(X = x_i, Y = y_j) \\ &= \sum_{i=1}^{\infty} x_i \sum_{j=1}^{\infty} y_j P(X = x_i) P(Y = y_j) \\ &= \left(\sum_{i=1}^{\infty} x_i P(X = x_i) \right) \left(\sum_{j=1}^{\infty} y_j P(Y = y_j) \right) \\ &= EXEY \end{aligned}$$

som ønsket. □

Korollar 2.19. Lad $X_1, X_2, \ldots, X_n$ være uafhængige stokastiske variable med middelværdi. Da gælder

$$EX_1 X_2 \cdots X_n = EX_1 EX_2 \cdots EX_n.$$

Bevis. Korollaret følger af et direkte induktionsargument. Det gælder trivielt for $n = 1$, så lad $n > 1$. Antag, at resultatet holder for $n - 1$ uafhængige stokastiske variable, og lad $X_1, X_2, \ldots, X_n$ være uafhængige. Da har vi per induktionsantagelsen samt forrige sætning, at

$$\begin{aligned} EX_1 X_2 \cdots X_n &= E(X_1 X_2 \cdots X_{n-1}) X_n \\ &= EX_1 X_2 \cdots X_{n-1} EX_n \\ &= EX_1 EX_2 \cdots EX_n \end{aligned}$$

som ønsket. □

Det er smart, at vi kan udregne middelværdien af summer af stokastiske variable samt produkter af uafhængige stokastiske variable, såfremt man kender hver enkel variabels middelværdi. Men hvad gør vi, hvis vi har en stokastisk

variabel X og f.eks. gerne vil bestemme $E(X^2)$? Eller hvad med $E(\sqrt{X})$ og $E(e^X)$? Givet en funktion $g : \mathbb{R} \to \mathbb{R}$ vil vi gerne kunne bestemme $Eg(X)$. Vi kan selvfølgelig bestemme tætheden for $g(X)$ og bruge definitionen af middelværdi. Dog findes der en endnu nemmere måde, som vi introducerer nu. Sætningen kaldes til tider for LOTUS (Law Of The Unconscious Statistician eller på dansk: den bevidstløse statistikers lov).

Sætning 2.20 (LOTUS)**.** Lad X være en diskret stokastisk variabel og $g : \mathbb{R} \to \mathbb{R}$ en funktion. Lad $x_1, x_2, \ldots$ være støtten for X. Da er

$$Eg(X) = \sum_{i=1}^{\infty} g(x_i)P(X = x_i)$$

Bevis. Vi benytter lemma 2.14 og får

$$\begin{aligned} Eg(X) &= \sum_{s\in S} g(X(s))P(\{s\}) = \sum_{i=1}^{\infty} \sum_{\substack{s\in S \\ X(s)=x_i}} g(X(s))P(\{s\}) \\ &= \sum_{i=1}^{\infty} g(x_i) \sum_{\substack{s\in S \\ X(s)=x_i}} P(\{s\}) = \sum_{i=1}^{\infty} g(x_i)P(X = x_i). \end{aligned}$$

□

Inden vi definerer varians, er det smart at definere momenter. Middelværdien for en stokastisk variabel X kaldes også for *førstemomentet* for X. Ligeledes kaldes middelværdien af X^2 (såfremt den findes) for *andenmomentet* og så videre. Vi gør dette til en definition:

Definition 2.21. Lad X være en stokastisk variabel, hvor $E(|X|^k) < \infty$. Da kaldes $E\left(X^k\right)$ for det $k$te *moment* for X. Vi skriver som regel EX^k i stedet for $E(X^k)$.

Ligesom med middelværdien bemærker vi, at alle stokastiske variable, som kun antager endeligt mange værdier med positiv sandsynlighed, opfylder $E|X|^k < \infty$ for alle værdier af k. Dermed har sådanne variable $k$te moment for alle $k \in \mathbb{N}$.

Eksempel 2.22. Lad X være den stokastiske variabel, der er lig antal øjne på et terningekast med en sekssidet terning. Per LOTUS er

$$\begin{aligned} EX^2 &= \sum_{i=1}^{6} i^2 P(X = i) = \frac{1}{6}(1 + 4 + 9 + 16 + 25 + 36) \\ &= \frac{91}{6} \approx 15{,}17. \end{aligned}$$

∘

Definition 2.23. Lad X være en stokastisk variabel. Såfremt $EX^2 < \infty$ defineres *variansen* af X til

$$VX = E(X - EX)^2.$$

Med andre ord er variansen det centraliserede andenmoment for X.

Variansen angiver, hvor langt X gennemsnitligt er fra sin middelværdi. Vi har en række egenskaber for varians.

Proposition 2.24. Lad X være en stokastisk variabel med andenmoment. Da gælder:

1. $VX = EX^2 - (EX)^2$.
2. $V(X + c) = VX$ for alle $c \in \mathbb{R}$.
3. $V(cX) = c^2 VX$ for alle $c \in \mathbb{R}$.

Bevis. 1. Vi udregner ved at bruge linearitet for middelværdier:

$$\begin{aligned} VX &= E(X - EX)^2 = E((X - EX)(X - EX)) \\ &= E(X^2 + (EX)^2 - 2EX \cdot X) \\ &= EX^2 + E((EX)^2) - 2(EX)^2 \\ &= EX^2 + (EX)^2 - 2(EX)^2 = EX^2 - (EX)^2. \end{aligned}$$

2. Lad $c \in \mathbb{R}$. Vi har da

$$\begin{aligned} V(X + c) &= E(X + c - E(X + c))^2 \\ &= E(X + c - EX + c)^2 \\ &= E(X - EX)^2 = VX. \end{aligned}$$

3. Øvelse. Se opgave 5.49.

□

Eksempel 2.25. Lad atter X være antal øjne på et kast med en sekssidet terning. Da er variansen:

$$VX = EX^2 - (EX)^2 = \frac{91}{6} - \left(\frac{7}{2}\right)^2 = \frac{35}{12}.$$

∘

Variansen af summer af variable er generelt meget svær at beregne. Dog er dette ikke tilfældet, hvis variablene er uafhængige. Følgende resultat bliver bl.a. nyttigt, når vi skal bestemme variansen af binomialfordelingen senere i forløbet.

Proposition 2.26. Lad X og Y være uafhængige stokastiske variable med andenmoment. Da gælder $V(X + Y) = VX + VY$.

Bevis. Vi har per proposition 2.24 samt proposition 2.18, at

$$\begin{aligned} V(X+Y) =& E(X+Y)^2 - (E(X+Y))^2 \\ =& E(X^2+Y^2+2XY) - (EX+EY)^2 \\ =& EX^2 + EY^2 + 2EXY - (EX)^2 \\ & - (EY)^2 - 2EXEY \\ =& EX^2 - (EX)^2 + EY^2 - (EY)^2 \\ & + 2EXEY - 2EXEY \\ =& EX^2 - (EX)^2 + EY^2 - (EY)^2 = VX + VY, \end{aligned}$$

hvilket viser det ønskede. □

Korollar 2.27. Lad $X_1, X_2, \ldots, X_n$ være uafhængige diskrete stokastiske variable med andenmoment. Da gælder

$$V(X_1 + X_2 + \cdots + X_n) = VX_1 + VX_2 + \cdots + VX_n.$$

Bevis. Se opgave 5.52. □

3 Diskrete fordelinger

Binomialfordelingen

Binomialfordelingen er en af de vigtigste diskrete fordelinger. Vi introducerer først et simpelt, omend vigtigt, specialtilfælde, nemlig *Bernoulli-fordelingen.*

Definition 3.1. En stokastisk variabel X siges at være *Bernoullifordelt* med parameter $p \in (0,1)$ hvis X har tæthed

$$p_X(x) = \begin{cases} p, & \text{hvis } x = 1 \\ 1-p, & \text{hvis } x = 0 \\ 0, & \text{ellers.} \end{cases}$$

En Bernoulli-variabel er altså en variabel, der antager værdien 1 med sandsynlighed p og 0 med sandsynlighed $1-p$. Man kan fortolke sådan en variabel som udfaldet af et eksperiment, der enten lykkedes (1) eller mislykkedes (0), og hvor sandsynligheden er p for succes. Af samme årsag kaldes p ofte for *succesparameteren*.

Eksempel 3.2. Lad X være udfaldet af et kast med en fair mønt, hvor $X = 1$ indikerer krone og $X = 0$ plat. Da er X Bernoulli-fordelt med succesparameter $\frac{1}{2}$. ∘

Middelværdien og variansen for en Bernoullifordelt variabel er simpel at udregne. Vi noterer os resultatet her og overlader udregningen som en øvelse.

Sætning 3.3. For en Bernoulli-fordelt variabel X med succesparameter p gælder, at $EX = p$ og $VX = p(1-p)$.

Bevis. Se opgave 5.55. □

Definition 3.4. Lad $X_1, X_2, \ldots, X_n$ være n Bernoulli-fordelte variable med samme succeparameter p. Da siges $X = X_1 + \cdots + X_n$ at være *binomialfordelt* med parametrene n og p.

Altså beskriver en binomialfordelt variabel antallet at succeser i n ens forsøg, hvor et forsøg har sandsynlighed p for at lykkedes. For at kunne arbejde med binomialfordelingen, skal vi bestemme dens tæthedsfunktion.

Proposition 3.5. Lad X være binomialfordelt med parametre n og p. Da er tæthedsfunktionen for X givet ved

$$p_X(x) = \binom{n}{x} p^x (1-p)^{n-x}$$

for $x = 0, 1, \ldots, n$ og $p_X(x) = 0$ ellers.

Bevis. $p_X(x) = P(X = x)$ er sandsynligheden for x succeser i de n forsøg. Denne er klart 0, hvis $x < 0$ eller $x > n$. Hvis x er i blandt $0, 1, \ldots, n$, er sandsynligheden for x succeser i en given streng af n forsøg lig $p^x(1-p)^{n-x}$ (sandsynlighed p for hver succes, sandsynlighed $1-p$ for hver fiasko, som der må være $n-x$ af). Vi skal da blot tælle antal strenge med x succeser. Vi behøver kun at specificere, hvor succeserne skal være, og derfor er dette lig antal kombinationer af længde x, man kan lave ud fra n elementer, dvs. $\binom{n}{x}$. Vi konkluderer, at

$$P(X = x) = \binom{n}{x} p^x (1-p)^{n-x}$$

for $x = 0, 1, \ldots, n$ og nul ellers som ønsket. Vi mangler blot at tjekke, at dette er en valid tæthedsfunktion. Den er klart ikke-negativ. For at vise, at tæthederne summerer til 1, anvender vi binomialsætningen, sætning 1.33. Denne giver

$$\sum_{i=0}^{n} P(X = i) = \sum_{i=0}^{n} \binom{n}{i} p^i (1-p)^{n-i} = (p+(1-p))^n = 1^n = 1,$$

og beviset er færdigt. □

Inden vi tager et eksempel på en binomialfordeling, fastlægger vi middelværdien og variansen for binomialfordelingen. Bemærk, at disse begge er veldefinerede, eftersom en binomialfordelt variabel kun antager endeligt mange værdier med positiv sandsynlighed.

Sætning 3.6. For en binomialfordelt variabel X med parametre n og p gælder, at

$$EX = np \quad \text{og} \quad VX = np(1-p).$$

Bevis. X er en sum af n uafhængige Bernoulli-fordelte variable med succesparameter p. Disse har alle middelværdi p og varians $p(1-p)$ jævnfør sætning 3.3. Dermed er $EX = np$

per linearitet af middelværdier. Korollar 2.27 giver, at $VX = np(1-p)$. □

Eksempel 3.7. Det er typisk, at flyselskaber overbooker deres fly for at sikre, at deres fly ikke letter med tomme sæder. Lad os sige, at vi har et fly med 100 sæder, som vi sælger 105 billetter til. Lad os antage, at hver person rejser uafhængigt af de andre passagerer (så ingen skal på ferie sammen), og at hver person har sandsynligheden 0.9 for at dukke op, inden flyet skal lette. Hvad er sandsynligheden for, at vi ikke har nok sæder?

Lad X betegne antallet af passagerer, der dukker op i tide. Da er X binomialfordelt med parameter $n = 105$ og $p = 0.9$. Vi er interesseret i sandsynligheden $P(X \geq 101)$. Denne sandsynlighed er lig summen $P(X = 101) + P(X = 102) + \cdots + P(X = 105)$. Denne udregnes til

$$\begin{aligned} P(X \geq 101) &= \sum_{i=101}^{105} P(X = i) \\ &= \sum_{i=101}^{105} \binom{105}{i} 0.9^i (1-0.9)^{105-i} \approx 0.017. \end{aligned}$$

Altså er der mindre end 2% risiko for, at vi skal afvise en passager. Så det kan sikkert betale sig at sælge lidt for mange billetter. Hvis vi valgte at sælge 110 billetter, ville risikoen være ca. 0.33. Altså ville vi skulle afvise en eller flere passagerer ved ca. hver tredje afgang. ○

Poisson-fordeling

Vi ønsker at finde en sandsynlighedsfordeling for, hvor mange arbejdsulykker, der sker på en losseplads inden for en måned. Dette ligner ikke en binomial fordeling, men vi kan finde en måde at kæde dem sammen på. Vi starter med at dele vores periode ind i et antal intervaller, n, sådan at inden for hvert

tidsinterval kan der maksimalt være én arbejdsulykke, ellers vil det have sandsynlighed 0. Vi kan derfor dele problemet op i to tilfælde:

$$\begin{aligned} P(\text{At ingen ulykker sker i intervallet}) &= 1-p, \\ P(\text{At 1 ulykke sker i intervallet}) &= p, \\ P(\text{At mere end 1 ulykke sker i intervallet}) &= 0. \end{aligned}$$

Vi ser nu, at dette er binomialfordelt med sandsynlighed p. Vi har nu to problemer. Der er ikke nogen unik måde at vælge disse intervaller på, og vi kender ikke p og n. Vi observerer også, at jo større n, vi vælger, jo lavere bliver sandsynligheden p for, at en ulykke sker i et specifikt interval. Vi ønsker at finde fordelingen, når n er meget stor, da vi så har et stort antal intervaller. Vi sætter $\lambda = pn$, og følgende kan vises:

$$\lim_{n\to\infty} \binom{n}{y} p^y (1-p)^{n-y} = \frac{\lambda^y}{y!} e^{-\lambda}.$$

Når en stokastisk variabel har denne fordeling, siger vi, at den er Poisson-fordelt. Eksemplet med arbejdsulykker er en Poisson-fordelt stokastisk variabel. Vi ser også, at for store n og små p kan Poisson fordelingen approksimere binomialfordelingen. En tommelfinderregel er, at når $\lambda \leq 7$. Vi har derfor følgende definition for Poisson-fordelingen:

Definition 3.8 (Poisson-fordeling)**.** Lad Y være en stokastisk variable. Da siges Y at være Poisson-fordelt hvis og kun hvis

$$p(y) = \frac{\lambda^y}{y!} e^{-\lambda},$$

for $\lambda > 0$ og $y \in \mathbb{N}_0$

Ydermere så er både middelværdien og variansen for en Poisson fordeling λ.

Sætning 3.9 (Middelværdi og varians for Poisson)**.** Lad Y være en Poisson fordelt stokastisk variabel med parameter λ. Vi har, at

$$\mu = E(Y) = \lambda,$$
$$\sigma^2 = V(Y) = \lambda.$$

Bevis. Per definition af middelværdien, ganger vi y på vores fordeling og summer over alle y i udfaldsrummet. Vi har derfor

$$E(Y) = \sum_{y=0}^{\infty} y \frac{\lambda^y e^{-\lambda}}{y!}$$

Siden det første led i summen er 0, har vi

$$\sum_{y=0}^{\infty} y \frac{\lambda^y e^{-\lambda}}{y!} = \sum_{y=1}^{\infty} y \frac{\lambda^y e^{-\lambda}}{y!}.$$

Vi ganger og deler også med y, og har derfor

$$\sum_{y=1}^{\infty} y \frac{\lambda^y e^{-\lambda}}{y!} = \sum_{y=1}^{\infty} \frac{\lambda^y e^{-\lambda}}{(y-1)!}$$

Ved at sætte $z = y - 1$ ændre vi indeks i summen

$$\sum_{y=1}^{\infty} \frac{\lambda^y e^{-\lambda}}{(y-1)!} = \sum_{z=0}^{\infty} \frac{\lambda^{z+1} e^{-\lambda}}{z!}.$$

Vi husker at $\lambda^{z+1} = \lambda \cdot \lambda^z$ og at vi kan tage termer ud af summen, som ikke afhænger af indeks. Vi har derfor

$$\sum_{z=0}^{\infty} \frac{\lambda^{z+1} e^{-\lambda}}{z!} = \lambda \sum_{z=0}^{\infty} \frac{\lambda^z e^{-\lambda}}{z!} = \lambda \sum_{z=0}^{\infty} p(z) = \lambda,$$

da summen over alle værdier i udfaldsrummet for sandsynlighedsfunktionen giver 1. Vi har derfor, at $E(Y) = \lambda$. Bemærk, at dette både viser, at middelværdien eksisterer (da alle led

i summen er positive), og hvad middelværdien er. Per definition af varians har vi

$$V(Y) = E(Y^2) - E(Y)^2.$$

Fra før har vi fundet middelværdien og har derfor

$$V(Y) = E(Y^2) - \lambda^2.$$

Ved at bruge LOTUS får vi

$$E(Y^2) = \sum_{y=0}^{\infty} y^2 \frac{\lambda^y e^{-\lambda}}{y!}.$$

Vi ser ligesom før, at første led er 0, og igen trækker vi et λ ud, men denne gang trækker vi også $e^{-\lambda}$ ud. Vi reducerer også med y. Vi har altså

$$\sum_{y=0}^{\infty} y^2 \frac{\lambda^y e^{-\lambda}}{y!} = \lambda e^{-\lambda} \sum_{y=1}^{\infty} y \frac{\lambda^{(y-1)}}{(y-1)!}.$$

Vi deler nu summerne i to, da vi ser, at tælleren har et $(y-1)!$, og vi gerne vil reducere det. Vi har

$$\begin{aligned} &\lambda e^{-\lambda} \sum_{y=1}^{\infty} y \frac{\lambda^{(y-1)}}{(y-1)!} \\ &= \lambda e^{-\lambda} \left(\sum_{y=1}^{\infty} (y-1) \frac{\lambda^{(y-1)}}{(y-1)!} + \sum_{y=1}^{\infty} \frac{\lambda^{(y-1)}}{(y-1)!} \right). \end{aligned}$$

Vi ser at i den venstre sum er led 1 nul, og at vi kan reducere $y-1$. Vi får

$$\begin{aligned} &\lambda e^{-\lambda} \left(\sum_{y=1}^{\infty} (y-1) \frac{\lambda^{(y-1)}}{(y-1)!} + \sum_{y=1}^{\infty} \frac{\lambda^{(y-1)}}{(y-1)!} \right) \\ &= \lambda e^{-\lambda} \left(\sum_{y=2}^{\infty} \frac{\lambda^{(y-1)}}{(y-2)!} + \sum_{y=1}^{\infty} \frac{\lambda^{(y-1)}}{(y-1)!} \right). \end{aligned}$$

Vi kan igen trække λ ud, og ved at sætte $i = y-2$ og $j = y-1$ skifte indekser på summerne. Det giver os

$$\lambda e^{-\lambda}\left(\sum_{y=2}^{\infty}\frac{\lambda^{(y-1)}}{(y-2)!}+\sum_{y=1}^{\infty}\frac{\lambda^{(y-1)}}{(y-1)!}\right)$$
$$=\lambda e^{-\lambda}\left(\lambda\sum_{i=0}^{\infty}\frac{\lambda^{i}}{i!}+\sum_{j=0}^{\infty}\frac{\lambda^{j}}{j!}\right).$$

Vi bruger nu at $e^x = \sum_{n=0}^{\infty}\frac{x^n}{n!}$ som giver os

$$\lambda e^{-\lambda}\left(\lambda\sum_{i=0}^{\infty}\frac{\lambda^{i}}{i!}+\sum_{j=0}^{\infty}\frac{\lambda^{j}}{j!}\right)$$
$$=\lambda e^{-\lambda}(\lambda e^{\lambda}+e^{\lambda})=\lambda^2 e^{\lambda-\lambda}+\lambda e^{\lambda-\lambda}=\lambda^2+\lambda.$$

Vi har nu $E(Y^2) = \lambda^2 + \lambda$ og derved

$$V(Y) = E(Y^2) - E(Y)^2 = \lambda^2 + \lambda - \lambda^2 = \lambda$$

□

Eksempel 3.10. Vi vil gerne undersøge en almindelig politibetjents job. Han skal besøge nogle specifikke steder i byen, når han går sin rute hver dag. Han besøger $Y = 0,1,2,\ldots$ gange hver lokation hver time, og i gennemsnit besøger han hvert sted 2 gange i timen. Vi antager at Y er Poisson fordelt. Vi vil nu gerne finde sandsynligheden for, at han ikke når sin lokalisation inden for timen. Vi vil også gerne finde sandsynligheden for at han når den mindst 3 gange inden for timen.

Vi starter med to observationer. Den første er, at vores tidsinterval er 1 time, og den anden er, at siden han i gennemsnit når hvert sted 2 gange, har vi $\lambda = 2$. Vi kigger nu på sandsynligheden for, at han ikke når lokationen på sin rute. Den er

$$P(Y=0)=\frac{2^0 e^{-2}}{0!}=e^{-2}\approx 0{,}135335.$$

Det næste, vi gerne vil finde, er sandsynligheden for, at han når det mindst 3 gange. Den er $P(Y \geq 3)$. Her kan vi bruge egenskaben at sandsynligheder altid summer til 1, så $P(Y \geq 3) = 1 - P(Y \leq 2)$. Den er

$$\begin{aligned} 1 - \sum_{y=0}^{2} p(y) &= 1 - \sum_{y=0}^{2} \frac{2^y}{y!} e^{-2} = 1 - e^{-2} + 2e^{-2} + 2e^{-2} \\ &= 1 - 5e^{-2} \approx 0{,}3233236. \end{aligned}$$

∘

Eksempel 3.11. Vi er givet en stokastisk variabel Y, som vi har fået at vide er binomialfordelt, hvor $n = 800$ og $p = 0{,}005$, men den giver ikke så helt så præcise resultater som vi får, når vi udfører vores eksperimenter. Vi mistænker, at en Poisson-fordeling kan være bedre i stedet for binomialfordelingen, og finder $P(Y \leq 2)$ med den fordeling.
Vi starter med at finde λ, som er givet ved $n \cdot p = 800 \cdot 0{,}005 = 4$. Det giver os tætheden

$$p_Y(y) = \frac{4^y}{y!} e^{-4}.$$

Vi kan nu finde sandsynlighen for, at Y er mindre end 2:

$$\begin{aligned} P(Y \leq 2) &= \sum_{y=0}^{2} \frac{4^y}{y!} e^{-4} = e^{-4} + 4e^{-4} + 8e^{-4} \\ &= 13e^{-4} \approx 0{,}23811, \end{aligned}$$

hvor binomialfordelingen giver 0,23736. Så vores formodning om, at Poisson-fordelingen approksimerer binomialfordelingen, passer i dette tilfælde. ∘

Inden for Poisson-fordelinger er det også meget almindeligt at have tidsperioder længere end det givet for λ. Hvis antallet af observationer inden for tidsintervallerne er uafhængige, kalder man det en Poisson-proces og $\lambda_{proces} = a\lambda_Y$, hvor a er antal tidsperioder.

Eksempel 3.12. Som vi har set tidligere, kan vi antage, at antallet af arbejdsulykker er Poisson-fordelte. En bilfabrik har haft 13 ulykker over de sidste 3 måneder, og har i gennemsnit 3 ulykker per måned. Vi vil gerne undersøge, om det er usædvanligt, at fabrikken oplever 13 ulykker over 3 måneder.
Vi starter med at finde vores nye λ. Da vores periode er på 3 måneder, og enheden for vores Poisson er 1 måned har vi $\lambda_{proces} = 3 \cdot \lambda_Y = 3 \cdot 3 = 9$. I gennemsnit vil der være 9 ulykker på 3 måneder under antagelsen, at ulykkerne er uafhængige af hinanden. Vi skal nu finde sandsynligheden for, at der er 13 eller flere ulykker på de 3 måneder. Vi skal altså finde $P(Y \geq 13)$. Vi har

$$P(Y \geq 13) = \sum_{y=13}^{\infty} \frac{9^y}{y!} e^{-y} = 1 - \sum_{y=0}^{12} \frac{9^y}{y!} e^{-y} \approx 0{,}12422.$$

Så sandsynligheden for at der sker 13 eller flere ulykker på 3 måneder er cirka 12,4%. Så det er ikke meget usandsynligt, at det sker, og vi behøver ikke undersøge fabrikken lige nu. ○

4 En anvendelse: Først til 100

Vi vil nu kigge nærmere på spillet først til hundrede. Vi skal først have reglerne på plads. På ens tur har man to valg, man kan tage. Det første er at slå med en sekssidet terning. Hvis man gør dette, er der to udfald på baggrund af resultatet. Slår man 2-6, tager man resultatet og lægger til en løbende sum, som er ens tidligere resultater. Et eksempel ville være, at jeg først slår 2, så min totale sum er 2. Derefter slår jeg 6, så nu er min nye sum 8. Hvis man slår 1, bliver ens sum fra den tur til 0, og man giver turen videre. Den anden mulighed man har på ens tur er at gemme ens sum, og så give turen videre. Hvis vi kigger på eksemplet fra tidligere, ville jeg have en sum på 8, som jeg så kunne gemme. Når det bliver min tur igen, kan jeg da lægge de 8 point til det, jeg har slået. Spillet slutter når en spiller har en gemt sum på 100 eller over, og den spiller vinder.

Vi vil gerne se nærmere på dette spil ved at bruge den sandsynlighedsteori, vi har arbejdet med. Vi vil se, om teorien kan give os en fordel til at sige hvornår, vi skal gemme vores sum, og hvad middelværdien af vores sum ville være. Vi starter med at anvende binomialfordelingen.

Vi skal først se på, om spillet kan beskrives ved at bruge binomialfordelingen. Vi definerer en succes som ikke at slå 1, når vi vælger at kaste med terningen. Vi har altså en Bernoulli-fordelt stokastisk variabel med $p = \frac{5}{6}$. Siden hvert terningkast er uafhængigt af de andre, kan vi altså beskrive n terningkast som en binomialfordelt stokastisk variabel med den givne succes $p = \frac{5}{6}$.

$$p_X(x) = \binom{n}{x} \left(\frac{5}{6}\right)^x \left(\frac{1}{6}\right)^{n-x}$$

Vi har dog et problem nu, da vores binomialfordelte variabel ikke fortæller os om, hvad vi forventer, at summen af

de forskellige terningkast bliver, kun sandsynligheden for, at vi ikke slår 1. Vi skal altså have inkorporeret værdien af terningkastene, før vi kan bruge det til spillet. Overvej, hvordan du ville gøre dette.
Vi ved, at når vi får en succes, har vi slået 2,3,4,5 eller 6. For at simplificere vores problem, regner vi gennemsnittet af disse tal, og siden de alle har samme sandsynlighed, er det

$$\mu_{sum} = \frac{1}{5} \cdot \sum_{k=2}^{6} k = 4.$$

Vi vil altså regne med for hver succes at få en værdi på 4 tilføjet til vores sum. Overvej, om dette er en god løsning, hvad er variansen? Hvor mange kast regner vi med at lave, inden vi stopper? For at regne, hvad vi forventer, vores sum bliver, regner vi to ting: Sandsynligheden for, at vi får så mange succeser, samt hvad vores sum ville være. Hvis vi tager $n = 5$, kaster vi vores terning 5 gange, og vi vil selvfølgelig gerne have 5 succeser, så $x = 5$. Vi har nu

$$p_X(x = 5) = \binom{5}{5} \left(\frac{5}{6}\right)^5 \left(\frac{1}{6}\right)^{5-5} \approx 0{,}40.$$

Vores sum ville så være $4 \cdot 5 = 20$. Vi ville altså have en sum på 20 med en 40% chance. Vi ser så, at vi i gennemsnit ved 5 terningkast ville have en sum på 8. I opgaverne vil I blive bedt om at finde udtryk for den forventede værdi af n kast, samt en vurdering af modellen.

Vi vil nu kigge på spillet ved at bruge en Poisson-fordeling. For at kunne anvende en Poisson-fordeling, skal vi først finde vores λ-parameter. Vi ved fra tidligere, at den er givet ved $n \cdot p$, da vi fandt fordelingen ved at kigge på binomialfordelinger. Vi kan altså antage et antal slag og så kigge på den resulterende Poisson-fordeling. Vi antager, at terningen bliver slået 12 gange, da vi ved, at Poisson-fordelingen er bedre

for store n. Er det realistisk?. Vi har da, at

$$\lambda_{100} = 12 \cdot \frac{5}{6} = 10.$$

Vi kan nu finde vores Poisson-fordeling

$$p_Y(y) = \frac{10^y}{y!} e^{-10}.$$

Igen har vi problemet med værdien af summen, da vi hvert slag kan få tal fra 2 til 6. Da vi har udregnet vores $\mu_{sum} = 4$ fra før, anvender vi denne igen. Overvej om gennemsnittet beregnet på denne måde passer til en Poisson fordeling. Som før vil vi gerne finde sandsynligheden for 5 succeser, vi har altså $y = 5$. Det giver os

$$p_Y(y = 5) = \frac{10^5}{5!} e^{-10} \approx 0{,}04.$$

Vi har en sandsynlighed på 4% for at få 5 succeser. Er dette realistisk? Fra før ved vi, at den gennemsnitlige sum efter 5 slag med succes er 20, så vores model fortæller os, at efter 5 slag ville vi i gennemsnit have en sum på 0,8. Giver dette mening? I opgaverne kigger vi nærmere på, hvorfor denne model ikke virker så realistisk, samt hvilke problemer den har.

5 Opgaver

Summer og sandsynligheder

- **Opgave 5.1:**
  Opskriv summen $1+4+9+16+25+36$ med sumtegn.

- **Opgave 5.2:**
  Opskriv summen $1+3+5+7+9+11+13$ med sumtegn. Husk, at alle ulige tal er på formen $2n-1$ hvor $n \in \mathbb{N}$.

- **Opgave 5.3:**
  Opskriv summen $2+4+6+8+10+12+14+16+18+20$ med sumtegn.

●● **Opgave 5.4:**
Udregn følgende:

$$\sum_{n=0}^{\infty} \left(\frac{1}{3}\right)^n, \quad \sum_{n=0}^{\infty} \left(\frac{1}{4}\right)^n, \quad \sum_{n=0}^{\infty} \left(-\frac{1}{7}\right)^n$$

●● **Opgave 5.5:**
Antag, at (tælleligt) uendelig mange matematikere går ind på en bar, dvs. vi kan betegne dem med $1, 2, 3, \ldots$. Den første matematiker bestiller en halv øl. Den næste bestiller en fjerdedel øl, den næste en ottendedel osv. Hvor mange øl skal matematikerne have i alt?

●●● **Opgave 5.6:**
I denne opgave viser vi, at

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

1) Vis, at udtrykket gælder for $n = 1$.

2) Antag, at formlen gælder for et $n > 1$. Vis, at formlen gælder for $n + 1$, dvs.

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

3) Konkludér per induktion, at formlen gælder for alle $n \in \mathbb{N}$.

4) Hvad er summen af de første 100 positive heltal?

●●● **Opgave 5.7:**
Brug strategien med induktion fra forrige opgave til at vise, at summen af de første n kvadrattal er $\frac{n(n+1)(2n+1)}{6}$, i symboler:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

●●●● **Opgave 5.8:**
Bevis, at

$$\sum_{n=1}^{N} \frac{1}{n(n+1)} = 1 - \frac{1}{1+N}$$

og brug dette til at vise, at

$$\sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1.$$

Kombinatorik: At tælle i matematik

● **Opgave 5.9:**
Der bliver kastet 10 mønter og 3 fem-sidet terninger hvor mange mulighede udfald er der i alt? Hvad er sandsynligheden for at slå 10 kroner og 3 femmere?

- **Opgave 5.10:**
  Lad $n \in \mathbb{N}$ være antallet af 13-sidet terninger blive kastet, hvor mange udfald er der?

- **Opgave 5.11:**
  Vis at produktreglen kan udvides sådan at den gælder for $n \in \mathbb{N}$ mange eksperimenter (hint: induktion) eller forklar ideen bag at udvide den formlen videre.

- **Opgave 5.12:**
  En deltager på matcamp skal vælge et projekt fra 3 lister, der er 10 projekter på liste 1, 15 projekter på liste 2 og 17 projekter på liste 3. Ingen af listerne har projekter der overlapper. Hvor mange mulige projekter kan deltageren vælge imellem?

- **Opgave 5.13:**
  Der bliver taget 15 kort ud fra et almindeligt spil kort, hvor mange af de kort vil med sikkerhed være af samme kulør.

- **Opgave 5.14:**
  Der er en urne med 17 røde bolde, 13 blå bolde og 7 grønne bolde. Du trækker fra urnen med lukkede øjne. Hvor mange bolde skal trækkes for at du med sikkerhed ved at du har 2 af hver farve? Hvor mange hvis du ønsker mindst 4 røde bolde?

- **Opgave 5.15:**
  Hvor mange kort skal du trække fra et almindeligt spil kort, før du er sikker på at have mindst 3 kort fordelt på 1 eller 2 kulører.

- **Opgave 5.16:**
  Vis at hvis et matcamp-hold skal deltage i mindst én matematikturnering hver dag hele ugen, men ikke mere end 10, da vil de deltage i præcist 3 på hinanden følgende turneringer.

●●● **Opgave 5.17:**
Vis, at hvis 25 der identificere sig som mænd og 25 der identificere sig som kvinder sætter sig ved et cirkulært bord da vil der altid være mindst en person hvis naboer identificere sig som mænd.

● **Opgave 5.18:**
Lad $A = \{a,b,c,d,e\}$. Hvor mange 2- og 3-permutationer er der for A? Hvor mange 2- og 3-kombinationer er der for A?

● **Opgave 5.19:**
Der er 5 matcamp deltagere og 3 matcamp ansvarlige som kan blive udvalgt til et ekstra projekt, men kun 2 deltagere og 1 ansvarlig skal vælges. Hvor mange mulige sammensætninger kan blive lavet?

●● **Opgave 5.20:**
Bevis korollar 1.24 og 1.30.

●● **Opgave 5.21:**
Betrakt sekvensen $ABCDEFGH$. Hvor mange permutationer indeholder sekvensen CGH?

●● **Opgave 5.22:**
Lad $n,k \in \mathbb{N}$ og lad $1 \leq k \leq n$. Vis, at $k\binom{n}{k} = n\binom{n-1}{k-1}$.

● **Opgave 5.23:**
Find udvidelsen af $(x+y)^3$.

● **Opgave 5.24:**
Find udvidelsen af $(2+x)^4$.

●● **Opgave 5.25:**
Hvad er koefficienten for x^4y^9 i udvidelsen $(x+y)^{13}$.

●● **Opgave 5.26:**

Find koefficienten for x^5y^2 i udvidelsen $(3x + \frac{1}{2}y)^7$

●●● **Opgave 5.27:**
Find binomialudvidelsen af 3^n.

Hvad er sandsynlighed?

● **Opgave 5.28:**
Antag, at vi har en 20-sidet terning, som vi slår med én gang. Antag, at terningen er fair, så øjne har samme sandsynlighed for at blive slået.

1) Hvad er udfaldsrummet S for forsøget?

2) Lad A være begivenheden, at vi slår 1 eller 20. Skriv A ned eksplicit og udregn $P(A)$.

3) Lad B være begivenheden, at vi slår et lige tal. Skriv B ned eksplicit og udregn $P(B)$.

● **Opgave 5.29:**
Lad A være en begivenhed med sandsynlighed 1, altså $P(A) = 1$. Vis, at $P(A^{\complement}) = 0$.

● **Opgave 5.30:**
Antag, at vi kaster tre 10-sidede terninger.

1) Hvad er sandsynligheden for at få tre ens?

2) Hvad er sandsynligheden for at få en sum på mindre end eller lig 5?

3) Hvad er sandsynligheden for at få mindre end eller lig 5 som sum eller tre ens?

●● **Opgave 5.31:**
Antag, at vi har en sekssidet terning. Lad A være begivenheden, at vi slår tre ens. Lad B være begivenheden, at vi slår mindst to ens. Forklar hvorfor, at $P(A) \leq P(B)$.

●● **Opgave 5.32:**
Vi har et almindeligt spil kort, og vi trækker fire kort. Hvad er sandsynligheden for at trække en hånd, hvor der er to af én kulør? Vink: find først sandsynligheden for at trække netop én af hver kulør.

●● **Opgave 5.33:**
Lad A være en begivenhed med sandsynlighed 1, dvs. $P(A) = 1$. Lad B være en vilkårlig begivenhed.

1) Vis, at $P(A \cup B) = 1$.

2) Vis, at $P(B) = P(A \cap B)$.

●● **Opgave 5.34:**
Antag, at vi har 12 blå kugler og 18 røde kugler i en pose. Vi trækker fem kugler op af posen med tilbagelægning (så vi altid har 30 kugler at trække fra i alt). Lad A være begivenheden, at vi trækker flest blå kugler, og B begivenheden, at vi kun trækker røde kugler.

1) Find $P(B)$.

2) Find $P(A)$. Vink: A er netop de udfald, hvor der trækkes nul, én eller to røde kugler.

3) Find sandsynligheden for, at der trækkes flest blå kugler, eller at der kun trækkes røde kugler.

●●● **Opgave 5.35:**
Lad A og B være begivenheder med $A \subseteq B$. Vis, at

$$P(B \setminus A) = P(B) - P(A).$$

●●● **Opgave 5.36:**
En by har fire distrikter. Antag, at der i en given uge er foregået fire røverier. Antag, at hvert distrikt har samme sandsynlighed for at blive røvet.

1) Hvad er sandsynligheden for, at der er foregået et røveri i hvert distrikt? Med andre ord, hvad er sandsynligheden for, at røverierne er ligeligt fordelt?

2) Hvad er sandsynligheden for, at et af de fire distrikter er blevet røvet flere gange? Vink: hvilken begivenhed er dette i forhold til den i forrige delspørgsmål?

●●● **Opgave 5.37:**

Lad A og B være begivenheder. Vi definerer den *symmetriske differens* $A\Delta B$ af A og B til at være $A\Delta B = (A\setminus B)\cup(B\setminus A)$. $A\Delta B$ er altså de elementer, der ligger i A eller B, men ikke i begge to.

1) Tegn et Venn-diagram af $A\Delta B$.

2) Argumentér for, at $A \setminus B = A \setminus (A \cap B)$ og $B \setminus A = B \setminus (A \cap B)$. Du kan f.eks. bruge din tegning fra før.

3) Vis, at

$$P(A\Delta B) = P(A) + P(B) - 2P(A \cap B).$$

●●● **Opgave 5.38:**

I denne opgave skal vi undersøge *nulmængder*. En nulmængde N er en begivenhed med sandsynlighed 0, altså $P(N) = 0$.

1) Hvilken mængde er altid en nulmængde?

2) Lad N være en nulmængde, og lad M være en delmængde af N. Vis, at M også er en nulmængde.

3) Lad $N_1, N_2, \ldots$ være en følge af nulmængder. Vis, at $\bigcap_{n=1}^{\infty} N_n$ er en nulmængde.

4) Lad igen $N_1, N_2, \ldots$ være en følge af nulmængder. Vis, at $\bigcup_{n=1}^{\infty} N_n$ er en nulmængde. Vink: benyt Booles ulighed.

●●● **Opgave 5.39:**

Lad $A_1, A_2, \ldots$ være begivenheder, der alle har sandsynlighed

1. Vis, at

$$P\left(\bigcap_{n=1}^{\infty} A_n\right) = 1.$$

Betinget og uafhængig sandsynlighed

- **Opgave 5.40:**
  Givet $P(A) = 0.7$, $P(B) = 0.25$ og $P(A \cap B) = 0.2$. Find følgende sandsynligheder:
  - $P(A|B)$
  - $P(B|A)$
  - $P(A|A \cap B)$
  - $P(A \cap B|B)$

- **Opgave 5.41:**
  Der bliver delt et kort ud af gangen fra et normalt kortspil (dvs ingen jokere). De første 3 kort er hjerter, hvad er sandsynligheden for det fjerde korte også er en hjerter.

- **Opgave 5.42:**
  I 1.44 er der 3 ligninger hvor hvis 1 holder er der uafhængighed. Vis følgende bi-implikationer
  - 1 $\iff$ 2.
  - 1 $\iff$ 3.
  - 2 $\iff$ 3.

Diskrete stokastiske variable

- **Opgave 5.43:**
  Beskriv eksperimentet, at vi kaster med en sekssidet terning, som en stokastisk variabel. Hvad er støtten og tæthedsfunktionen?

- **Opgave 5.44:**
  Antag, at vi har et almindeligt kortspil, og at vi trækker tre kort med tilbagelægning. Lad X betegne antal es, vi trækker i alt. Find støtten for X og angiv tæthedsfunktionen.

- **Opgave 5.45:**
  Antag, at vi slår plat eller krone fem gange med en fair mønt. Lad X_1 være den stokastiske variabel defineret ved, at $X_1 = 0$, hvis der slås plat på første kast og $X_1 = 1$, hvis der slås krone på første kast. Definér X_2, X_3, X_4 og X_5 tilsvarende.

  1) Hvad er udfaldsrummet S for eksperimentet? Du kan lade P betegne plat og K betegne krone. Hvor mange elementer er i udfaldsrummet?

  2) Lad T være den stokastiske variabel defineret som antal krone, der slås sammenlagt på de fem slag. Opskriv et udtryk for T ud fra de fem variable X_1 til X_5.

  3) Bestem $P(T = 1)$, $P(T = 4)$ og $P(T = 13)$. Er der en sammenhæng mellem $P(T = 1)$ og $P(T = 4)$?

  4) Hvad er støtten for T?

- **Opgave 5.46:**
  I denne opgave introducerer vi såkaldte *indikatorvariable*. Lad S være et udfaldsrum for et eksperiment og $A \subseteq S$ en begivenhed. Vi definerer den stokastiske variabel $1_A : S \to \mathbb{R}$ ved

$$1_A(s) = \begin{cases} 1, & \text{hvis } s \in A \\ 0, & \text{hvis } s \notin A \end{cases}.$$

Altså indikerer 1_A om et element i S ligger i A. Derfor kaldes 1_A for en *indikatorvariabel*. Lad A og B være begivenheder.

1) Vis, at $1_A \cdot 1_B = 1_{A \cap B}$.

2) Vis, at $A \subseteq B$ hvis og kun hvis $1_A \leq 1_B$. Konkludér, at $A = B$ hvis og kun hvis $1_A = 1_B$.

3) Hvad er $P(1_A = 1)$ og $P(1_A = 0)$?

4) Vis, at $1_{A \cup B} = 1_A + 1_B - 1_{A \cap B}$. Vink: tjek, at de to funktioner er ens i alle tilfælde.

•• **Opgave 5.47:**
Lad X være antallet af øjne på et kast med en sekssidet terning. Lad $Y = 6 - X$. Idet Y afhænger af X vil vi forvente, at X og Y er afhængige. Bevis, at dette er tilfældet ud fra definitionen af uafhængighed.

Middelværdi og varians

• **Opgave 5.48:**
Lad X være den stokastiske variabel fra opgave 1.8.39. Bestem middelværdien og variansen for X.

•• **Opgave 5.49:**
Bevis punkt 3 i proposition 2.24.

•• **Opgave 5.50:**
Lad X betegne antal krone, vi får ved at flippe en fair mønt tre gange.

1) Find tætheden p_X for X.

2) Bestem middelværdien for X.

3) Bestem variansen for X.

•• **Opgave 5.51:**
Lad A være en begivenhed. Hvad er $E1_A$? Hvad er det k'te moment $E1_A^k$, hvor $k \in \mathbb{N}$?

●● **Opgave 5.52:**
Bevis korollar 2.27.

●● **Opgave 5.53:**
Lad X være en variabel med $P(X = c) = 1$ for et $c \in \mathbb{R}$, så X er næsten sikkert konstant. Bestem variansen for X.

●●● **Opgave 5.54:**
Antag, at X er en stokastisk variabel med $VX = 0$. Vis, at X er næsten sikkert konstant, dvs. at der eksisterer et $c \in \mathbb{R}$ så $P(X = c) = 1$.

Diskrete fordelinger

●● **Opgave 5.55:**
Bevis sætning 3.3.

● **Opgave 5.56:**
Antag, at vi flipper en fair mønt 30 gange, hvor vi betegner krone med 1 og plat med 0. Lad X angive antal krone, vi får.

1) Hvilken fordeling har X?

2) Hvad er middelværdien og variansen for X?

●● **Opgave 5.57:**
Lad X være binomialfordelt med parametre $n = 5$ og $p = \frac{1}{3}$. Beregn følgende sandsynligheder

- $P(X = 2)$
- $P(X \leq 4)$
- $P(X \geq 3)$

●● **Opgave 5.58:**
Lad Y være Poisson fordelt med parameter $\lambda = 5$. Regn følgende sandsynligheder

- $P(Y = 3)$
- $P(Y \leq 6)$
- $P(Y \geq 5)$

●● **Opgave 5.59:**
Du sidder og spiller først til 100, et spil hvor man ikke må slå 1 og er derfor interesseret i sandsynligheder for a slå 1. Du ved at hvis du slår 6 gange forventer du at have slået 1 en gang. Brug en Poisson proces til at finde sandsynligheden for at observere 3 enere over de seks slag? 2 eller mindre? 0 enere? Hvad med over 12 slag?

●● **Opgave 5.60:**
Du observerer et binomialfordelt eksperiment, hvor de gentager det 40 gange med en sandsynlighed for succes på 0,25. Hvad ville være Poisson fordelingen for dette eksperiment. Find sandsynligheden for 2 observationer for Poisson fordelingen.

●●● **Opgave 5.61:**
Vis at Poisson fordelingen summer til 1. Det vil sige vis at $\sum_0^\infty \frac{\lambda^y}{y!} e^{-\lambda} = 1$.

En anvendelse: Først til 100

● **Opgave 5.62:**
Giv et udtryk for, hvad vores forventede sum ville være for n terningkast for den binomialfordelte stokastiske variabel. Hvilke antagelser laver du?

●● **Opgave 5.63:**
Hvilke antagelser ville vi altid lave, når vi bruger den binomialfordelte stokastiske variabels sandsynlighedsfunktion.

●● **Opgave 5.64:**
Er den binomialfordelte model god? Ville I bruge denne model? Hvorfor/ hvorfor ikke?

●●● **Opgave 5.65:**
Lav en bedre model/ fordeling af spillet ved at bruge en binomialfordelt stokastisk variabel.

● **Opgave 5.66:**
Ville I bruge Poisson-modellen eller binomialmodellen?

● **Opgave 5.67:**
Hvilke antagelser i Poisson-modellen er med til, at den er så dårlig?

●● **Opgave 5.68:**
Hvilke antagelser skal der til for, at man kan bruge en Poisson-model?

●● **Opgave 5.69:**
Vi har i en anden opgave kigget på en model af spillet ved at bruge Poisson-processer.Var denne model god? Hvad ville I ændre i modellen, hvis der skal ændres noget?

●●● **Opgave 5.70:**
Lav en model for først til 100, hvor I bruger en Poisson-fordeling, *ikke* en Poisson proces.

●●● **Opgave 5.71:**
Lav en model for først til 100 ved at bruge en Poisson-proces. I kan tage den, vi har lavet, men forklar da hvilke problemer/ mangler, den har.

●●● **Opgave 5.72:**
Redegør for hvilken af de 3 modeller, I har lavet, som I ville bruge for at kunne vinde fremtidige først til 100 spil.

6 Hints til opgaverne

Opg 5.8:
Du kan bruge, at

$$\frac{1}{n(n+1)} = \frac{n+1}{n(n+1)} - \frac{n}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}.$$

Induktion også en fin fremgangsmåde.
Opg 5.35:
Tegn et Venn-diagram og brug regel nummer 2. Giv også en intuitiv forklaring af resultatet.
Opg 5.37:
Brug forrige opgave.
Opg 5.39:
Brug de Morgans love og Booles ulighed. Det er også en god idé at have lavet de forrige opgaver.
Opg 5.52:
Brug induktion ligesom i korollar 2.19
Opg 5.63:
Overvej hvilke antagelser vi lavede. Lav dine egne antagelser. Brug disse antagelser til at omskrive den givne binomialfordelte stokastiske variabel.
Opg 5.65:
Tænk over hvilke antagelser, vi har lavet, og hvordan de har indflydelse. Specielt tænk over hvor mange terningkast, vi laver på en tur.

7 Projekt: Sjove fordelinger

I dette projekt skal vi udforske nogle sjove fordelinger, der har anvendelser i forskellige sammenhænge. Det er mere end tilladt at bruge lommeregner til udregningerne!

Den geometriske fordeling

Husk, at binomialfordelingen med parametre $n \in \mathbb{N}$ og $0 < p < 1$ beskriver antal successer i en følge af n uafhængige eksperimenter, der alle har sandsynlighed p for at lykkedes. Hvad hvis vi er interesserede i at bestemme antallet af fiaskoer før den første succes? Dette benytter vi den geometriske fordeling til. En variabel X er geometrisk fordelt med parameter $0 < p < 1$, hvis den har tæthedsfunktion

$$p_X(x) = (1-p)^x p$$

for $x = 0, 1, 2, \ldots$ og nul ellers.

- **Opgave 7.1:**
  Forklar, hvorfor tætheden ser ud, som den gør. Hvad er støtten?

- **Opgave 7.2:**
  Vis, at funktionen ovenover faktisk definerer en tæthed. Altså skal I vise, at den er ikke-negativ, og at den summerer til 1. Vink: hvorfor mon den hedder den "geometriske" fordeling?

- **Opgave 7.3:**
  Beregn middelværdien for den geometriske fordeling.

- **Opgave 7.4:**
  Bestem variansen for den geometriske fordeling. I udregningen er I velkomne til at benytte, at

$$\sum_{k=0}^{\infty} k^2(1-p)^k = \frac{(p-2)(p-1)}{p^3}.$$

●● **Opgave 7.5:**
I pakkeleg går en terning på skift mellem en masse mennesker omkring et bord. Slår man andet end 6, sendes den blot videre, men slår man 6, må man tage en pakke.

1) Hvad er sandsynligheden for, at person nummer fem får den første pakke?

2) Hvad er sandsynligheden for, at den første person, der får en pakke, er person nummer 1, 2 eller 3?

Zipf-fordelingen

Zipf-fordelingen bruges til at beskrive tendenser, hvor en lille andel har høj frekvens og en stor andel har en lille frekvens. Tænk på et bibliotek. Få bøger står for størstedelen af udlån (bestsellere). Derudover er der en del klassikere, der jævnligt udlånes, samt en meget stor andel, der udlånes få gange årligt eller slet ikke. En stokastisk variabel X siges at have Zipf-fordelingen med parametre $\alpha \geq 0$ og $n \in \mathbb{N}$, hvis den har tæthed

$$p_X(x) = \frac{1}{x^\alpha H_{n,\alpha}},$$

for $x = 1, 2, \ldots, n$, hvor $H_{n,\alpha}$ er det såkaldte *generaliserede harmoniske tal* defineret som

$$H_{n,\alpha} = \sum_{i=1}^{n} \frac{1}{i^\alpha}.$$

●● **Opgave 7.6:**
Vis, at p_X er en gyldig tæthed.

●● **Opgave 7.7:**
I denne opgave ser vi på Zipf-fordelingen med parametre $n = 4$ og $\alpha = 1$.

1) Beregn $H_{n,\alpha}$.

2) Beregn $p_X(x)$ for alle x.

●● **Opgave 7.8:**
Funktionen $F(x) = P(X \leq x)$ for en stokastisk variabel X kaldes *fordelingsfunktionen* for X. Antag, at X er Zipf-fordelt med parametre $\alpha \geq$ og $n \in \mathbb{N}$. Vis, at

$$P(X \leq x) = \frac{H_{x,\alpha}}{H_{n,\alpha}}.$$

●● **Opgave 7.9:**
Vis, at middelværdien for en Zipf-fordelt variabel X med parametre $\alpha \geq 0$ og $n \in \mathbb{N}$ er

$$EX = \frac{H_{n,\alpha-1}}{H_{n,\alpha}}.$$

●●● **Opgave 7.10:**
Vis, at variansen for en Zipf-fordelt variabel X med parametre $\alpha \geq 0$ og $n \in \mathbb{N}$ er

$$VX = \frac{H_{n,\alpha-2}H_{n,\alpha} - H_{n,\alpha-1}^2}{H_{n,\alpha}^2}.$$

●● **Opgave 7.11:**
En stokastisk variabel X siges at have den diskrete uniforme fordeling på n elementer, hvis den har tæthed

$$p_X(x) = \frac{1}{n}$$

for $x = 1, 2, \ldots, n$ og nul ellers. Vi har set denne fordeling flere gange før, f.eks. i alle opgaver med terningekast. Vis, at

den diskrete uniforme fordeling er et specialtilfælde af Zipf-fordelingen (husk at $a^0 = 1$ for alle reelle tal a).

Zipf-fordelingen beskriver bl.a. forekomsten af ord i sprog. Nogle ord fremkommer meget ofte, mens langt størstedelen forekommer meget sjældent.

Den hypergeometriske fordeling

Betragt en pose med r røde kugler og b blå kugler. Vi udtrækker n kugler af posen *uden* tilbagelægning. Lad X betegne antallet af røde kugler blandt de udtrukne kugler. Da siges X at være *hypergeometrisk fordelt* med parametre r, b og n.

●●● **Opgave 7.12:**
I denne opgave viser vi, at tætheden for en *hypergeometrisk variabel* X med parametre r, b og n er givet ved:

$$p_X(x) = \frac{\binom{r}{x}\binom{b}{n-x}}{\binom{r+b}{n}}$$

for heltal x, der opfylder $0 \leq x \leq r$ og $0 \leq n - x \leq b$. Ellers er tætheden nul.

1) Hvad er det samlede antal måder, man kan udtrække n kugler?

2) Forklar, hvorfor tætheden skal være nul, hvis $0 \leq x \leq r$ eller $0 \leq n - x \leq b$ ikke er opfyldt.

3) Forklar, hvorfor man kan udtrække x hvide kugler på $\binom{r}{x}\binom{b}{n-x}$ måder, såfremt $0 \leq x \leq r$ og $0 \leq n - x \leq b$. Vink: produktreglen.

4) Konkludér, at tætheden ovenfor er korrekt.

Vi har nu selve kombinatorikken på plads. Vi mangler dog at vise, at det er en gyldig tæthed, dvs. at den summerer til

1 og er ikke-negativ. For at kunne vise, at den summerer til 1, skal vi bruge *Vandermondes identitet* for binomialkoefficienter.

●● **Opgave 7.13:**
Bevis Vandermondes identitet,

$$\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j}$$

ved at bruge et kombinatorisk argument. Vink: Venstresiden tæller antallet af måder, man kan udvælge en komité af personer, der er inddelt i to grupper af hhv. n og m individer. Hvad tæller højresiden?

●● **Opgave 7.14:**
Brug Vandermondes identitet til at vise, at tætheden i den første opgave er en gyldig tæthed.

●● **Opgave 7.15:**
En poker-hånd har fem kort. Lad X betegne antallet af es i en tilfældigt trukket pokerhånd.

1) Hvilken fordeling har X?

2) Hvad er sandsynligheden for at trække præcist 2 esser i en pokerhånd?

●● **Opgave 7.16:**
En matematiker skal holde en afslappende ferie og har derfor brug for en masse matematikbøger til godnatlæsning. Hun har plads til fem bøger i kufferten. På sin hylde har hun 12 bøger om algebra og 7 bøger om analyse. Hun udvælger bøgerne helt tilfældigt blandt bøgerne på hylden.

1) Hvad er sandsynligheden for, at to af de fem bøger er analysebøger?

2) Hvad er sandsynligheden for, at alle bøgerne er analysebøger?

●●● **Opgave 7.17:**
Vi beregner middelværdien af en hypergeometrisk fordelt variabel X med parametre r, b og n. Vi kan skrive

$$X = I_1 + \cdots + I_n$$

hvor $I_i = 1$ hvis kugle i i prøven er rød, og $I_i = 0$, hvis den er blå.

1) Gør rede for, at hver variabel I_i er bernoulli-fordelt. Hvad er succesparameteren?

2) Find middelværdien af I_i?

3) Brug linearitet af middelværdi til at finde middelværdien af X.

Bemærk, at $I_1, \ldots, I_n$ ikke er uafhængige, da vi udtager kuglerne uden tilbagelægning. Dog gælder linearitet af middelværdi altid!

8 Projekt: Momentfrembringende funktioner

Hvis vi er givet en stokastisk variable, Y, og ikke kender fordelingen, eller hvis vi er givet en sum af stokastiske variable, hvor det kan være svært at se hvad fordelingen for summen er, hvordan finder vi så deres fordeling?

Definition 8.1. Lad $m(t)$ være den *momentfrembringende funktion* for en stokastisk variable, Y, defineret ved

$$m(t) = E(e^{tY}).$$

Momentfrembringende funktioner eksisterer hvis og kun hvis, at der eksisterer en positiv konstant b sådan at $m(t)$ er endelig for $|t| < b$.

Eksempel 8.2. Hvad er den momentfrembringende funktion for en Poisson- og binomialfordeling?
Vi starter med Poissonfordelingen. Per LOTUS har vi

$$m_{pois}(t) = E(e^{tY}) = \sum_{y=0}^{\infty} e^{ty}\frac{\lambda^y}{y!}e^{-\lambda} = e^{-\lambda}\sum_{y=0}^{\infty}\frac{(\lambda e^t)^y}{y!}.$$

Vi kan igen anvende, at $e^x = \sum_{n=0}^{\infty}\frac{x^n}{n!}$ og får derved

$$e^{-\lambda}\sum_{y=0}^{\infty}\frac{(\lambda e^t)^y}{y!} = e^{-\lambda}\cdot e^{\lambda e^t} = e^{\lambda(e^t-1)}.$$

Dermed har vi $m_{pois}(t) = e^{\lambda(e^t-1)}$. For binomialfordelingen starter vi på samme måde

$$\begin{aligned} m_{binom}(t) = E(e^{tY}) &= \sum_{y=0}^{n}\binom{n}{y}p^y(1-p)^{n-y}e^{ty} \\ &= \sum_{y=0}^{n}\binom{n}{y}(pe^t)^y(1-p)^{n-y}. \end{aligned}$$

Vi kan nu anvende binomial sætningen, sætning 1.33, og får

$$\sum_{y=0}^{n} \binom{n}{y} (pe^t)^y (1-p)^{n-y} = (pe^t + 1 - p)^n.$$

Vi har derfor $m_{binom}(t) = (pe^t + 1 - p)^n$. ∘

Vi kan også finde fordelinger direkte fra momentfrembringende funktioner.

Eksempel 8.3. Vi er givet to momentfrembringende funktioner, $m_1(t) = e^{1,5(e^t-1)}$ og $m_2(t) = (0{,}75e^t + 0{,}25)^4$. Hvad er deres fordelinger?
Vi ser, at den første er en Poissonfordeling med parameter $\lambda = 1{,}5$, og den anden er en binomialfordeling med parameter $p = 0{,}75; n = 4$. De har derfor følgende sandsynlighedstætheder:

$$f_{Y_1}(y) = \frac{1{,}5^y}{y!} e^{1,5}$$
$$f_{Y_2}(y) = \binom{4}{y} 0{,}75^y 0.25^{4-y}$$

∘

Momentfrembringende funktioner er også unikke i forhold til fordelinger.

Sætning 8.4. Lad $m_X(t)$ og $m_Y(t)$ være momentfrembringende funktioner for henholdsvis X og Y. Hvis $m_X(t) = m_Y(t)$, så har X og Y samme fordeling.

Sætning 8.5 (Momentfrembringende funktion for sum af stokastiske variable.)**.** Lad Y_1,Y_2,...,Y_n være uafhængige stokastiske variable med momentfrembringende funktioner henholdsvis $m_1(t)$,$m_2(t)$,...,$m_n(t)$, og lad U være en stokastisk variable med momentfrembringende funktion $m_U(t)$. Hvis $U = Y_1 + Y_2 + \cdots + Y_n$, da er

$$m_U(t) = m_1(t) \cdot m_2(t) \cdot \cdots \cdot m_n(t)$$

Bevis. Per definition af momentfrembringende funktioner har vi, at

$$m_U(t) = E(e^{t(Y_1+Y_2+\cdots+Y_n)}) = E(e^{tY_1}e^{tY_2} \cdot \cdots \cdot e^{tY_n}).$$

Eftersom de er uafhængige, har vi, at

$$\begin{aligned} E(e^{tY_1}e^{tY_2} \cdot \cdots \cdot e^{tY_n}) &= E(e^{tY_1})E(e^{tY_2}) \cdot \cdots \cdot E(e^{tY_n}) \\ &= m_1(t)m_2(t) \cdot \cdots \cdot m_n(t), \end{aligned}$$

hvor vi anvender definitionen af momentfrembringende funktioner. Vi får altså, at

$$m_U(t) = m_1(t)m_2(t) \cdot \cdots \cdot m_n(t),$$

som ønsket. □

Eksempel 8.6. Vi vil gerne finde fordelinger for summer af Poissonfordelte stokastiske variable og binomialfordelte stokastiske variable. Vi starter med Poisson.
Lad Y_1,Y_2,...,Y_n være uafhængige Poissonfordelte stokastiske variable med parameter λ_1,λ_2,...,λ_n. Lad $U = \sum_{i=1}^{n} Y_i$. Vi anvender 8.5 til at finde den momentfrembringende funktion for U. Vi har, at

$$\begin{aligned} m_U(t) &= m_{Y_1}(t)m_{Y_2}(t) \cdot \cdots \cdot m_{Y_n}(t) \\ &= e^{\lambda_1(e^t-1)}e^{\lambda_2(e^t-1)} \cdot \cdots \cdot e^{\lambda_n(e^t-1)} = e^{\sum_{i=0}^{n}\lambda_i(e^t-1)}, \end{aligned}$$

ved at bruge $e^x e^y = e^{x+y}$. Vi ser, at dette blot er en momentfrembringende funktion for en Poissonfordeling med parameter $\sum_{i=0}^{n}\lambda_i = \lambda_U$. Vi kan derfor finde sandsynlighedsfunktionen, som er

$$P(U = u) = \frac{\lambda_U^u}{u!}e^{-\lambda_U}.$$

Vi ser, at summen af Poissonfordelte stokastiske variable igen er Poissonfordelt, som også er, hvad vi regnede med, da vi kendte til Poissonprocesser.

Lad X_1,X_2,...,X_n være uafhængige binomialfordelte stokastiske variable med parametre (p,k_1),(p,k_2),...,(p,k_n) respektivt. Lad $V = X_1+X_2+\cdots+X_n$. Vi anvender definitionen af den momentfrembringende funktion for binomialfordelinger sammen med sætning 8.5. Vi har, at

$$\begin{aligned} m_V(t) &= m_{X_1} m_{X_2} \cdot \cdots \cdot m_{X_n} \\ &= (pe^t + 1 - p)^{k_1} (pe^t + 1 - p)^{k_2} \cdot \cdots \cdot (pe^t + 1 - p)^{k_n} \\ &= (pe^t + 1 - p)^{\sum_{i=1}^n k_i}. \end{aligned}$$

Vi ser, at dette er den momentfrembringende funktion for binomialfordelingen med parametre $p, \sum_{i=1}^n k_i = k_V$. Vi kan derfor finde sandsynlighedsfunktionen for V:

$$P(V = v) = \binom{k_V}{v} p^v (1-p)^{k_V - v}.$$

Vi har dermed også for binomialfordelte stokastiske variable, at deres sum igen bliver binomialfordelt under antagelsen af, at de har samme succesparameter. ∘

Til sidst kan det nævnes, at grunden til navnet "momentfrembringende" funktion er, at man kan bruge dem til at finde momenter for stokastiske variable. Til dem som kender til infinitesimalregning, kan det bevises, at når den momentfrembringende funktion eksisterer vil

$$E(Y^k) = m_Y^{(k)}(0).$$

Vi har altså at det, k'te moment er lig den momentfrembringende funktion differentieret k gange m.h.t t og evalueret i 0.

Opgaver

- **Opgave 8.1:**
  Hvad er sandsynlighedsfunktionen for den stokastiske varia-

bel med følgende momentfrembringende funktion

$$m_1(t) = (0{,}45e^t + 0{,}55)^7$$

- **Opgave 8.2:**
  Hvad er sandsynlighedsfunktionen for den stokastiske variabel med følgende momentfrembringende funktion

$$m_2(t) = e^{6(e^t-1)}$$

- **Opgave 8.3:**
  Hvad er sandsynlighedsfunktionen for den stokastiske variabel med følgende momentfrembringende funktion

$$m_3(t) = 0{,}5(e^t + 1)$$

- **Opgave 8.4:**
  Hvad er sandsynlighedsfunktionen for den stokastiske variabel med følgende momentfrembringende funktion

$$m_4(t) = e^{3e^t}e^{-3}$$

- **Opgave 8.5:**
  Givet følgende sandsynlighedsfunktion, udregn dens momentfrembringende funktion

$$f_X(x) = \frac{8^x}{x!}e^{-8}$$

- **Opgave 8.6:**
Givet følgende sandsynlighedsfunktion, udregn dens moment-frembringende funktion

$$f_Y(y) = \binom{13}{y} 0{,}68^y \cdot 0{,}32^{13-y}$$

- **Opgave 8.7:**
Givet følgende sandsynlighedsfunktioner,

  - $f_W(w) = \frac{4^w}{w!} e^{-4}$.
  - $f_V(v) = \frac{2^v}{v!} e^{-2}$.
  - $f_X(x) = \frac{9^x}{x!} e^{-9}$.

  Udregn den momentfrembringende funktion af deres sum, samt angiv sandsynlighedsfunktionen. Antag, at variablene er uafhængige.

- **Opgave 8.8:**
Givet følgende sandsynlighedsfunktioner

  - $f_W(w) = \binom{46}{w} 0{,}23^w \cdot 0{,}77^{46-w}$.
  - $f_V(v) = \binom{42}{v} 0{,}23^v \cdot 0{,}77^{42-v}$.
  - $f_X(x) = \binom{49}{x} 0{,}23^x \cdot 0{,}77^{49-x}$.

  Udregn den momentfrembringende funktion af deres sum, samt angiv sandsynlighedsfunktionen. Antag, at variablene er uafhængige.

- **Opgave 8.9:**
En anden kendt fordeling er den geometriske fordeling givet ved

$$p_Y(y) = (1-p)^y p.$$

Find dens momentfrembringende funktion og angiv hvilke t, den er defineret for, dvs. udregn

$$m_{geo}(t) = E(e^{tY}).$$

2 Gruppeteori

1 Forord

Man inddeler ofte tallene i forskellige kategorier: Der er de naturlige tal $\mathbb{N}$, det er 1, 2, 3 og så videre. Der er heltallene, $\mathbb{Z}$, det er 0, ± 1, ± 2, ± 3 og så videre. Der er alle de rationale tal, $\mathbb{Q}$, det er brøkerne, f.eks. $\frac{2}{5}$ og $\frac{-6}{21}$. Der er de såkaldte reelle tal, $\mathbb{R}$, som er alle decimaltal - altså både brøker men også tal som e og π.

Fælles for alle kategorierne er, at man altid kan lægge to tal fra samme kategori sammen, og at man altid kan gange to tal fra samme kategori med hinanden, og i begge tilfælde får man et nyt tal fra samme kategori. F.eks. er $3 + 21 = 24$ og $\frac{1}{2} \cdot \left(-\frac{4}{5}\right) = -\frac{2}{5}$.

Inden du læser videre, så prøv at komme med dit eget bud på, hvilke forskelle og ligheder der ellers er mellem kategorierne.

En ting der adskiller $\mathbb{N}$ fra $\mathbb{Z}$ og $\mathbb{Q}$ er, at man nogle gange kan trække to positive heltal fra hinanden og få et resultat der ikke er et positivt heltal. F.eks. er $27 - 84 = -57$. I $\mathbb{Z}$ og $\mathbb{Q}$ kan man altid trække to tal fra hinanden uden at havne i en ny kategori. $\mathbb{N}$ og $\mathbb{Z}$ adskiller sig fra $\mathbb{Q}$ ved, at man ikke kan være sikker på, at kunne dividere to hele tal og få et heltal. F.eks. er $30/18 = \frac{5}{3}$.

Hvis man ønsker at blive indenfor den samme kategori,

så kan man i $\mathbb{N}$ kun gange og lægge tal sammen, hvor man i $\mathbb{Z}$ kan lægge til, trække fra og gange, imens man i $\mathbb{Q}$ kan udføre alle fire regneoperationer (pånær division med 0).

Når det f.eks. går galt med at trække visse tal fra hinanden i $\mathbb{N}$ så er det fordi, man i virkeligheden arbejder med $\mathbb{Z}$ så snart man begynder at trække tal fra hinanden. For egentlig betyder $a - b$ nemlig pr. definition $a + (-b)$, hvor $-b$ så igen betyder tallet der opfylder at $b + (-b) = 0$. Vi siger at $-b$ er *additiv invers* til b. Tilsvarende betyder a/b pr. definition $a \cdot b^{-1}$, hvor b^{-1} er tallet, der opfylder, at $b \cdot b^{-1} = 1$. Vi siger at b^{-1} er *multiplikativ invers* til b. Med denne tankegang er det at trække fra og dividere ikke en særskilt operation, men i virkeligheden et udtryk for hvordan mængden, man arbejder med, spiller sammen med operationerne addition og multiplikation.

Mængderne $\mathbb{Z}$ og $\mathbb{Q}$ adskiller sig fra $\mathbb{N}$ ved at ethvert tal har en additiv invers. Så snart man skriver $a - b$ har man bevæget sig over i disse mængder, fordi man er afhængig af at et element $-b$ findes. Derfor kan man ikke være sikker på, at resultatet ligger i $\mathbb{N}$. På samme vis adskiller $\mathbb{Q}$ og $\mathbb{R}$ sig fra $\mathbb{N}$ og $\mathbb{Z}$ ved at der for ethvert tal forskelligt fra 0, findes en multiplikativ invers, og så snart man skriver a/b har man benyttet sig af at b^{-1} findes. Dermed har man indirekte valgt at arbejde med $\mathbb{Q}$ og $\mathbb{R}$ i stedet.

Arbejder man med addition, har $\mathbb{Z}$ alle de egenskaber vi godt kan lide. Der er en del egenskaber, men vi vil vælge at fokusere på de følgende:

1. For alle tal a, b og c er $a + (b + c) = (a + b) + c$.

2. Der findes et tal e så $a + e = e + a = a$ for alle tal a (nemlig $e = 0$).

3. For alle tal a, findes et tal b så $a + b = b + a = 0$ (nemlig $b = -a$).

Arbejder man med multiplikation i $\mathbb{Q}$ (og ser man bort fra 0), så gælder det tilsvarende at

1. For alle tal a, b og c er $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

2. Der findes et tal e så $a \cdot e = e \cdot a = a$ for alle tal a (nemlig $e = 1$).

3. For alle tal a, findes et tal b så $a \cdot b = b \cdot a = 1$ (nemlig $b = a^{-1}$).

Læg mærke til, at hvis du ser bort fra bemærkningerne i parenteserne, så står der det samme på de to lister, hvis du skifter $+$ ud med $\cdot$. Addition og multiplikation på hhv. $\mathbb{Z}$ og $\mathbb{Q}$ uden 0 virker altså, når man ser bort fra de specifikke symboler, på samme vis.

Det er en af de helt store gennembrud i vejen mod moderne matematik, at matematikere begyndte at erkende at mange af de konkrete objekter og operationer, de arbejdede med, når man blot ser bort fra de specifikke symboler, faktisk opfører sig på tilsvarende måder. Vi skal i dette kapitel se nærmere på en lille bid af det fag matematikere kalder for algebra. Indenfor algebra prøver man at bevise så meget som muligt ud fra nogle på forhånd fastsatte "regneoperationer" og "regneregler" samt nogle krav til de mængder regneoperationerne er defineret på. På den måde kan man nemlig nøjes med at bevise resultater én gang i stedet for at skulle bevise dem for hver konkret mængde og regneoperation.

2 Grupper - hvad er de for noget?

Definition 2.1 (Komposition)**.** Lad G være en mængde af elementer. En *komposition*, $\star$, på mængden G er en operation der tager to elementer, a og b i G, og sammensætter dem til

et nyt element $\star(a,b)$, ofte noteret, $a \star b$, der igen er et element i G.

Definition 2.2 (Grupper)**.** Lad G være en mængde og $\star$ være en komposition på G. $(G,\star)$ er en gruppe hvis G og $\star$ tilsammen opfylder følgende

1. Den *associative* lov:
   For alle a, b og c i G er $a \star (b \star c) = (a \star b) \star c$.

2. G har et *neutralelement* e:
   Der findes et e i G så $a \star e = e \star a = a$ for alle a i G.

3. Alle elementer har et *inverst element*:
   For alle a i G, findes et b i G så $a \star b = b \star a = e$.

Definition 2.3. Vi kalder en gruppe *abelsk* hvis

$$a \star b = b \star a$$

for alle elementer a og b i G.

Definition 2.4 (Orden af et element)**.** For et element x i gruppen $(G,\star)$, siger vi, at g har orden n, hvis n er det mindste naturlige tal således, at $\underbrace{g \star ... \star g}_{n \text{ gange}} = e$ og vi noterer det $|g| = n$. Hvis der ikke findes et sådant n, siger vi, at ordenen er uendelig.

Definition 2.5 (Orden af en gruppe)**.** Vi definerer ordenen af en gruppe, $(G,\star)$, til at være antallet af elementer i G. Dette skrives $|G|$. Hvis der er uendeligt mange elementer i gruppen, så siger vi, at gruppen har uendelig orden.

Bemærkning 2.6. I en additiv gruppe, $(G,+)$, vil vi ofte skrive $\overbrace{x \star ... \star x}^{n \text{ gange}}$ som nx.

På samme måde vil vi, i en multiplikativ gruppe, $(G,\cdot)$, ofte notere det som x^n.

Bemærkning 2.7. Med ovenstående notation, vil vi i en additiv gruppe sige, at $0x = e$, og lignende, i en multiplikativ gruppe, at $x^0 = e$.

Vi ønsker nu at tage et kig på nogle eksempler. Vi starter med den simpleste af alle grupper.

Eksempel 2.8 (Den trivielle gruppe)**.** Gruppen $(\{0\},\star)$ kaldes *den trivielle gruppe*. Det eneste element i gruppen er 0 og kompositionen $\star$ virker således at $0 \star 0 = 0$. ∘

Bemærkning 2.9. Vi ser at den trivielle gruppe er abelsk da $0 \star 0 = 0 \star 0$.

Derudover lægger vi mærke til at 0 har orden 1 i den trivielle gruppe, og at gruppens orden også er 1.

Der sker ikke så forfærdeligt meget i denne gruppe, så vi introducerer nu talgrupperne, som er lidt mere spændende at kigge på.

Talgrupper

Et glimrende eksempel på nogle grupper, som vi allerede har kendskab til, er det vi kalder for talgrupper - altså *grupper* bestående af *tal*. De talgrupper vi vil kigge på er

de additive:	$(\mathbb{Z},+)$, $(\mathbb{Q},+)$ og $(\mathbb{R},+)$,
de multiplikative:	$(\mathbb{Q}\setminus\{0\},\cdot)$ og $(\mathbb{R}\setminus\{0\},\cdot)$.

Lad os kigge lidt nærmere på et par af dem og vise hvorfor disse opfylder betingelserne for at være en gruppe.

Eksempel 2.10. $(\mathbb{Z},+)$ er en gruppe.

For at vise at $(\mathbb{Z},+)$ er en gruppe skal vi vise at $+$ er en kompositionsregel, og at de tre betingelser er opfyldt. Vi ser at $+$ er en kompositionsregel, da vi kan tage to elementer

fra $\mathbb{Z}$ og bruge operationen $+$ på dem ved blot at lægge dem sammen. Vi mangler derfor blot at tjekke at de tre betingelser er opfyldt.

1. Det er velkendt at $(a+b)+c = a+(b+c)$ for $a, b, c \in \mathbb{Z}$, så $+$ er associativ.

2. Vi skal nu finde et neutralelement i $(\mathbb{Z},+)$. Et oplagt gæt er 0, da der ikke sker noget når man adderer med 0. Bemærk at $a + 0 = 0 + a = a$, så 0 er faktisk et neutralelement.

3. Vi mangler nu blot at vise, at ethvert element har et inverst element. Lad $a \in \mathbb{Z}$ være et vilkårligt heltal. Vi skal finde en invers til a, og bemærker at $a + (-a) = (-a) + a = 0$ så $-a \in \mathbb{Z}$ er et inverst element til a.

Da alle tre betingelser er opfyldt er $(\mathbb{Z},+)$ en gruppe. Vi ser også at $a + b = b + a$ så $(\mathbb{Z},+)$ er en abelsk gruppe. ∘

Bemærkning 2.11. Overbevis dig selv om at $(\mathbb{Q},+)$ og $(\mathbb{R},+)$ også er grupper. Her er $\mathbb{Q}$ de rationelle tal og $\mathbb{R}$ de reelle tal.

Eksempel 2.12. $(\mathbb{Q} \setminus \{0\}, \cdot)$, de rationale tal uden 0, er en gruppe.

Vi ser at $\cdot$ er en kompositionsregel for $\mathbb{Q} \setminus \{0\}$, da vi for to rationale tal a og b, får komponeret et nyt rationalt tal $\cdot(a,b)$ i form af produktet $a \cdot b$.

Vi tjekker nu, som i forrige eksempel, at de tre gruppebetingelser er opfyldt.

1. Det passer at $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for $a, b, c \in \mathbb{Q} \setminus \{0\}$, så $\cdot$ er associativ.

2. Vi skal nu finde et neutralelement i $(\mathbb{Q} \setminus \{0\},\cdot)$. Vi gætter på 1, da der ikke sker noget når man ganger med

1. Bemærk at $a \cdot 1 = 1 \cdot a = a$, så 1 er rigtigt nok et neutralelement.

3. Vi mangler nu blot at vise, at ethvert element har et inverst element. Lad $\frac{a}{b} \in \mathbb{Q} \setminus \{0\}$ være en vilkårlig brøk forskellig fra 0. Vi skal finde en invers til $\frac{a}{b}$, og bemærker at $\frac{a}{b} \cdot \left(\frac{1}{\frac{a}{b}}\right) = \left(\frac{1}{\frac{a}{b}}\right) \cdot \frac{a}{b} = 1$ så $\frac{1}{\frac{a}{b}} = \frac{b}{a} \in \mathbb{Q} \setminus \{0\}$ er et inverst element til $\frac{a}{b}$.

Alle betingelserne er opfyldt, så ergo er $(\mathbb{Q}\setminus\{0\}, \cdot)$ en gruppe. Bemærk desuden at gruppen er abelsk. ∘

Bemærkning 2.13. Tjek selv efter og overbevis dig selv om at $(\mathbb{R} \setminus \{0\}, \cdot)$ også er en gruppe.

Bemærkning 2.14 (Entydighedsbeviser)**.** I matematik ønsker man ofte at bevise, at der i en given mængde kun findes ét element med en vis egenskab. Dette gør man ved at antage, at der findes to elementer med egenskaben og derefter vise, at de i så fald er lig hinanden.

Sætning 2.15 (Entydighed af neutralelement)**.** Lad $(G,\star)$ være en gruppe. Der findes kun ét neutralelement i G.

Bevis. Antag, at e_1 og e_2 er neutralelementer i G. Da e_1 er neutralelement, gælder at $e_2 \star e_1 = e_2$, og da e_2 også er neutralelement, så er $e_2 \star e_1 = e_1$. Dette betyder at

$$e_1 = e_2 \star e_1 = e_2,$$

så der findes kun ét neutralelement i G. □

Da der kun findes ét neutralelement i en gruppe, taler vi derfor om neutralelement*et* i gruppen.

Sætning 2.16 (Entydighed af inverselement)**.** Lad $(G, \star)$ være en gruppe. For hvert g i G findes kun én invers til g.

Bevis. Antag, at g_1 og g_2 begge er inverse til g. Da g_1 er invers til g gælder at $g \star g_1 = e$, og da g_2 ligeledes er invers til g gælder at $g_2 \star g = e$. Samlet får vi

$$g_1 = e \star g_1 = g_2 \star g \star g_1 = g_2 \star e = g_2.$$

Altså findes der kun én invers til hvert gruppeelement. □

Da der kun findes én invers til hvert element g i G, taler vi om *den inverse* til g og skriver g^{-1}.

Bemærkning 2.17. Lad $(G,\star)$ være en gruppe. Vi vil ofte udelade at skrive kompositionsreglen, når vi arbejde i en gruppe. Vi benytter da den multiplikative skrivemåde som kendt fra bogstavsregning, dvs. vi skriver gh i stedet for $g\star h$.

Bemærkning 2.18. Lad G være en gruppe og lad a og b tilhøre G. Der gælder, at $(ab)^{-1} = b^{-1}a^{-1}$.

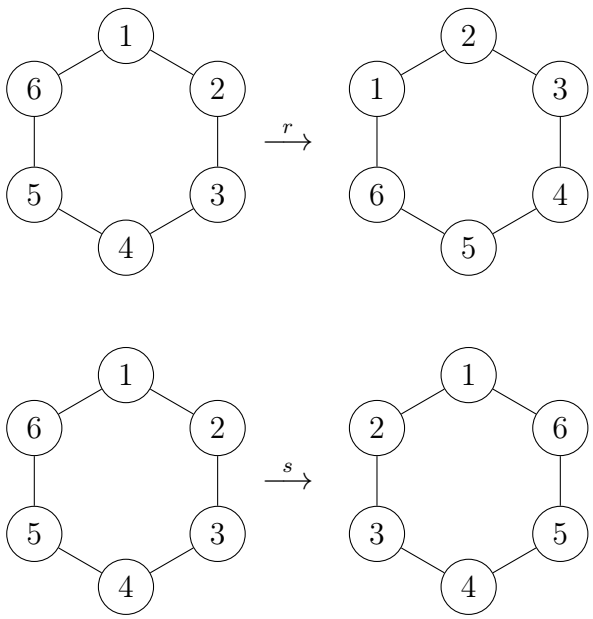
3 Diedergrupper

Frem til nu har vi betragtet grupper bestående af tal. Vi vil nu kigge på vore første gruppe som har elementer der ikke er tal. Det er Diedergruppen, ofte betegnet D_{2n}, som består af symmetrier af regulære polygoner.[1] En symmetri er en afbildning fra polygonen ind i polygonen, som bevarer afstanden mellem punkterne. Intuitivt vil det sige, at hvis man tegner en n-kant, navngiver hjørnerne $1,\ldots,n$, og lægger en kopi af n-kanten ovenpå, så den dækker hele den originale polygon, svarer dette til en symmetri. Denne gruppe kaldes Diedergruppen og betegnes D_{2n}.

Der er grundlæggende to elementer i gruppen: Rotation og

[1] En regulær polygon er en polygon, hvor alle sider er lige lange, og hvor alle vinkler er lige store. For eksempel er et kvadrat en regulær polygon.

spejling af polygonen. Elementet i gruppen, der svarer til at rotere en gang i urets retning, betegnes r. Elementet, der svarer til at spejle over symmetriaksen, som skærer den første kant og centrum i figuren, betegnes s. I følgende figurer ses det, hvordan symmetrierne r og s ser ud i D_{12}. Dis-



se to grundlæggende symmetrier, r og s, kan sammensættes til at lave nye symmetrier af n-kanten. For eksempel er sr den symmetri, der først roterer polygonen i urets retning og derefter spejler den. Det er sådan, at man skal forstå kompositionsreglen i gruppen. Den er nemlig sammensætningen af symmetrier. Neutralelementet er da den symmetri, hvor man ikke gør noget ved n-kanten. Det viser sig faktisk, at alle symmetrier i en Diedergruppe for en n-kant kan skrives som et produkt af r og s, hvilket betyder, at gruppen er frembragt af disse to elementer. Det vil vi komme nærmere ind på senere i dette afsnit.

Der er indtil videre ikke givet noget argument eller bevis for, at D_{2n} faktisk er en gruppe. Det vil blive givet nu. For

det første er symmetrier faktisk afbildninger. Det er bijektive afbildninger mellem geometriske figurer, der bevarer formen af figurerne. Sammensætning af afbildninger er en associativ komposition, og derfor er sammensætning af symmetrier en associativ kompositionsregel. Bemærk, at identitetsafbildningen er neutralelementet. Derudover, da symmetrier er bijektive, har de specielt også inverser. Derfor er D_{2n} en gruppe. Det er ikke vigtigt, at man på dette tidspunkt forstår dette argument, men det er en god idé at danne en intuition om, hvorfor det er en gruppe.

Sætning 3.1. Regneregler i D_{2n}:

(i) $|s| = 2$ og $|r| = n$

(ii) $s \neq r^k$ for alle $k \in \mathbb{Z}$

(iii) $rs = sr^{-1}$

(iv) $r^k s = sr^{-k}$ for alle $k \in \{1, \ldots, n\}$

Bevis. Bemærk først, at $s \neq e$, og at $s^2 = e$. Det gælder, da hvis man spejler to gange over samme akse sker ingenting. Derfor er $|s| = 2$. Hvis man roterer en n-kant n gange sker ingenting, og derfor er $r^n = e$. Hvis man roterer n-kanten k gange, hvor $0 < k < n$, så vil kant 1 blive afbildet til kant k. Det medfører, at $r^k \neq e$, og derfor er $|r| = n$. Dette viser (i).

Lad $k \in \mathbb{Z}$. I symmetrien s bliver kant 1 afbildet til kant 1. Dette er kun tilfældet for r^k, hvis $r^k = e$. Da $s \neq e$, er $s \neq r^k$. Dette viser (ii).

Lad $k \in \{1, \ldots, n\}$. Bemærk, at s afbilder kant k til kant $n-k+2$, at r afbilder kant k til kant $k+1$, og at r^{-1} afbilder kant k til kant $k-1$. Her er kant 0 og n den samme kant, og kant $n+1$ og 1 er den samme kant. Det ses nu, at rs afbilder kant k til kant $n-(k+1)+2 = n-k+1$, og sr^{-1} afbilder

kant k til kant $(n-k+2)-1 = n-k+1$. Derfor gælder der, at $rs = sr^{-1}$, hvilket viser (iii).

Lad $k \in \{1,\ldots,n\}$. Ved brug af (iii) fås, at $r^k s = r^{k-1}rs = r^{k-1}sr^{-1}$. Denne regneoperation bruges så i alt k gange, og det giver, at $r^k s = sr^{-k}$. □

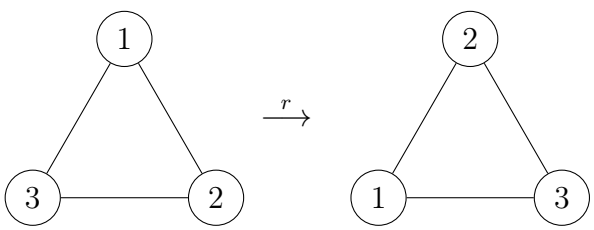
Bemærkning 3.2. Bemærk, at D_{2n} ikke er abelsk. Fra sætning 3.1.(iii) har vi at $rs = sr^{-1}$. Eftersom en polygon har mindst tre kanter, er $r \neq r^{-1}$. Derfor er $rs = sr^{-1} \neq sr$, og dermed er gruppen ikke abelsk.

Sætning 3.3. Ordenen af gruppen D_{2n} er $2n$. Med andre ord er

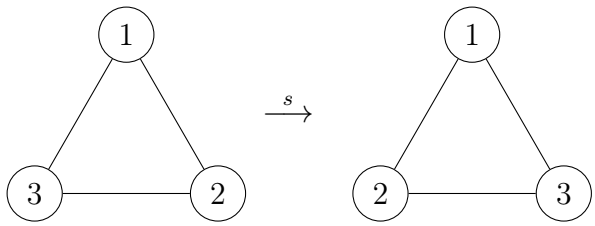
$$|D_{2n}| = 2n.$$

Bevis. Bemærk først, at der findes en symmetri, der afbilder kant 1 til kant k, hvor $k \in \{1,\ldots,n\}$. Her vil kant 2 blive afbildet til enten kant $k-1$ eller $k+1$. Dette bestemmer entydigt, hvad resten af kanterne bliver afbildet til, da formen i en symmetri bevares. Derfor er der 2 symmetrier, hvor 1 bliver afbildet til k. Da der er n kanter, findes der $2 \cdot n$ symmetrier i alt. □

Eksempel 3.4. Den mindste af Diedergrupperne er altså D_6, så lad os betragte den lidt.



Det giver mening at der må være $2{\cdot}3$ elementer i gruppen, da vi kan tegne 6 forskellige trekanter. Vi har tre muligheder



når vi vælger hvilken værdi den første af cirklerne har, og så to valgmuligheder tilbage til den næste, og så er den tredje bestemt af de andre to. Vi får altså 6 forskellige trekanter, og dermed også seks forskellige elementer i vores gruppe. ∘

Korollar 3.5. Fra beviset i Sætning 3.3 ses, at samtlige elementer i D_{2n} er følgende

de n rotationer:	$r^0 = e, r^1, r^2, \ldots, r^{n-1}$,
og hver af disse spejlet:	$s, sr, sr^2, \ldots, sr^{n-1}$.

Altså får vi

$$D_{2n} = \{s^0r^0, s^0r^1, s^0r^2, \ldots, s^0r^{n-1}, s^1r^0, s^1r^1, \ldots, s^1r^{n-1}\}.$$

Dermed kan alle elementer i Diedergruppen skrives på formen s^ir^j, hvor i er 0 eller 1 og j er et tal mellem 0 og $n-1$.

Dette giver anledning til at definere frembringere, som er et meget nyttigt maskineri inden for gruppeteorien.

4 Restklassegrupper

En familie af grupper der er nært beslægtede med talgrupperne, er de såkaldte restklassegrupper. Ligesom med talgrupperne findes der både additive og multiplikative restklassegrupper.

Definition 4.1 (Division med rest)**.** Lad b være et naturligt tal og lad a være et heltal. Division med rest af a med b er en opskrivning af a på følgende form

$$a = qb + r,$$

hvor q og r er heltal og $0 \leq r < b$. Tallet r kaldes for *resten*.

Bemærk at r skal være strengt mindre end b, og man skal altså gøre q så numerisk stor som muligt. Lad for eksempel $a = 13$ og $b = 4$, da er

$$13 = 2 \cdot 4 + 5,$$

men vi har ikke lavet division med rest, da $5 \geq 4$. Til gengæld er

$$13 = 3 \cdot 4 + 1$$

division med rest, idet $0 \leq 1 < 4$, og vi får her at resten er $r = 1$.

Division med rest svarer altså til en situation, hvor du skal dele en pose slik med en gruppe venner, hvor alle ønsker at få så meget slik som muligt, men hvor der samtidig er enighed i gruppen om, at alle skal have lige meget. Resten er så den mængde slik, der er tilbage, når der ikke længere er nok til, at alle kan få endnu et stykke.

Proposition 4.2. Givet a og b er resten, r, ved division med rest af a med b entydig.

Bevis. Antag $a = q_1 b + r_1$ og $a = q_2 b + r_2$, for $0 \leq r_1 < b$ og $0 \leq r_2 < b$ og lad os antage at $r_1 \geq r_2$. Da vil $q_1 b + r_1 = q_2 b + r_2$ så $r_1 - r_2 = q_2 b - q_1 b = b(q_2 - q_1)$. Dermed går b op i $r_1 - r_2$ som er et positivt tal der er mindre end b. Dermed må $r_1 - r_2 = 0$. □

Definition 4.3. Lad a være et heltal og n være et naturligt tal, hvor a har rest r ved division med n, altså $a = qn + r$. Alle de heltal der har r som rest ved division med n kalder vi *restklassen* for a og vi noterer denne mængde $[a]_n$.

Restklasser kan godt virke meget abstrakt første gang man stifter bekendskab med det, men det er en super vigtig og grundlæggende ting at forstå inden for store dele af algebra og talteori.

Hvis vi for eksempel kigger på $a = 13$ og $n = 4$ og ønsker at bestemme restklassen for a, noterer vi os først at 13 har rest 1 ved division med 4 eftersom $13 = 3 \cdot 4 + 1$.

Restklassen $[13]_4$ er derfor alle de tal, der også har rest 1 ved division med 4.

Overbevis dig selv om at dette netop bliver følgende mængde,

$$[13]_4 = \{..., -7, -3, 1, 5, 9, 13, 17, ...\}.$$

Bemærkning 4.4. Restklassen $[a]_n$ består af alle heltal på formen $qn + a$ hvor q er et heltal.

Definition 4.5. Vi siger at to heltal a og b er kongruente modulo n hvis de har samme rest ved division med n. Altså hvis $[a]_n = [b]_n$. Vi skriver også $a \equiv b \pmod{n}$.

Korollar 4.6. $[a]_n = [b]_n \Leftrightarrow n$ går op i $b - a$.

Bevis. Se Opgave 11.28. □

Hvis vi skal se på hvor mange restklasser vi har for et givent n, altså hvor mange forskellige rester vi får når vi dividerer forskellige tal med n, kan vi hurtigt overbevise os selv om at der må være præcis n af disse. Dette er fordi vi kan have resterne fra 0 til $n - 1$.

Lad os igen kigge på eksemplet hvor $n = 4$. Tallet 1 har rest 1, 2 har rest 2, 3 har rest 3, 4 har rest 0, 5 har rest 1, 6

har rest 2 og så videre. Vi får altså de fire restklasser

$$[0]_4 = \{..., -8, -4, 0, 4, 8, 12, ...\} = 4\mathbb{Z},$$
$$[1]_4 = \{..., -7, -3, 1, 5, 9, 13, ...\} = 4\mathbb{Z} + 1,$$
$$[2]_4 = \{..., -6, -2, 2, 6, 10, 14, ...\} = 4\mathbb{Z} + 2,$$
$$[3]_4 = \{..., -5, -1, 3, 7, 11, 15, ...\} = 4\mathbb{Z} + 3.$$

Vi ønsker nu at definere en passende (additiv) kompositionsregel, som vi kan bruge på mængden af restklasser. Vi gør det ret naivt, men det viser sig at give mening.

Hvis vi gerne vil lægge restklasser sammen kunne vi umiddelbart gøre følgende

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

Hvorfor giver dette så god mening? Jo, prøv at overbevise dig selv om at hvis a har rest r_1 ved division med n og hvis b har rest r_2 ved division med n, så har $a+b$ rest r_1+r_2 ved division med n. Du kan eventuelt kigge på eksemplet hvor n er 4 og kig på de fire restklasser ovenfor. Opgave 11.25 giver os at denne kompositionsregel faktisk er veldefineret. Betragter vi mængden af disse fire restklasser med den overstående komposition får vi netop en gruppe.

Definition 4.7. Grupper af formen $(\{[0]_n,...,[n-1]_n\},+)$ for et n i $\mathbb{N}$ kaldes restklassegrupper, og vi skriver den n'te restklassegruppe $\mathbb{Z}/n\mathbb{Z}$, som udtales Z modulo n Z. Vi kan også definere dem for $-m$ i $\mathbb{Z} \setminus \mathbb{N}_0$. Vi lader $[m]_{-m} = [m]_m$ så vi får at den $-m$'te restklassegruppe blot er den m'te, altså $\mathbb{Z}/-m\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$.

Eksempel 4.8. Den -7'ende restklassegruppe er gruppen $(\{[0]_7,...,[6]_7\},+)$ idet dette er den 7'ende restklassegruppe. Et eksempel på addition her vil være $[-8]_7+[9]_7 = [-8+9]_7 = [1]_7$. ∘

Vi har nu fundet en additiv gruppestruktur på restklasserne, men i særlige tilfælde kan vi også lave en multiplikativ gruppe. Vi starter med at give definitionen og viser bagefter at det faktisk er en gruppe.

Definition 4.9. Mængden af restklasser modulo p hvor p er et primtal, $\{[1]_p, \ldots, [p-1]_p\}$ sammen med multiplikation som komposition er en gruppe. Her skal multiplikation forstås som

$$[a]_p \cdot [b]_p = [a \cdot b]_p.$$

Faktisk går det kun godt med at lave en multiplikativ gruppe, så længe p er et primtal.

Proposition 4.10. $(\{[1]_p, \ldots, [p-1]_p\}, \cdot)$ er en gruppe hvis og kun hvis p er et primtal.

Bevis. Lad os starte med at antage at $p > 1$ ikke er et primtal. Da kan vi skrive $p = m \cdot n$ for to naturlige tal $n > 1$ og $m > 1$. Lad os nu prøve at finde en invers til restklassen $[n]_{m \cdot n}$. Vi skal da finde a der løser ligningen

$$[a]_{m \cdot n} \cdot [n]_{m \cdot n} = [1]_{m \cdot n}.$$

Det er ikke muligt da $[a]_{m \cdot n} \cdot [n]_{m \cdot n} = [a \cdot n]_{m \cdot n} \neq [1]_{m \cdot n}$ for alle a, idet vi ellers ville have $a \cdot n = k \cdot n \cdot m + 1$ og her går n op i venstresiden men ikke i højresiden. Dermed har vi ikke en gruppe når p er et sammensat tal.

Det vi nu mangler for at bevise propositionen, er at vise at vi rent faktisk *har* en gruppe, så længe p er et primtal. Dette kræver lidt yderligere teori, som gennemgås sammen med resten af beviset, i projekt 3, afsnit 15. □

Bemærkning 4.11. Når vi vil notere gruppen

$$(\{[1]_p, \ldots, [p-1]_p\}, \cdot)$$

skriver vi $((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$, hvor $\times$ blot symboliserer at vi ikke tager 0 med.

Eksempel 4.12. Lad os betragte $(\{[1]_2\},\cdot)$. Denne gruppe har kun 1 element, og $[1]_2 \cdot [1]_2 = [1]_2$. Vi har dermed fundet en ny måde at skrive den trivielle gruppe på, hvor vi bare kalder vores element '$[1]_2$' i stedet for 0. ∘

Eksempel 4.13. Lad os betragte $(\{[1]_5,[2]_5,[3]_5,[4]_5\},\cdot)$, som vi også skriver $((\mathbb{Z}/5\mathbb{Z})^\times,\cdot)$. Dette er en gruppe, hvor neutralelementet er $[1]_5$. Vi har at den inverse til $[2]_5$ er $[3]_5$ idet

$$[2]_5 \cdot [3]_5 = [2 \cdot 3]_5 = [1]_5.$$

Elementerne $[1]_5$ og $[4]_5$ har blot sig selv som inverser. ∘

Eksempel 4.14. Lad os kigge på $(\{[1]_4,[2]_4,[3]_4\},\cdot)$. Vi ved at hvis det skal være en gruppe skal vi kunne komponere alle elementer i vores mængde, og blive inden for vores mængde, men vi ser at

$$[2]_4 \cdot [2]_4 = [0]_4,$$

som ikke ligger i vores mængde, og derfor er det ikke en gruppe.

Man kunne måske have lyst til at inkludere $[0]_4$ i vores mængde, men denne restklasse har ikke en invers restklasse, da der ikke findes en restklasse $[a]_4$ så $[a]_4 \cdot [0]_4 = [1]_4$. Vi kan altså ikke løse problemet ved blot at tilføje $[0]_4$. ∘

5 Frembringere

Definition 5.1. Lad G være en gruppe. Delmængden S af G siges at *frembringe* G, hvis alle elementer i G kan skrives som en sammensætning af elementer fra S. Vi skriver $\langle S\rangle = G$ og kalder elementer fra S for *frembringere*.

Eksempel 5.2. Gruppen $G = \mathbb{Z}/7\mathbb{Z}$ er frembragt af mængden $S = \{[1]_7\}$ da vi kan sammensætte $[1]_7$ med sig selv

passende mange gange for at få samtlige elementer i G. For eksempel er $[4]_7 = [1]_7 + [1]_7 + [1]_7 + [1]_7$. ∘

Når S skrives på elementform, udelades mængdeklammerne ofte. For eksempel er $\mathbb{Z}$ frembragt af $\{1\}$, og der skrives $\mathbb{Z} = \langle 1 \rangle$ i stedet for $\mathbb{Z} = \langle \{1\} \rangle$. Bemærk, at $D_{2n} = \langle s,r \rangle$. Bemærkningen følger direkte af Korollar 3.5 og Definition 5.1.

Definition 5.3. Lad G være en gruppe frembragt af S, og lad $R_1, \ldots, R_k$ være regneregler defineret for frembringerne, så enhver udregning imellem frembringerne i S kan udføres. Så skrives:

$$G = \langle S \mid R_1, \ldots, R_k \rangle.$$

Eksempel 5.4. $D_{2n} = \langle s,r \mid rs = sr^{-1}, |s| = 2, |r| = n \rangle$. ∘

Ud fra denne opskrivning kan man udlede, hvordan hele strukturen på gruppen er. Bemærk, at det er tilstrækkeligt at give regneregler, der bestemmer ordnerne af frembringerne og beskriver, hvordan man kan kommutere frembringerne. Denne meget kompakte måde at opskrive gruppestrukturer på er en af grundene til, at frembringermaskineriet er et kraftigt værktøj i gruppeteorien.

6 Cykliske grupper

Vi viste helt i starten, at man på en meningsfuld måde kan definere potenser i en vilkårlig gruppe. En cyklisk gruppe er en gruppe, hvor alle elementer opstår som en potens af et særligt element.

Definition 6.1 (Cyklisk gruppe)**.** En gruppe G er cyklisk, hvis der findes et element a, der frembringer hele gruppen,

$\langle a \rangle = G$. Dvs, at der for alle andre elementer g i gruppen findes et heltal n, så $g = \underbrace{a \star ... \star a}_{n \text{ gange}}$.

Bemærkning 6.2. I definitionen af en cyklisk gruppe ovenfor benyttes den multiplikative skrivemåde for grupper. Hvis man i stedet benytter den additive skrivemåde skal a^n erstattes med na.

Sætning 6.3 (Eksistens af cykliske grupper)**.** For hvert naturligt tal n findes en cyklisk gruppe af orden n.

Bevis. Lad n være et naturligt tal. Den trivielle gruppe er en cyklisk gruppe med et element, så antag $n > 1$. Vælg et symbol a, og lad mængden $G = \{1,a,\ldots,a^{n-1}\}$, og lad $a^n = 1$. Da er G en gruppe under multiplikation defineret med de almindelige potensregler. □

Bemærkning 6.4. Her er der egentlig noget at vise, da det ikke a priori er givet at potensreglerne som vi kender dem virker i grupper. Det viser sig dog at være tilfældet.

Vi skriver Z_n for den cykliske gruppe af orden n som vi konstruerede i beviset ovenfor.

Vi havde faktisk ikke behøvet at konstruere en ny gruppe for a finde cykliske grupper, nogle af de grupper, vi allerede har set på er cykliske:

Eksempel 6.5. Grupperne $(\mathbb{Z}/n\mathbb{Z},+)$ og $((\mathbb{Z}/p\mathbb{Z})^\times,\cdot)$ er cykliske. ○

Cykliske grupper behøver ikke at være endelige:

Eksempel 6.6. Gruppen $(\mathbb{Z},+)$ er cyklisk. ○

Definition 6.7. Lad G være en gruppe, og lad g være et element i G. Vi skriver $\langle g \rangle$ for mængden bestående af alle

potenser af g, altså

$$\langle g \rangle = \{g^n | n \text{ er et heltal}\}.$$

Definition 6.8. Lad $(G,\star)$ være en gruppe, og lad g være et element i G. Da er $(\langle g \rangle,\star)$ en gruppe, som vi kommer til at se i opgave 11.53. Vi kalder den for gruppen frembragt af g.

Sætning 6.9. Lad G være en gruppe, og lad g være et element i G. Antag ordenen af g er n. Da er ordenen af gruppen frembragt af g lig n:

$$|\langle g \rangle| = |g|.$$

Korollar 6.10. Lad G være en endelig cyklisk gruppe med frembringer g, da gælder af $|g| = |G|$.

De to forskellige ordensbegreber er altså forbundne.

7 Isomorfier

Vi har nu set eksempler på forskellige grupper, og vi har set at grupper kan have forskellige egenskaber. I dette afsnit skal vi se, hvordan man kan sammenligne grupper. I det følgende arbejder vi med to grupper $(G,\star)$ og $(H,\diamond)$.

Definition 7.1 (Isomorfi)**.** En afbildning $\varphi : G \to H$ kaldes en *isomorfi*, hvis den opfylder disse to krav

(i) φ skal være en bijektiv afbildning,

(ii) for alle g_1 og g_2 i G, skal

$$\varphi(g_1 \star g_2) = \varphi(g_1) \diamond \varphi(g_2).$$

Bemærkning 7.2. Hvis vi har en isomorfi, φ, fra G til H, har vi automatisk også en isomorfi fra H til G i form af den inverse afbildning af φ.

En isomorfi er altså en afbildning der *respekterer gruppestrukturen*, i den forstand, at det er ligegyldigt, om man sammensætter i G før man benytter afbildningen eller om man benytter afbildningen på g_1 og g_2 hver for sig og derefter sammensætter i H. Betingelsen at φ skal være bijektiv, fortæller os at hvis G og H er endelige, så har de lige mange elementer[2].

Definition 7.3 (Isomorfe grupper)**.** Vi siger at to grupper, G og H, er *isomorfe med hinanden* hvis vi kan finde en isomorfi imellem dem. Vi notere det som $G \cong H$.

Definition 7.4 (Homomorfi)**.** En afbildning $\varphi : G \to H$ der blot overholder det ene kriterium at $\varphi(g_1 \star g_2) = \varphi(g_1) \diamond \varphi(g_2)$, kalder vi en *homomorfi*. Hvis vores homomorfi også er bijektiv, er den altså en isomorfi.

Eksempel 7.5. Lad $G = \mathbb{Z}/16\mathbb{Z}$ og lad $H = \mathbb{Z}/4\mathbb{Z}$. Afbildningen $\varphi : G \to H$ defineret ved

$$\varphi([a]_{16}) = [a]_4$$

er en homomorfi men er ikke bijektiv og er derfor ikke en isomorfi. ∘

Eksempel 7.6. Vi kan også lave en homomorfi den anden vej, altså fra $G = \mathbb{Z}/4\mathbb{Z}$ til $H = \mathbb{Z}/16\mathbb{Z}$, defineret ved

$$\varphi([a]_4) = [4a]_{16}.$$

[2]Dette gælder faktisk også selvom grupperne er uendelige, men så skal vi introducere et nyt begreb, nemlig *kardinalitet*. Det kommer vi ikke til at gøre i dette forløb, men man kan for eksempel komme frem til at $\mathbb{Z}$ og $\mathbb{Q}$ har lige mange elementer.

Da denne heller ikke er bijektiv, er den derfor ikke en isomorfi. ∘

Eksempel 7.7. Eksponentialfunktionen $f(x) = e^x$ er en homomorfi fra gruppen $(\mathbb{R}, +)$ til gruppen $(\mathbb{R}_+, \cdot)$. Dette kommer af eksponentialregnereglen

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y).$$

∘

Lad os nu se på et eksempel af en afbildning der opfylder *begge* kriterier, og dermed er en isomorfi.

Eksempel 7.8. Lad $G = (\mathbb{Z}/3\mathbb{Z}, +)$ og $H = (Z_3, \cdot)$. I Z_3, den cykliske gruppe af orden 3, ser vi elementerne 1, a, a^2 og vi definerer afbildningen $\varphi : G \to H$ således

$$\varphi([n]_3) = a^n.$$

φ er en isomorfi da den opfylder begge kriterier i definitionen:

φ er bijektiv da vi kan finde en invers afbildning, altså den der sender a^n til restklassen for n modulo 3. Derudover er andet kriterium opfyldt da

$$\varphi([n_1]_3 + [n_2]_3) = a^{n_1+n_2} = a^{n_1} \cdot a^{n_2} = \varphi([n_1]_3) \cdot \varphi([n_2]_3)$$

og dermed er φ en isomorfi og grupperne er *isomorfe*. ∘

Bemærkning 7.9. Bemærk at enhver gruppe G er isomorf til sig selv, da identitetsafbildningen på G er en isomorfi.

Vi vil nu opskrive en række regneregler for isomorfier og homomorfier, som vi kan bruge fremover.

Sætning 7.10 (Regneregler for isomorfe grupper)**.** Lad $\varphi : G \to H$ være en isomorfi og lad $\psi : G \to H$ være en homomorfi. Da gælder følgende:

(i) Enheder bevares:

(a) $\psi(e_G) = e_H$ (b) $\varphi(e_G) = e_H$

(ii) Inverser bevares

(a) $\psi\left(g^{-1}\right) = (\psi(g))^{-1}$ (b) $\varphi\left(g^{-1}\right) = (\varphi(g))^{-1}$

(iii) Potenser bevares

(a) $\psi\left(g^n\right) = (\psi(g))^n$ (b) $\varphi\left(g^n\right) = (\varphi(g))^n$

(iv) Ordner

(a) $|\psi(g)| \leq |g|$ (b) $|\varphi(g)| = |g|$

(v) Abelskhed bevares

(a) G er abelsk $\Rightarrow$ $\psi(G)$ er abelsk

(b) G abelsk $\Leftrightarrow$ $\varphi(G) = H$ er abelsk

(vi) Cykliskhed bevares

(a) G er cyklisk $\Rightarrow$ $\psi(G)$ er cyklisk

(b) G er cyklisk $\Leftrightarrow$ $\varphi(G) = H$ er cyklisk

Bevis. For at se at homomorfier bevarer enheder, skal vi benytte at $g = e_G \star g$ og bruge ψ på ligheden

$$\psi(g) = \psi(e_G \star g) = \psi(e_G) \diamond \psi(g).$$

På samme måde kan vi komme frem til at $\psi(g) = \psi(g) \diamond \psi(e_G)$ og dermed er $\psi(e_G)$ neutralelement i H.

Dette kan vi nu bruge til at vise at inverser også bevares. Vi ønsker at vise at $\psi(g^{-1})$ er invers element til $\psi(g)$.

$$\psi(g) \diamond \psi(g^{-1}) = \psi(g \star g^{-1}) = \psi(e_G) = e_H.$$

På samme måde kan vi komme frem til at $\psi(g^{-1}) \diamond \psi(g) = e_H$ og derfor må $\psi(g^{-1})$ netop være invers element til $\psi(g)$ i H.

For nu at se, at homomorfier bevarer potenser, kigger vi på $g^n = \underbrace{g \star ... \star g}_{n \text{ gange}}$.

$$\begin{aligned}
\psi(\underbrace{g \star ... \star g}_{n \text{ gange}}) &= \psi(\underbrace{g \star ... \star g}_{n-1 \text{ gange}} \star g) \\
&= \psi(\underbrace{g \star ... \star g}_{n-1 \text{ gange}}) \diamond \psi(g) \\
&= \psi(\underbrace{g \star ... \star g}_{n-2 \text{ gange}} \star g) \diamond \psi(g) \\
&= \psi(\underbrace{g \star ... \star g}_{n-2 \text{ gange}}) \diamond \psi(g) \diamond \psi(g) \\
&\vdots \\
&= \underbrace{\psi(g) \diamond ... \diamond \psi(g)}_{n \text{ gange}} = \Big(\psi(g)\Big)^n.
\end{aligned}$$

Lad os nu kigge på ordner. Hvis $|g| = n$ betyder det pr. definition, at $g^n = e_G$ hvor n er det mindste naturlige tal der opfylder dette. Vi vil nu vise at $(\psi(g))^n = e_H$, men n er *ikke nødvendigvis* det mindste tal, der opfylder dette.

$$\Big(\psi(g)\Big)^n = \psi(g^n) = \psi(e_G) = e_H.$$

Altså er $|\psi(g)| \leq |g|$. Hvis vi kigger på isomorfien φ gælder det naturligvis stadig. Husk at en isomorfi er en homomorfi, der har en invers, som igen er en homomorfi. Vi kan altså bruge regnereglen på φ^{-1} og opnå $|\varphi^{-1}(h)| \leq |h|$.

$$|g| = |\varphi^{-1}\Big(\varphi(g)\Big)| \leq |\varphi(g)| \leq |g|,$$

og dermed konkluderer vi at $|\varphi(g)| = |g|$.

Antag nu at G er abelsk. Det vil sige at det er ligegyldigt hvilket rækkefølge vi sammensætter ting i G. Se nu at

$$\psi(g_1) \diamond \psi(g_2) = \psi(g_1 \star g_2) = \psi(g_2 \star g_1) = \psi(g_2) \diamond \psi(g_1),$$

og derfor er billedet, altså $\psi(G)$, abelsk. Hvis vi kigger på φ^{-1} vil denne også sende abelske grupper til abelske grupper. Derfor, hvis H er abelsk vil $\varphi^{-1}(H) = G$ også være abelsk.

Til sidst betragter vi en cyklisk gruppe G. Vi kan altså frembringe G med blot ét element, dvs. $G = \langle a \rangle$. For et givent element g i G kan vi altså finde et n således at $g = a^n$, og da får vi

$$\psi(g) = \psi(a^n) = \psi(a)^n,$$

så $\psi(g)$ kan frembringes af $\psi(a)$. Dette sker ligegyldig valg af g, så hele $\psi(G) = \langle \psi(a) \rangle$.

Igen kan vi bruge denne egenskab på φ^{-1} og komme frem til at hvis H er cyklisk, så er $\varphi^{-1}(H) = G$ også cyklisk. □

Overordnet kan vi altså sige, at hvis vi har to isomorfe grupper, kan vi for hvert element g i G parre det med et tilsvarende element h i H, hvor h vil have alle de samme egenskaber i H, som g har i G. Isomorfe grupper er altså ens på alle måder vi betragter dem, pånær eventuelt hvad vi kalder de forskellige ting. Vi kan derfor betragte H som værende en kopi af G, hvor vi har givet elementerne nye navne.

Bemærkning 7.11. Hvis vores grupper ikke er for store og uoverskuelige, kan det være hjælpsomt at illustrere gruppestrukturen i det vi kalder en "kompositionstabel", ligesom den gangetabel vi kender fra folkeskolen. Vi kan for eksempel se på de to tabeller for $\mathbb{Z}/3\mathbb{Z}$ samt Z_3.

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

$\cdot$	1	a	a^2
1	1	a	a^2
a	a	a^2	1
a^2	a^2	1	a

Gruppestrukturen er illustreret ved placeringen af de forskellige elementer. Hvis vi definere en afbildning mellem de

to grupper, ud fra hvad der er placeret hvor i tabellerne, $[0]_3 \mapsto 1$, $[1]_3 \mapsto a$ og $[2]_3 \mapsto a^2$, er tabellerne identiske (pånær symbolet for vores kompositionsregel men det er ikke vigtigt). Dette betyder at vores afbildning er en isomorfi og grupperne er altså isomorfe.

Bemærkning 7.12. Pas på med at konkludere at to grupper ikke er isomorfe hvis deres kompositionstabeller ikke er helt ens. Hvis nu vi havde valgt at skrive søjlerne og rækkerne i en anden rækkefølge, ville det ikke være lige så tydeligt. For eksempel ved vi at Z_3 er isomorf med sig selv, men vi kan skrive dens gangetabel op på mindst to forskellige måder:

$\cdot$	1	a	a^2
1	1	a	a^2
a	a	a^2	1
a^2	a^2	1	a

$\cdot$	a	a^2	1
a	a^2	1	a
a^2	1	a	a^2
1	a	a^2	1

Vi vil derfor gerne have nogle flere værktøjer til at kunne vise at en afbildning er en isomorfi. For at tjekke om afbildningen er en homomorfi, bør vi som udgangspunkt gå aritmetisk frem, altså bare regne og se om ligheden holder. Til gengæld, når vi skal tjekke bijektivitet, tjekker vi surjektivitet og injektivitet hver for sig. Dette er ikke altid helt så ligetil. Vi introducerer derfor nu, det vi kalder *kernen* for en afbildning, hvilket hjælper os gevaldigt, når vi skal vise at en afbildning er injektiv.

Definition 7.13 (Kerne)**.** Lad $\varphi : G \to H$ være en afbildning. Kernen for φ er mængden

$$\ker \varphi := \{g \in G \mid \varphi(g) = e_H\},$$

altså alle de gruppeelementer, der bliver sendt til neutralelementet i H.

Eksempel 7.14. Vi har tidligere kigget på afbildningen $\varphi : \mathbb{Z}/16\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ defineret ved

$$\varphi([a]_{16}) = [a]_4.$$

Her har vi at neutralelementet i $\mathbb{Z}/4\mathbb{Z}$ er $[0]_4$. De elementer der bliver afbildet til $[0]_4$ er netop mængden $\{[0]_{16}, [4]_{16}, [8]_{16}, [12]_{16}\}$. Denne mængde er derfor kernen af φ. ∘

Eksempel 7.15. Vi kan også se på afbildningen $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ der er defineret ved

$$\varphi(a) = [a]_n.$$

Her er kernen alle hele tal, der er delelige med n. ∘

Sætning 7.16. Lad $\varphi : G \to H$ være en homomorfi. Da er φ injektiv hvis og kun hvis $\ker \varphi = \{e_H\}$.

Bevis. Vi ser fra sætning 7.10 at $\varphi(e_G) = e_H$, så kernen af φ består, som minimum, af elementet e_G.

Antag at φ er injektiv. Dette betyder at e_H maksimalt kan blive "ramt af" ét element fra G via φ. Vi ved at det allerede bliver ramt af e_G, så vi kan ikke have flere elementer i kernen end netop e_G.

Antag omvendt, at $\ker \varphi = \{e_G\}$. Antag endvidere, at $\varphi(a) = \varphi(b)$. Dette medfører, at $\varphi(a) \diamond \varphi(b)^{-1} = e_H$. Eftersom φ er en homomorfi opnås

$$\varphi(a) \diamond \varphi(b)^{-1} = \varphi(a) \diamond \varphi(b^{-1}) = \varphi(a \star b^{-1}),$$

hvilket betyder at $\varphi(a \star b^{-1}) = e_H$, så $a \star b^{-1}$ er et element i kernen, men pr. antagelse, var e_G det eneste element i $\ker \varphi$, så $a \star b^{-1} = e_G$. Dette giver os at $a = b$, så φ er injektiv. □

Dette afslutter vores kapitel om isomorfier. Vi har nu samlet os en god mængde værktøjer til at sammenligne forskellige grupper med. Det viser sig nemlig at man kan nøjes med nogle få familier af grupper, som man så kan bruge til at beskrive resten med. Bagerst i kapitlet, finder vi et skema over *samtlige* grupper op til orden 11. Hvis du synes der mangler nogle grupper i skemaet er det netop fordi gruppen er isomorf til noget der allerede er på listen.

8 Permutationsgrupper

De næste grupper vi skal se på er ganske simple at beskrive, men kan være yderst komplicerede.

Intuitivt er permutationer ombytninger. Forestil dig, at du på et bord lægger talkortene 1 til 7 i rækkefølge. Hvis du f.eks. ombytter 3 og 5, og 7 og 2, har du permuteret kortene. I symboler skriver vi,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 5 & 4 & 3 & 6 & 2 \end{pmatrix},$$

hvor øverste række angiver placeringen af kortene før ombytningen, og nederste række angiver placeringen af kortene efter ombytningen.

Definition 8.1 (Permutation (intuitiv))**.** Lad n være et naturligt tal. En permutation af tallene 1 til n er en ombytning af ingen eller flere af tallene.

Definition 8.2 (Skemanotation for permutationer)**.** En permutation kan skrives som et talskema med 2 rækker. På øverste og nederste række står hvert tal mellem 1 og n præcis én gang:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

hvor $\sigma(1), \ldots, \sigma(n-1), \sigma(n)$ angiver tallene 1 til n i ombyttet rækkefølge. Skemaet fortæller, at et tal på øverste række ombyttes med tallet umiddelbart nedenunder. Bemærk at σ er en bijektiv afbildning.

Eksempel 8.3. Det er ikke vigtig hvilken rækkefølge søjlerne står i, men blot hvilke tal der står over og under hinanden. Dermed repræsenterer

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

og

$$\begin{pmatrix} 2 & 3 & 1 \\ 3 & 2 & 1 \end{pmatrix}$$

den samme permutation. ∘

Vi kan på naturlig vis sammensætte permutationer af samme længde. Hvis σ og τ er permutationer af længde n, så kan man starte med at ombytte som foreskrevet af σ og dernæst ombytte som foreskrevet af τ. Hvis man glemmer, at man har ombyttet af to omgange og blot noterer hvor tallene ender, så har man en ny permutation. Denne permutation kalder vi $\tau\sigma$.

Definition 8.4 (Sammensætning af permutationer)**.** Lad σ og τ være permutationer. Da er sammensætningen af τ og σ permutationen givet ved

$$\tau\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \cdots & \tau(\sigma(n-1)) & \tau(\sigma(n)) \end{pmatrix}$$

hvor $\tau(\sigma(k))$ for $1 \leq k \leq n$ angiver, at der først er ombyttet ifølge σ og derefter er resultatet ombyttet ifølge τ.

Sætning 8.5 (Permutationsgruppen)**.** Lad S_n være mængden af permutationer af længde n. Udstyret med sammensætningen som defineret i definition 8.4 er S_n en gruppe.

Neutralelementet, vil være identitetspermutationen *id*, som er givet ved

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}$$

og den inverse til $\sigma \in S_n$ er givet ved

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & \sigma(n) \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}.$$

Når man arbejder med permutationer er skemanotationen lidt kluntet og vi vil derfor i stedet opskrive permutationer på form af *disjunkte cykler*. For at forstå, hvad dette betyder, er det lettest at se på et eksempel.

Eksempel 8.6 (Permutation som produkt af disjunkte cykler)**.** Betragt permutationen

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 1 & 6 & 5 & 2 & 3 \end{pmatrix}.$$

Prøv at se hvad der sker, hvis vi vælger et bestemt tal, lad og sige 4, og benytter permutationen gentagende gange (herunder betyder $\overset{\sigma}{\mapsto}$ at vi benytter permutationen på tallet til venstre og derved opnår tallet til højre):

$$4 \overset{\sigma}{\mapsto} 6 \overset{\sigma}{\mapsto} 2 \overset{\sigma}{\mapsto} 4.$$

På et tidspunkt får vi altså igen 4, så hvis vi fortsatte ville mønsteret blot gentage sig selv. Vi har fundet en såkaldt *cykel*. I symboler skriver vi $(2\,4\,6)$, hvilket skal læses som at hvert tal bliver sendt over i tallet til højre, indtil man når til den højre parentes og derfra sender tilbage til det første tal. Cykelnotationen definere også en permutation, og det er underforstået at alle tal der ikke bliver nævnt i cyklen ikke bliver ændret af permutationen, og altså blot bliver sendt til sig selv.

Tilsvarende finder vi, at

$$1 \overset{\sigma}{\mapsto} 7 \overset{\sigma}{\mapsto} 3 \overset{\sigma}{\mapsto} 1,$$

hvilket leder til cyklen (1 7 3). Derudover bliver 5 sendt til sig selv, så vi har cyklen (5).

Vi kan nu bruge de fundne cykler til at skrive σ på en mere kompakt form, som

$$\sigma = (1\,7\,3)(2\,4\,6).$$

Her udelader vi (5), og vi udelader generelt cykler af længde en. Bemærk at cyklerne ovenfor ikke har nogle tal til fælles. ∘

Definition 8.7. Et produkt af cykler der ikke har nogle tal til fælles kaldes *et produkt af disjunkte cykler*.

Alle permutationer kan ved at følge fremgangsmåden beskrevet her opskrives som et produkt af disjunkte cykler. Hvis alle cyklerne er af længde 1 er der tale om identitetspermutationen og vi skriver id eller blot (1). Lad os tage et eksempel mere.

Eksempel 8.8. Betragt permutationen

$$\sigma = \begin{pmatrix} 2 & 4 & 3 & 1 & 6 & 5 \\ 1 & 2 & 5 & 6 & 4 & 3 \end{pmatrix}.$$

Her ser vi at

$$1 \overset{\sigma}{\mapsto} 6 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 2 \overset{\sigma}{\mapsto} 1,$$

og tager vi nu et tal der ikke er i denne cykel, lad os sige 3, får vi

$$3 \overset{\sigma}{\mapsto} 5 \overset{\sigma}{\mapsto} 3$$

og dette er alle cyklerne, da alle tal fra 1 til 6 indgår i en af de fundne cykler. Vi får dermed at

$$\sigma = (1\,6\,4\,2)(3\,5).$$

∘

Man kan godt gange ikke-disjunkte cykler sammen, men vi vil altid tilstræbe at skrive et generelt produkt af cykler om til et produkt af disjunkte cykler.

Eksempel 8.9 (Produkt af ikke disjunkte cykler)**.** Lad $\sigma = (1\,2\,5\,3)$ og $\tau = (2\,3)$, da er

$$\sigma\tau = (1\,2\,5\,3)(2\,3).$$

Dette er ikke et produkt af disjunkte cykler, fordi 2 og 5 går igen i begge cykler.

For at gøre dette produkt til et produkt af disjunkte cykler, skal man, ligesom når man finder cyklerne ud fra skemanotationen, følge tallenes vej gennem permutationen. Det gør vi ved at følge permutationen fra højre mod venstre. Tag for eksempel 1. Permutationen $(2\,3)$ ændrer ikke 1, så 1 sendes videre til $(1\,2\,5\,3)$ som sender 1 over i 2. Tallet 2 sendes af τ over i 3, og derefter sendes 3 af σ over i 1, så $\sigma\tau$ sender 2 over i 1. Dermed bliver den ene cykel $(1\,2)$. Tag nu et tal der ikke er i denne cykel, så som 3. Tallet 3 sendes af τ over i 2 og af σ sendes 2 videre over i 5, så 3 sendes af $\sigma\tau$ over i 5. Desuden indgår 4 ikke i nogen af cyklerne, så $\sigma\tau$ fastholder 4. Dermed er

$$\sigma\tau = (1\,2)(3\,5)$$

og dette er et produkt af disjunkte cykler. ∘

Bemærkning 8.10. Det gælder ikke generelt, at permutationer kommuterer (så S_n er ikke en abelsk gruppe), men disjunkte cykler kommuterer. Det vil sige at vi godt må bytte om på disjunkte cykler.

Bemærkning 8.11. Lad $(a_1\,a_2\,\ldots\,a_n)$ være en cykel med n elementer. Da er $(a_1\,a_2\,\ldots\,a_n)^{-1} = (a_n\,a_{n-1}\,\ldots\,a_1)$. Cykler inverteres altså ved at opskrive dem baglæns.

Definition 8.12 (Permutation, formel)**.** Lad n være et naturligt tal. En permutation σ er en bijektiv afbildning fra $\{1, 2, \ldots, n\}$ til $\{1, 2, \ldots, n\}$.

Bemærkning 8.13. Vi kan også permutere andet end bare tal, for eksempel ses nedenunder en permutation af de fire kulører for spillekort

$$\sigma = \begin{pmatrix} \spadesuit & \heartsuit & \clubsuit & \diamondsuit \\ \heartsuit & \diamondsuit & \clubsuit & \spadesuit \end{pmatrix}.$$

Definition 8.14 (Permutation, generel)**.** Lad X være en mængde. En permutation af X er en bijektiv afbildning fra X til X.

Med dette grundlag kan vi nu definere permutationsgrupperne mere generelt end vi gjorde i Sætning 8.5.

Sætning 8.15 (Permutationsgrupper, generel)**.** Lad X være en mængde, og lad S_X være mængden af bijektioner på X (S_X er permutationerne af X). Da er $(S_X, \circ)$ en gruppe, hvor $\circ$ er funktionssammensætning.

Eksempel 8.16. Hvis vi lader K være mængden af spillekortkulører, altså $K = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$, vil S_K være alle permutationer af kulørerne, og sætningen fortæller os at vi har en gruppe af disse permutationer sammen med funktionssammensætning. ∘

Vi vil dog primært betragte permutationer i S_n, da enhver permutation af n elementer, kan skrives som en permutation af de første n tal. Ligesom at en permutation på K kan oversættes til en permutation på $\{1, 2, 3, 4\}$ ved at tildele hver kulør en unik værdi mellem 1 og 4.

Det vil altså sige at S_4 og S_K isomorfe, og derfor er det ikke så vigtigt for os hvilken af de to grupper vi betragter, fordi de grundlæggende er ens.

Definition 8.17. Lad σ være en permutation. Da kalder vi a for et *fixpunkt* for σ hvis $\sigma(a) = a$. Hvis a ikke er et fixpunkt, siger vi at σ *flytter* a.

Definition 8.18. Lad os definere en funktion m, der for enhver permutation σ i S_n giver antallet af cykler i σ's cykeldekomposition *inklusiv* cykler af længde 1.

Eksempel 8.19. Lad σ være permutationen $(1\,2\,3)$ fra S_3. Der er netop én cykel i denne opskrivning, så $m(\sigma) = 1$.

Hvis vi derimod betragter $\sigma = (1\,2\,3)$ som en permutation fra S_4, indgår der to cykler i opskrivningen, da vi skal huske (4) som vi ellers undlader at skrive. Da er $m(\sigma) = 2$. ∘

Eksempel 8.20. Hvis vi nu betragter permutationen $\tau = (1)(2\,4)(3\,4\,5)$ i S_5, har vi ikke været dovne og undladt (1), men vi skal stadig passe på. Hvis vi kigger en ekstra gang, ser vi at opskrivningen ikke er et produkt af disjunkte cykler, så vi omskriver først $(2\,4)(3\,4\,5)$ til $(2\,4\,5\,3)$ og får derfor at $\tau = (1)(2\,4\,5\,3)$. Dermed er $m(\tau) = 2$. ∘

9 Undergrupper

I dette kapitel skal vi undersøge det vi kalder *undergrupper*, som er grupper inde i andre grupper. Vi er interesserede i undergrupper af mange årsager, men blandt andet fordi de kan fortælle os ting om den store gruppe.

Definition 9.1 (Undergruppe)**.** $(U,\star)$ er en undergruppe af $(G,\star)$ hvis $U \subseteq G$ og $(U,\star)$ er en gruppe.

Bemærkning 9.2. De to grupper har samme kompositionsregel, hvilket vil sige at hvis u og v er to elementer i U (og dermed også i G) vil $u \star v$ være ens i U og i G.

Bemærkning 9.3. Da $(U,\star)$ skal være en gruppe betyder det, at hvis vi har to elementer x og y i U, må vi også have x^{-1}, y^{-1} og $x \star y$.

Eksempel 9.4. Som det første eksempel på en undergruppe, betragter vi $(\langle r\rangle,\cdot)$ som undergruppe af D_{2n}.

Vi ser at $\langle r\rangle = \{1,r,r^2,...,r^{n-1}\}$. Dette er tydeligt en delmængde af $\langle r,s\rangle$. Vi ender med en gruppe, der bare består af de n rotationer af vores n-kant.

Samme argument kan bruges om gruppen $(\langle s\rangle,\cdot)$. Denne er også en undergruppe af D_{2n}, bestående af de to elementer 1 og s. ∘

Eksempel 9.5. Hvis vi betragter

$$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$$

med + som operation har vi en undergruppe af $(\mathbb{Z},+)$, idet vi har neutralelementet, 0, og det inverse element til et hvert lige tal også er lige, så dem har vi også med. Vi arver også fra $(\mathbb{Z},+)$ at den associative lov gælder, og dermed er det en gruppe. ∘

Eksempel 9.6. Med nogenlunde samme argumentation som i det forrige eksempel har vi at $n\mathbb{Z}$ er en undergruppe af $(\mathbb{Z},+)$. ∘

Proposition 9.7. Givet en gruppe $(G,\star)$ og en delmængde $H \subseteq G$ er det nok at tjekke at H er *stabil* under at tage inverser og under komposition. Det vil sige at hvis vi tager x i H skal vi tjekke om x^{-1} ligger i H og tager vi derudover et ekstra element y i H tjekker vi om $x \star y$ ligger i H. Hvis dette er tilfældet, uafhængigt af vores valg af x og y, er H en undergruppe.

Bevis. Resultatet kommer af, at når vi ved vores mængde ligger inden i en gruppe og vi har samme operation, får vi en

masse foræret. Lad os tjekke de tre kriterier for at være en gruppe.

For a, b, c i H ved vi at $a \star (b \star c) = (a \star b) \star c$ idet a, b og c også er elementer i G, hvor vi ved det gælder.

Hvis vi ved at x^{-1} ligger der når x ligger der, og vi ved at H er stabil under at komponerer elementer, ved vi også at $x^{-1} \star x = e$ er et element i H.

Her brugte vi at de inverse elementer findes, men det ved vi fordi G er en gruppe, og vi antager altså blot at de ligger i vores mængde H.

□

Eksempel 9.8. Vi ved at $(\mathbb{Q},+)$ og $(\mathbb{Z},+)$ er grupper, og da de har samme operation og $\mathbb{Z} \subseteq \mathbb{Q}$, har vi at $(\mathbb{Z},+)$ er en undergruppe af $(\mathbb{Q},+)$. ∘

Nogle gange når vi har en delmængde af en gruppe kan det være svært at tjekke om det faktisk er en undergruppe, ved direkte at vise at det er en gruppe. Det viser sig dog at vi kan slippe afsted med ikke at tjekke alle betingelserne fra definitionen af en gruppe. Det er det denne proposition giver os.

Sætning 9.9. Lad $(G,\star)$ være en gruppe og $H \subseteq G$ være en delmængde af G. Da er H en undergruppe af G hvis og kun hvis de følgende to betingelser er opfyldt:

1. H er ikke den tomme mængde, altså der er mindst et element x i H.

2. For alle x, y i vores mængde H vil $x \star y^{-1}$ også være et element i H.

Hvis H er en endelig mængde, er det nok at tjekke at H ikke er tom, og at mængden er lukket under komposition, altså at hvis vi har x,y i H vil $x \star y$ være i H.

Bevis. Lad os starte med at vise at hvis H er en undergruppe, så er de to betingelser opfyldt. Hvis H er en undergruppe, ved vi at H specielt er en gruppe, så for x og y i H (som må findes da H om ikke andet i hvert fald indeholder neutralelementet) vil y^{-1} være i H, og gruppen er desuden lukket under kompositionsreglen, så $x \star y^{-1}$ vil være et element i H. Dermed har vi vist den ene retning i vores proposition.

Lad os nu antage at for $H \subseteq G$ er de to betingelser opfyldt, og vise H må være en undergruppe. Vi vælger først et x i H, hvilket vi kan da H ikke er tom. Lad nu $y = x$. Da får vi ved at bruge den anden egenskab at $x \star x^{-1} = e$ ligger i H, så vi har vores neutralelement. Ved at bruge betingelse 2 igen får vi at $e \star x^{-1} = x^{-1}$ ligger i H, så da vi kunne have valgt et vilkårligt x i H er H lukket under at tage inverser, altså for et vilkårligt element, har vi også dets inverse element med.

Hvis vi nu lader x og y være to elementer i H, så indeholder H både x og y^{-1} på grund af det vi lige har vist, og dermed får vi også at $x \star (y^{-1})^{-1} = xy$ ligger i H. Dermed er H også lukket under at komponerer to vilkårlige elementer, så H er en undergruppe af G per Proposition 9.7.

□

Bemærkning 9.10. Vi har ikke argumenteret for at det, når H er endelig, er nok at H er lukket under multiplikation. Kan du overbevise dig selv om at det er sandt? Det er ikke helt nemt, men vi kigger mere på det i opgaverne.

Definition 9.11. Lad $(G,\star)$ være en gruppe, og lad N være en undergruppe. Lad nu n være et element i undergruppen og x et element i G. Da kaldes elementet $x \star n \star x^{-1}$ for den *konjugerede* af n med x og mængden

$$xNx^{-1} = \{x \star n \star x^{-1} | n \in N\}$$

kaldes den *konjugerede* af N med x. Hvis $xNx^{-1} = N$ for et x i G siges dette x at normalisere N, og hvis ethvert x i G

normaliserer N siger vi at N er en *normal* undergruppe af G, og skriver $N \trianglelefteq G$.

Vi kommer til at kigge mere på normale undergrupper i øvelserne, men lad os se på nogle eksempler.

Eksempel 9.12. Enhver gruppe har sig selv som normal undergruppe, og den trivielle undergruppe $\langle e \rangle$ er også en normal undergruppe, idet e kommuterer med alle andre elementer, fordi $n \star e \star n^{-1} = n \star n^{-1} \star e = e$. ∘

Eksempel 9.13. Betragt Z_{10} og $\langle a^2 \rangle = \{1,a^2,a^4,a^6,a^8\} = \{a^{2i} | i \in \{0,1,2,3,4\}\}$. Dette er en normal undergruppe, idet et hvert element i Z_{10} kan skrives som a^k for $0 \leq k \leq 9$. Vi får derfor $a^k a^{2i} a^{-k} = a^{k+2i-k} = a^{2i} \in \langle a^2 \rangle$, og da dette er generelt, er undergruppen normal. ∘

Eksempel 9.14. Lad os kigge på D_{12}. Undergruppen $\langle r^3 \rangle = \{1,r^3\}$ er normal, idet 1 kommuterer med alt i alle multiplikative grupper, og r^3 desuden kommuterer med alt, fordi elementet både kommuterer med s og med r idet $sr^3s = ssr^{-3} = r^{-3} = r^3$ og $rr^3r^{-1} = r^{1+3-1} = r^3$. Det er nok, fordi ethvert element kan skrives på formen $r^i s^j$ for $i \in \{0,1,...,5\}$ og $j \in \{0,1\}$. ∘

10 Tabel over grupper af lille orden

Herunder ses en komplet tabel af grupper af orden op til 11.

Orden	Abelske grupper	Ikke-abelske
1	Z_1	Ingen
2	Z_2	Ingen
3	Z_3	Ingen
4	Z_4 & $Z_2 \times Z_2$	Ingen
5	Z_5	Ingen
6	Z_6	S_3
7	Z_7	Ingen
8	Z_8, $Z_4 \times Z_2$ & $Z_2 \times Z_2 \times Z_2$	D_8 & Q_8
9	Z_9 & $Z_3 \times Z_3$	Ingen
10	Z_{10}	D_{10}
11	Z_{11}	Ingen
p	Z_p	Ingen

Bemærk at vi ikke har stiftet bekendskab med Q_8 endnu. Q_{2n} er familien af kvarterniongrupper. De er *også* nogle interessante grupper, som du kan lære mere om hvis du vil studere abstrakt algebra i fremtiden.

11 Opgaver

Opgaver til grupper

●● **Opgave 11.1:**
Vis at grupperne fra Bemærkning 2.11 og 2.13 faktisk er grupper. Du kan søge inspiration i Eksempel 2.10 og 2.12. Er grupperne abelske?

● **Opgave 11.2:**
Afgør hvilke af de følgende kompositionsregler, $\star$, der er associative.

1) kompositionsreglen $\star$ på $\mathbb{Z}$ defineret ved $a \star b = a - b$.

2) kompositionsreglen $\star$ på $\mathbb{R}$ defineret ved $a \star b = a + b + ab$.

3) kompositionsreglen $\star$ på $\mathbb{Q}$ defineret ved $a \star b = \frac{a+b}{5}$.

4) kompositionsreglen $\star$ på $\mathbb{Q} \setminus \{0\}$ defineret ved $a \star b = \frac{a}{b}$.

●● **Opgave 11.3:**
Hvilke af følgende afbildninger $*$ er kompositionsregler på de tilhørende mængder?

1) $a * b = \frac{a}{b}$ på $\mathbb{Q}$

2) $a * b = \frac{a}{b}$ på $\mathbb{Z} \setminus \{0\}$

3) $a * b = \frac{a}{b}$ på $\mathbb{Q} \setminus \{0\}$

4) $a * b = \frac{a}{b}$ på $\mathbb{Q}_+$

5) $a * b = a + b + ab$ på $\mathbb{Z}$.

● **Opgave 11.4:**
Lad G være mængden $\{0,1\}$ og lad $\star$ være defineret på G således at

$$0 \star 0 = 0 \qquad 0 \star 1 = 1 \qquad 1 \star 1 = 0 \qquad 1 \star 0 = 1.$$

Vis at $(G,\star)$ er en gruppe og bestem ordnen af begge elementer.

- **Opgave 11.5:**
  Hvilke af følgende kompositionsregler er associative, og hvilke er kommutative?

  1) $+$ defineret på $\mathbb{Z}$.

  2) $-$ defineret på $\mathbb{Z}$.

  3) $\cdot$ defineret på $\mathbb{Z}$.

  4) $/$ defineret på $\mathbb{Q} \setminus \{0\}$.

●●● **Opgave 11.6:**
Afgør hvilke af de følgende mængder, der er grupper med addition, $+$:

1) de rationale tal, der skrevet på forkortet form, har ulige nævner (inklusive $0 = 0/1$),

2) de rationale tal, der skrevet på forkortet form, har lige nævner sammen med tallet 0,

3) mængden af rationale tal med 1 eller 2 som nævner,

4) mængden af rationale tal med 1, 2 eller 3 som nævner.

- **Opgave 11.7:**
  Bevis at påstanden fra Bemærkning 2.18 er sand. Altså at ab's invers er $b^{-1}a^{-1}$.

●● **Opgave 11.8:**
Lad $(G, \star)$ være en gruppe. Antag at der gælder $x \star x = e$ for alle x i G. Vis at G er abelsk, altså at der gælder at $x \star y = y \star x$ for alle x og y.

●●● **Opgave 11.9:**
Lad $(G,\star)$ være en endelig gruppe, og lad $a \in G$.

1) Vis at ordenen af a er endelig

2) Antag at $|a| = n$. Vis følgende biimplikation:

$$n|k \Leftrightarrow a^k = e.$$

●● **Opgave 11.10:**
Lad x være et element i gruppen G. Vis at $x^2 = 1$ hvis og kun hvis $|x|$ er enten 1 eller 2.

●● **Opgave 11.11:**
Lad x være et element i gruppen G og lad n være et positivt heltal.

1) Vis at hvis $|x| = n$, så gælder der at $x^{-1} = x^{n-1}$.

2) Vis at hvis $x^{-1} = x^{n-1}$, så er $|x| \leq n$.

● **Opgave 11.12:**
Lad x være et element i gruppen G. Vis at x og x^{-1} har samme orden.

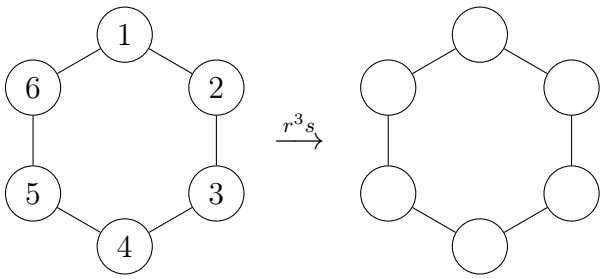
●●● **Opgave 11.13:**
Lad x være et element af uendelig orden i en gruppe G. Vis at alle potenser af x vil være forskellige i G, altså at hvis n og m er forskellige positive heltal, så er $x^n \neq x^m$.

●●● **Opgave 11.14:**
Lad $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a,b \in \mathbb{Q}\}$. Vis at G er en gruppe under addition.

●● **Opgave 11.15:**
Lad $G = \{e,a,b,c\}$. Definer en kompositionsregel,$\star$, på G således at $(G,\star)$ er en gruppe med e som neutralelement.

Opgaver til Diedergrupper

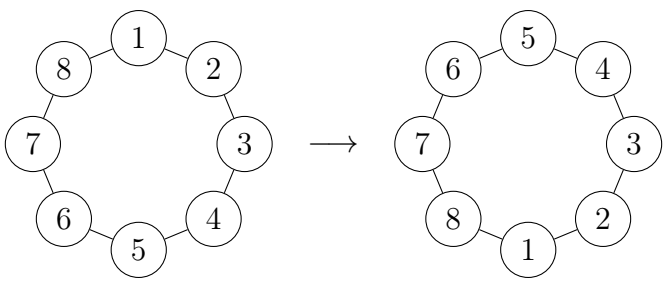
●● **Opgave 11.16:**
I denne opgave vil vi betragte D_{12}. Hvad sker der hvis vi først spejler, og derefter roterer 3 gange? Altså bruger r^3s på vores sekskant?



Hvad sker der hvis vi stedet bruger sr^3, altså hvor vi først roterer og derefter spejler? Hvad med r^2s og sr^2? Er der nogle af disse fire der giver det samme resultat?

●● **Opgave 11.17:**
Opskriv alle elementer i D_{12}. Der er i alt 12 elementer.

●● **Opgave 11.18:**
Find en sammensætning af r og s, som giver os transformationen



som svarer til en vandret spejling. Hvordan ville vi lave denne spejling med en tikant? Kan vi lave den med en syvkant?

●● **Opgave 11.19:**
Opskriv alle elementerne i D_{16}.

●● **Opgave 11.20:**
I denne opgave betragter vi D_{16}. Tænk for hver opgave også over hvilke elementer der giver det ønskede.

1) Hvor mange ottekanter findes hvor 1 står øverst, og hvor mange hvor 7 står øverst?

2) Lad os gå med uret rundt i ottekanten. Hvor mange måder kan vi have fem efterfulgt af seks på? Hvor mange måder kan vi blot have dem ved siden af hinanden?

3) Hvor mange måder kan vi have 5 og 3 på samme vandrette linje? Hvad med 4 og 8?

4) Kan I finde en kombination af krav fra de tidligere opgaver vi kan kræve samtidig, som da giver os en entydig ottekant?

•• **Opgave 11.21:**
Bestem ordnerne af alle elementer i grupperne D_6, D_8 og D_{10}.

Opgaver til restklasser

• **Opgave 11.22:**
Gruppér tal der er kongruente modulo 3.

17	14	27	31	41
9	300	7	64	0

• **Opgave 11.23:**
Udregn følgende udtryk:

1) $[23]_5 + [101]_5$

2) $[31]_8 \cdot [33]_8$

3) $[58]_{60} \cdot [59]_{60}$

4) $[3578]_{11} \cdot ([36]_{11} + [8]_{11})$

•• **Opgave 11.24:**
Find inverser til følgende

1) $[2]_7$ i $(\mathbb{Z}/7\mathbb{Z},+)$ og i $((\mathbb{Z}/7\mathbb{Z})^\times,\cdot)$

2) $[-1]_{987}$ i $(\mathbb{Z}/987\mathbb{Z},+)$ og i $((\mathbb{Z}/987\mathbb{Z})^\times,\cdot)$

3) $[5]_{13}$ i $(\mathbb{Z}/13\mathbb{Z},+)$ og i $((\mathbb{Z}/13\mathbb{Z})^\times,\cdot)$

4) $[7]_{24}$ i $(\mathbb{Z}/24\mathbb{Z},+)$

●● **Opgave 11.25:**
Vis at hvis a har rest r_1 ved division med n og hvis b har rest r_2 ved division med n, så findes der et heltal k således at $a+b = kn + (r_1 + r_2)$.

●● **Opgave 11.26:**
Betragt den 1'te restklassegruppe, $\mathbb{Z}/1\mathbb{Z}$.

1) Hvordan ser gruppen $\mathbb{Z}/1\mathbb{Z}$ ud?

2) $\mathbb{Z}/1\mathbb{Z}$ har samme gruppestruktur som et af de eksempler vi så i starten af kapitlet. Hvilken gruppe?

● **Opgave 11.27:**
Bestem ordnerne af samtlige elementer i gruppen $\mathbb{Z}/12\mathbb{Z}$.

●●● **Opgave 11.28:**
Bevis Korollar 4.6.

●● **Opgave 11.29:**
Skriv elementerne i $((\mathbb{Z}/7\mathbb{Z})^\times,\cdot)$ op, og bestem deres inverse elementer, med udgangspunkt i Eksempel 4.13.

●● **Opgave 11.30:**
Følgende opgaver er eksempler på hvorfor $((\mathbb{Z}/n\mathbb{Z})^\times,\cdot)$ ikke altid er en gruppe.

1) Vi betragter mængden $\{[1]_6,...,[5]_6\}$ sammen med multiplikation. Kom med et konkret eksempel på hvorfor dette ikke er en gruppe.

2) Vis ligeledes hvorfor $\{[1]_{10},...,[9]_{10}\}$ med multiplikation heller ikke kan ses som en gruppe.

Opgaver til Cykliske grupper og frembringere

- **Opgave 11.31:**
  Lad $G = Z_{12} = \{1,a,a^2,...,a^{11}\}$.

  1) Find elementer af orden henholdsvis 12, 6, 4 og 3.

  2) Find den inverse til a^5.

- **Opgave 11.32:**
  Betragt $G = \mathbb{Z}/4\mathbb{Z} = \langle [1]_4 \rangle$. Vis at vi kan vælge $[3]_4$ som frembringer i stedet for $[1]_4$.

- **Opgave 11.33:**
  Vi ved at $G = (\mathbb{Z},+)$ er frembragt af 1, men vi vil nu kigge på andre måder at frembringe gruppen.

  1) Frembringer mængden $\{2,3,4,5\}$ hele vores gruppe $(\mathbb{Z},+)$? Hvis ja, kan vi så nøjes med nogle af elementerne? Hvis nej, kan I så forklare hvorfor det går galt?

  2) Hvad med $\{2,8,16\}$, frembringer denne mængde G? Hvis ja, kan vi så nøjes med nogle af elementerne? Hvis nej, kan I så forklare hvorfor det går galt?

  3) Hvad så med $\{9,16\}$? Hvis det går godt, kan vi så nøjes med nogle af elementerne? Hvis det ikke gør, kan I så forklare hvorfor det går galt?

- **Opgave 11.34:**
  Betragt $G = \mathbb{Z}/6\mathbb{Z} = \langle [1]_6 \rangle$. Find et andet element, der frembringer gruppen. Hvor mange forskellige mulige frembringere har vi?

- **Opgave 11.35:**

  1) Vis at gruppen $\mathbb{Z}/7\mathbb{Z}$ som defineret i Sætning 4.7 er frembragt af restklassen $[15]_7$.

2) Mind dig selv om hvilket element der frembringer $(\mathbb{Z},+)$. Overvej hvordan de to frembringere giver mening i forhold til hinanden.

- **Opgave 11.36:**
  Hvad er ordenen af den gruppe der er frembragt af r inde i D_8? Hvad med i D_{14}? Og hvad med i D_{2n}?

Opgaver til Isomorfier

- **Opgave 11.37:**
  Betragt grupperne $G = (\{0\}, +)$ og $H = (\{1\}, \cdot)$. Bestem en isomorfi $\varphi : G \to H$, som altså viser at de to gruper er isomorfe.

- **Opgave 11.38:**
  Overbevis dig selv om at to endelige grupper har lige mange elementer hvis der findes en isomorfi mellem dem, som skrevet lige under definition 7.1.

- **Opgave 11.39:**
  Vis at de tre grupper, $\mathbb{Z}/2\mathbb{Z}$, Z_2 og S_2 er isomorfe indbyrdes med hinanden.

- **Opgave 11.40:**
  Betragt $G = \mathbb{Z}/7\mathbb{Z}$ og $H = Z_7$. Vi definerer en afbildning, $\varphi : G \to H$ ved

$$\varphi([x]_7) = a^x.$$

1) Vis at φ er en isomorfi.

2) Kan vi gøre noget tilsvarende for at opnå en generel isomorfi imellem $Z/n\mathbb{Z}$ og Z_n?

●● **Opgave 11.41:**
Vis at hvis G_1 er isomorf til G_2 og G_2 er isomorf til G_3, så er G_1 isomorf til G_3.

●●● **Opgave 11.42:**
Vis at S_3 er isomorf med D_6.

●● **Opgave 11.43:**
Lad G være en gruppe med elementet g som har orden n. Lad H være en gruppe hvor ingen gruppeelementer har orden n. Vis at de to grupper ikke er isomorfe med hinanden.

●●● **Opgave 11.44:**
Lad $G = \langle a \rangle$ og $H = \langle b \rangle$ være to cykliske grupper. Antag at de begge har orden n. Vis at $G \cong H$.

Opgaver til Permutationsgrupper

● **Opgave 11.45:**
Lad σ og τ være to permutationer i S_6 givet ved

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix} \quad \text{og} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix}.$$

Opskriv permutationerne som produkter af disjunkte cykler.

● **Opgave 11.46:**
Vi minder os selv om, hvad et fixpunkt er. Fra Definition 8.17 har vi at det er et element der ikke flyttes af vores permutation.

1) Bestem fixpunkter for permutationen i Eksempel 8.6 og i Bemærkning 8.13.

2) Bestem fixpunkter for de følgende permutationer:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}.$$

●● **Opgave 11.47:**
Vi vil nu kigge nærmere på permutationerne fra Opgave 11.46.

1) Bestem sammensætningerne $\rho \circ \tau$ og $\tau \circ \rho$ og deres fixpunkter.

2) Bestem σ^{-1}, τ^{-1} og ρ^{-1}.

3) Bestem $\tau \circ \tau^{-1}$ og $\tau^{-1} \circ \tau$ og deres fixpunkter.

4) Omskriv σ, τ og ρ til cykelform. Find nu $\rho \circ \tau$ og $\tau \circ \rho$ ud fra cyklerne.

5) Kan vi sige noget om sammenhængen mellem fixpunkter og cykellængder?

●● **Opgave 11.48:**
Lad os se om vi kan sige nogle generelle ting om S_n.

1) Find to permutationer σ,τ fra S_3 der ikke kommuterer, altså to permutationer så $\tau \circ \sigma \neq \sigma \circ \tau$. Dermed er S_3 ikke en abelsk gruppe.

2) Brug nu din permutation fra delopgave 1 til at vise at S_n for alle $n \geq 3$ ikke er abelsk.

3) Overvej hvad der sker når $n = 1$ eller $n = 2$.

●● **Opgave 11.49:**
Bevis at ordenen af S_n er $n!$, altså $n(n-1)\cdots 2 \cdot 1$.

● **Opgave 11.50:**
På mængden {1,2,3,4,5,6,7,8} er givet følgende produkt af cykler: $(1\,5\,6\,7\,3)(8\,2\,4\,6)(3\,5\,7)$.

Opskriv permutationen som et produkt af disjunkte cykler.

Opgaver til Undergrupper

●● **Opgave 11.51:**
Vis at $(n\mathbb{Z},+)$ er en undergruppe af $(\mathbb{Z},+)$ som påstået i Eksempel 9.6.

●● **Opgave 11.52:**
Find to undergrupper af $(\mathbb{R},+)$.

●● **Opgave 11.53:**
Lad G være en gruppe og lad g være et element i G. Vis at $\langle g \rangle$ er en undergruppe af G.

●●● **Opgave 11.54:**
Vis resten af Sætning 9.9 som beskrevet i Bemærkning 9.10.

●●● **Opgave 11.55:**
Lad $(\langle S \rangle,\star)$ være en gruppe og lad M være en delmængde af S, dvs. $M \subseteq S$. Vis at $(\langle M \rangle,\star)$ er en undergruppe af $(\langle S \rangle,\star)$.

● **Opgave 11.56:**
Lad $(V,\star)$ være en undergruppe af $(U,\star)$, hvor $(U,\star)$ er en undergruppe af $(G,\star)$. Vis at $(V,\star)$ er en undergruppe af $(G,\star)$.

●●● **Opgave 11.57:**
Lad os betragte D_8.

1) Vis at $\langle r^2 \rangle$ er en normal undergruppe af D_8. Husk både at argumentere for at det er en undergruppe og for at den er normal.

2) Vis at $\langle r^3 \rangle$ ikke er en normal undergruppe.

●● **Opgave 11.58:**
Vis at i en abelsk gruppe er alle undergrupper normale.

12 Hints til opgaverne

11.7

Se hvad der sker når vi ganger de to elementer sammen.

11.8

Brug bemærkning 2.18.

11.10

Du skal både vise at hvis ordnen er 1 eller 2 så vil $x^2 = 1$ og også vise at hvis $x^2 = 1$ så vil ordnen være 1 eller 2.

11.17

Brug Korollar 3.5.

11.21

Brug Korollar 3.5 til at liste alle elementerne.

11.25

Skriv a og b op som udtryk af n og r_1 samt n og r_2.

11.28

Husk formlen for hvad det vil sige at gå op i.

11.30

Kig på Eksempel 4.12 vedrørende $(\{[1]_4,...,[3]_4\}, \cdot)$.

11.34

Kig på opgave 11.32.

11.35

Til 1): Hvilke restklasser er lig $[15]_7$? Er der en af dem som gør det nemmere for os at se det vi ønsker?

11.36

Altså hvor mange elementer kan vi lave hvor vi kun bruger r og ikke s?

11.39

Du kan se at de er isomorfe ved at opskrive gruppernes gangetabeller.

11.42

Betragt ordnerne af dine elementer og brug det som inspiration til at definere en isomorfi.

11.47

- Til at omskrive til cykelform kan man med fordel læse gennem Eksempel 8.6, og teksten efter Definition 8.7.
- Til 2) brug Sætning 8.5 hvor der bliver beskrevet hvordan man let konstruerer inverser til permutationer på denne form.

11.52

Hvilke pæne mængder kender vi som er delmængder af $\mathbb{R}$? Der er to af de grupper vi har snakket om allerede helt i begyndelsen, som er undergrupper af $\mathbb{R}$.

11.53

Brug undergruppekriteriet, Sætning 9.9.

11.54

Kig på elementerne $x, x^2, x^3, \ldots$ for ethvert vilkårligt x i H.

13 Projekt: To kompositionsregler samtidig

I dette notesæt, har vi beskæftiget os med grupper. I en gruppe er der kun én kompositionsregel. På flere af de mængder, vi har set på indtil videre, er der faktisk to operationer, men vi har hver gang blot valgt af se bort fra den ene. På heltallene $\mathbb{Z}$ er der to operationer, addition og multiplikation. Du ved nu, at $(\mathbb{Z},+)$ er det vi kalder en abelsk gruppe, og at operationen multiplikation er associativ. Hvis vi tager tre heltal a,b,c så respekterer operationerne addition og multiplikation hinanden i den forstand, at

$$a(b+c) = ab + ac$$
$$(a+b)c = ac + bc.$$

Du har måske hørt, at man siger vi kan *distribuere* faktorerne over ledene - og vi kalder denne egenskab for den *distributive lov*.

Historisk var heltallene $\mathbb{Z}$ inspirationen til det, vi kalder for *ringe*, og det var ud fra dem man senere begyndte at kigge på grupper. I dette projekt skal vi se nærmere på, hvad en ring er.

Som du måske allerede har bemærket, så piller vi matematikere gerne så meget ekstra struktur væk som muligt, når vi skal definere nye koncepter. Den generelle definition af en ring overtager derfor ikke alle de fine egenskaber fra heltallene.

Definition 13.1 (Ring)**.** En mængde R udstyret med to kompositionsregler $+$ og $\times$ er en ring, hvis

- $(R,+)$ er en abelsk gruppe,
- operationen $\times$ er associativ,

- den distributive lov gælder i R.

Opgave 13.1:
Opskriv de regneregler som begreberne i definitionen af en ring dækker over.

Vi kalder inspireret af $\mathbb{Z}$ gerne operationen $+$ for addition og $\times$ for multiplikation. I en del tilfælde er der lidt ekstra struktur.

Definition 13.2 (Ring med enhed)**.** En ring R er en *ring med enhed* (en *ring med* 1), hvis der findes et neutralelement i R mht. $\times$, dvs. der skal findes et element 1 i R, så $1 \times r = r \times 1$ for alle r i R.

Det kan også ske, men er ikke påkrævet, at multiplikation i ringen er kommutativ.

Definition 13.3 (Kommutativ ring)**.** Hvis R er en ring, hvor operationen $\times$ er kommutativ, dvs. $a \times b = b \times a$, da kalder vi R for en *kommutativ ring*.

Opgave 13.2:
(Talringe). Redegør kort for, at hver af mængderne $\mathbb{Z}$, $\mathbb{Q}$ og $\mathbb{R}$ med de sædvanlige operationer $+$ som addition og $\cdot$ som multiplikation er en kommutativ ring med enhed.

Så der findes altså ringe. Du kender fra dette forløb også andre ringe.

Eksempel 13.4 (Restklasseringene)**.** For alle naturlige tal $n \geq 2$ er $\mathbb{Z}/n\mathbb{Z}$ udstyret med addition modulo n som addition og multiplikation modulo n som multiplikation en kommutativ ring med enhed. ∘

Eksempel 13.5 (Den trivielle ring)**.** Mængden $\{0\} \subseteq \mathbb{Z}$ udstyret med addition fra $\mathbb{Z}$ som addition samt multiplikation fra $\mathbb{Z}$ som multiplikation er en ring med enhed. ∘

Opgave 13.3:
Antag, at R er en ring uden enhed. Tag et element r i R. Findes der en invers til r med hensyn til multiplikation?

Selv hvis R er en ring med enhed, behøver et element r i R ikke at have en multiplikativ invers. Når man tjekker for, om et element er en multiplikativ invers, er det nødvendigt at gøre det fra begge sider.

Definition 13.6 (Multiplikativ invers)**.** Lad R være en ring med enhed, og lad r være et element i R. Da er et element a en multiplikativ invers til r, hvis $a \times r = r \times a = 1$.

Men hvis R er en kommutativ ring, kan vi gøre helt som vi plejer i grupper:
Opgave 13.4:
Lad R være en kommutativ ring med enhed, og lad r og a være elementer i R. Antag $r \times a = 1$. Vis at a er multiplikativ invers til r.

På samme måde kan dette vises under antagelsen $a \times r = 1$, så det er nok i en kommutativ ring med enhed at gange sammen fra én side, når man tjekker om et element er en multiplikativ invers. Du har nu arbejdet med grupper, hvor alle elementer er invertible. Man kan nemt ved et uheld når man arbejder i en ring, komme til at antage, at et element r har en multiplikativ invers r^{-1}. Det er rigtig vigtigt at huske at dette ikke altid er tilfældet. I en ring kan det forekomme at ingen eller kun få elementer har en multiplikativ invers. Det er $\mathbb{Z}$ du skal have i tankerne (men glem at multiplikation er kommutativ), når du tænker på en ring. I ringen $\mathbb{Z}$ har stort set ingen elementer en multiplikativ invers.
Opgave 13.5:
Vis at elementerne 1 og -1 i $\mathbb{Z}$ begge har en multiplikativ invers. Findes der andre elementer i $\mathbb{Z}$ med multiplikativ invers?

Bemærkning 13.7. Ligesom i grupper vil vi nu benytte den multiplikative skrivemåde, når vi arbejder med ringe og skrive ab i stedet for $a \times b$.

Vi er nu klar til at udlede nogle generelle egenskaber for ringe ligesom vi startede med at gøre for grupper.

Opgave 13.6:
(Entydighed af multiplikativ neutralelement). Lad R være en ring med enhed. Vis at enhedet er entydigt.

Opgave 13.7:
(Entydighed af multiplikativ invers). Lad R være en ring med enhed. Antag at der findes en multiplikativ invers til et element r i R. Vis at denne invers er entydig.

Bemærkning 13.8. I en ring med enhed kalder vi derfor neutralelementet med hensyn til multiplikation for enheden og skriver 1, og hvis et element r har en invers, betegner vi den inverse r^{-1}.

En del af de sædvanlige regneregler fra $\mathbb{Z}$ gælder også i en ring.

Opgave 13.8:
Lad R være en ring med enhed.

1) Vis at $0a = a0 = 0$.

2) Vis, at $-a = (-1)a = a(-1)$ (den additive inverse til a er lig med $(-1)a$.

3) Vis, at $(-a)b = a(-b) = ab$.

4) Vis, at $(-1)(-1) = 1$ og konkluder $(-a)(-b) = ab$.

5) Lad n være et naturligt tal. Overbevis dig selv om at $(na)b = a(nb) = n(ab)$, hvor

$$nr = \underbrace{r + ... + r}_{n \text{ gange}}.$$

Det er ret svært at lave et rigtigt matematisk bevis for dette.

Du har nu igennem din skoletid nok mange gange hørt at det ikke er muligt at dividerer med nul. Selvom det at være i stand til at dividere med 0, måske lyder som en spændende mulighed, så bliver ringen meget kedelig, hvis det er muligt.

Opgave 13.9:
Lad R være en ring med enhed, hvor elementet 0^{-1} findes.

1) Vis at i R er $0 = 1$.

2) Konkluder at det for alle r i R gælder at $r = 0$, så $R = \{0\}$.

Når man arbejder i en ring, skal man passe på med at bruge sin intuition fra $\mathbb{Z}$ for meget.

Opgave 13.10:
Betragt ringen $\mathbb{Z}/6\mathbb{Z}$.

1) Opskriv gangetabellen for $\mathbb{Z}/6\mathbb{Z}$.

2) Sammenlignet med multiplikation i $\mathbb{Z}$, er der da noget anderledes ved multiplikation i $\mathbb{Z}/6\mathbb{Z}$?

Definition 13.9 (Nuldivisorer)**.** Lad R være en ring. Da kalder vi ringelementer a og b for *nulkdivisorer*, hvis både $a \neq 0$ og $b \neq 0$, men $ab = 0$.

Opgave 13.11:
Lad R være en ring med enhed. Vis, at hvis et element r i R har en multiplikativ invers, da er r ikke en nuldivisor.

Hvis man arbejder med en ring som indeholder nuldivisorer, da gælder den velkendte forkortningsregel fra $\mathbb{Z}$ om at hvis $ca = cb$ da er $a = b$ eller $c = 0$ ikke længere. I et specialtilfælde gælder den dog stadig.

Opgave 13.12:
Vis at hvis c er invertibel, og $ca = cb$, da er $a = b$.

Definition 13.10 (Integritetsområde)**.** Lad R være en kommutativ ring med enhed (som ikke er den trivielle ring). Da siger vi at R er et *integritetsområde*, hvis R ikke indeholder nuldivisorer.

Det rare ved et integritetsområde er, at vi i højere grad kan bruge vores intuition fra $\mathbb{Z}$, når vi regner.

Opgave 13.13:
Lad R være et integitetsomårde. Vis at forkortningsreglen gælder, dvs. at $ca = cb$ er enbetydende med at $a = b$ eller $c = 0$.

Hints til 'To kompositionsregler samtidig'

13.1

Se på definitionen af en gruppe, og af at være abelsk.

13.2

Udnyt listen fra den forrige opgave. Gælder disse regneregler i de nævnte talmængder?

13.3

Hvad kræves af en invers? Kan dette opfyldes i R?

13.4

Hvad betyder det, at R er kommutativ?

13.5

Udregn 1^2 og $(-1)^2$. Hvad kan du komkludere? Tag et heltal a som ikke er 1 eller -1. Er a^{-1} indeholdt i $\mathbb{Z}$?

13.6

Søg inspiration i beviset for entydighed af neutralelementer i grupper.

13.7

Søg inspiration i beviset for entydighed af inverse elementer i grupper.

13.8

1) Det gælder, at $0 + 0 = 0$ (hvorfor?). Multiplicer med a på begge sider af lighedstegnet. På venstresiden kan det gøres fra to retninger.

2) Udnyt, at $1 + (-1) = 0$.

3) Brug forrige opgave til første lighed. Til anden lighed, regn videre på udtrykket $ab + a(-b)$ og vis, at det er lig med 0.

4) Udnyt, at $1 + (-1) = 0$ og brug forrige opgave.

5) Husk vi har den distributive lov, og at $+$ operationen er kommutativ.

13.9

1) Udregn 0×0^{-1} på to forskellige måder. Hvad er $r \times 0$ og hvad er $r \times r^{-1}$. 2: Det gælder at $r = r \times 1$. Brug forrige spørgsmål.

13.10

2) Hvornår er $ab = 0$ i $\mathbb{Z}$?

13.11

Hvis r er invertibel, er $1 = rr^{-1}$. Hvis r er en nuldivisor, findes $a \neq 0$ så $0 = ar$. Find en modstrid.

13.12

Kan vi finde et smart element at gange med på begge sider af lighedstegnet?

13.13

Vis, at $ca = cb$ er ensbetydende med $c(a - b) = 0$. Udnyt så, at R er et integritetsområde.

14 Projekt: Nye grupper fra gamle

Dette projekt handler om måder, hvorpå vi kan skabe nye grupper ud fra grupper, man kender i forvejen. I ved i forvejen at hvis vi tager et element i en gruppe, kan vi kigge på undergruppen frembragt af elementet, og det vil give os en gruppe der maksimalt er lige så stor som den gruppe vi startede med. Vi vil i dette projekt kigge på en måde hvor vi kan lave nye og større grupper.

Det vi skal betragte er direkte produkter.

Direkte produkter

Definition 14.1. Lad G og H være grupper. Mængden

$$G \times H = \{(g,h) | g \text{ er et element i } G, h \text{ er et element i } H\}$$

kaldes produktmængden af G og H.

Grunden til at denne mængde er interessant for os er, at den kan gøres til en gruppe.

Sætning 14.2. Hvis G og H er grupper, da er $G \times H$ udstyret med kompositionen $(g,h) \cdot (g',h') = (gg',hh')$ en gruppe.

Bemærkning 14.3. Udtrykket (gg',hh') ovenfor skal forstås således, at gg' er kompositionen af g og g' i G og hh' er kompositionen af h og h' i H.

Opgave 14.1:
Bevis at det direkte produkt af grupperne G og H er en gruppe.

Opgave 14.2:
Antag at G og H er grupper af endelig orden. Hvilken orden har gruppen $G \times H$?

Opgave 14.3:
Betragt det direkte produkt $G_1 \times G_2$.
1) Antag, at $H_1 \leq G_1$ og $H_2 \leq G_2$. Vis at $H_1 \times H_2 \leq G_1 \times G_2$.

2) Antag, at $H_1 \trianglelefteq G_1$ og $H_2 \trianglelefteq G_2$. Vis at $H_1 \times H_2 \trianglelefteq G_1 \times G_2$.

Det gør ingen forskel i hvilken rækkefølge grupperne i det direkte produkt optræder.
Opgave 14.4:
Lad G og H være grupper. Vis at $G \times H$ er isomorf til $H \times G$.

Vi behøver ikke begrænse os til to grupper:

Sætning 14.4 (Direkte produkt, flere faktorer)**.**
Hvis $G_1, G_2, \ldots, G_n$ er grupper, da er $G_1 \times G_2 \times \cdots \times G_n$ udstyret med kompositionsreglen

$$(g_1, g_2, \ldots, g_n) \cdot (g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n')$$

en gruppe.

Opgave 14.5:
Inden du fortsætter, så overbevis dig selv om, at resultaterne fra de første 4 opgaver kan generaliseres til denne situation.

Opgave 14.6:
Lad $(x_1, \ldots, x_n)$ være et element i $G_1 \times \cdots \times G_n$. Argumenter for, at $|(x_1, \ldots, x_n)| = \text{mfm}\{|x_1|, \ldots, |x_n|\}$ hvor mfm er mindste fælles multiplum, altså det mindste tal som alle $|x_i|$'erne går op i.

Visse egenskaber overføres til det direkte produkt.
Opgave 14.7:
Vis at $G_1 \times \cdots \times G_n$ er abelsk hvis og kun hvis G_i er abelsk for alle $1 \leq i \leq n$.

Når vi ved dette kunne vi måske foranlediges til at tro at $G_1 \times G_2$ er cyklisk hvis G_1 og G_2 er det, men det er ikke altid tilfældet.

Opgave 14.8:

Lad os vise at $Z_2 \times Z_2$ ikke er cyklisk.

1) Antag at $Z_2 \times Z_2$ er cyklisk. I så fald findes en frembringer a for $Z_2 \times Z_2$. Hvilken orden har a?

2) Hvilken orden har elementerne i $Z_2 \times Z_2$?

3) Argumenter for, at $Z_2 \times Z_2$ ikke er cyklisk.

Det direkte produkt af to cykliske grupper kan dog godt være cyklisk.

Opgave 14.9:

Hvis sfd$(m,n) = 1$ (hvis m og n ikke har nogle divisorer til fælles), da er $Z_{nm} \cong Z_n \times Z_m$. Det vil vi vise nu.

1) Husk at, eller overbevis dig selv om, at for alle naturlige tal n og m, er

$$\text{mfm}(m,n) = \frac{mn}{\text{sfd}(m,n)}.$$

Konkluder at mfm$(m,n) = mn$ hvis og kun hvis sfd$(m,n) = 1$, og at mfm$(m,n) < mn$ hvis sfd$(m,n) \neq 1$.

Lad $k = \text{mfm}(m,n)$. Lad envidere $Z_m = \langle x \rangle$ og $Z_n = \langle y \rangle$, dvs x er frembringer for Z_m og y er frembrigner for Z_n.

2) Antag først at sfd$(m,n) \neq 1$ og betragt gruppen $Z_m \times Z_n$. Lad (x^a,y^b) være et element i $Z_m \times Z_n$ og vis at $|(x^a,y^b)| < mn$. Konkluder at $Z_m \times Z_n$ ikke er isomorf til Z_{mn}.

3) Antag nu i stedet at sfd$(m,n) = 1$. Vis at $\langle (x,y) \rangle = Z_m \times Z_n$. Konkluder at $Z_m \times Z_n \cong Z_{mn}$.

Hints til 'Nye grupper fra gamle'

14.1

Vis at alle gruppeaxiomerne er opfyldt.

14.2

Elementerne i $G \times H$ består af alle mulige par (g,h) hvor $g \in G$ og $h \in H$.

14.4

Hvilken afbildning mellem $G \times H$ og $H \times G$ kunne være naturlig at bruge? Vis så, at denne afbildning er en homomorfi og bijektiv.

14.6

Er det muligt, at $(x_1, x_2, \ldots, x_n)^k = e$ for $k < \text{mfm}\{|x_1|, \ldots, |x_n|\}$?

14.7

$(x_1, \ldots, x_n) = (x_1', \ldots, x_n')$ hvis og kun hvis $x_i = x_i'$ for alle $1 \leq i \leq n$.

14.8

1) Brug Sætning 6.9.

2) Tag $(a,b) \in Z_2 \times Z_2$ og beregn $2(a,b)$ - ellers opskriv gangetabellen.

14.9

1) Hvilke værdier kan sfd(m,n) antage?

2) Brug potensreglerne og opgave 14.4 til at beregne $(x^a,y^b)^k$. Konkluder at $|(x^a,y^b)| < mn$ ved hjælp af første spørgsmål. Hvad er den højeste orden af et element i Z_{mn} kan have?

3) $\langle(x,y)\rangle \leq Z_m \times Z_n$ jævnfør 11.53. Hvilken orden har $\langle(x,y)\rangle$ og $Z_m \times Z_n$? Brug Opgave 11.44 der siger at cykliske grupper af samme orden er isomorfe.

15 Projekt: Multiplikative restklassegrupper

I dette projekt vil vi arbejde os frem til at kunne vise at $(\{[1]_p, [2]_p, \ldots, [p-1]_p\}, \cdot)$ er en gruppe, når p er et primtal, og vil i den forbindelse introducere en del teori, som høre til området af matematikken vi kalder talteori.

Det kan være en god ide at starte med at genlæse Proposition 4.10 og beviset.

Den største fælled divisor bliver vigtig for os, så lad os betragte den.

Definition 15.1. Lad a og b være heltal. Den *største fælles divisor* af a og b er et positivt heltal d, så $d \mid a$, $d \mid b$ og hvis et andet heltal k opfylder $k \mid a$ og $k \mid b$, da vil $k \mid d$. Vi betegner den største fælles divisor med $\text{sfd}(a, b)$.

Lad os starte med et eksempel:

Eksempel 15.2. Vi ønsker at finde $\text{sfd}(10, 25)$. Divisorerne for 10 er $\pm 1, \pm 2, \pm 5$ og ± 10. Divisorerne for 25 er $\pm 1, \pm 5$ og ± 25. Man kan f.eks. se dette ved at primtalsfaktorisere 10 og 25. Vi ser, at den største fælles divisor er 5. ∘

- **Opgave 15.1:**
  Udregn:

  1) $\text{sfd}(11, 66)$

  2) $\text{sfd}(36, 124)$

  3) $\text{sfd}(2003, 10015)$ [Vink: 2003 er et primtal]

Bemærkning 15.3. Vi bemærker en ting ved definitionen. Der står *den* største fælles divisor, hvilket antyder, at den er unik. Dette er tilfældet

●● **Opgave 15.2:**
Bevis, at hvis d_1 og d_2 begge er største fælles divisorer for a og b, da vil $d_1 = d_2$.

Følgende lemma viser faktisk, at vi helt kan se bort fra fortegn, når vi skal udregne den største fælles divisor af to heltal:

Lemma 15.4. For to heltal a og b gælder:

$$\text{sfd}(a, b) = \text{sfd}(-a, b) = \text{sfd}(a, -b) = \text{sfd}(-a, -b).$$

Bevis. Vi nøjes med at bevise $\text{sfd}(a, b) = \text{sfd}(-a, b)$. De andre ligheder vises på samme måde. Lad $d_1 = \text{sfd}(a, b)$ og $d_2 = \text{sfd}(-a, b)$. d_1 deler både $-a$ og b, så $d_1 \mid d_2$, da d_2 er største fælles divisor for $-a$ og b. d_2 deler dog også både a og b, så $d_2 \mid d_1$. Da både d_1 og d_2 er positive, må $d_1 = d_2$ som ønsket. □

Opgave 15.3:
Udregn sfd(−22,49).

Når to har har største fælles divisor lig 1, har det sit eget navn:

Definition 15.5. To heltal a og b kaldes *indbyrdes primiske*, hvis deres største fælles divisor er 1, altså hvis $\text{sfd}(a, b) = 1$.

Det er ikke svært at se, at vores metode med at finde samtlige divisorer i to tal og derefter udvælge den største, er ret upraktisk for store tal. Vi skal nu udvikle en smart metode til at udregne den største fælles divisor, og her kommer Euklids algoritme ind i billedet.

Hele algoritmen bygger på den centrale betragtning, at hvis vi skriver $a = bq + r$, da vil $\text{sfd}(a, b) = \text{sfd}(b, r)$. Lad os vise dette:

Lemma 15.6. For heltal a og b gælder, at hvis $a = qb + r$ for heltal q og r, da vil $\text{sfd}(a, b) = \text{sfd}(b, r)$.

Bevis. Lad $d_1 = \text{sfd}(a, b)$ og $d_2 = \text{sfd}(b, r)$. Det er nok at vise, at $d_1 \mid d_2$ og $d_2 \mid d_1$, idet begge tal er positive. d_1 deler både a og b, så d_1 deler også r, da $r = a - qb$. Dermed deler d_1 både b og r. Da d_2 er den største fælles divisor for b og r, vil $d_1 \mid d_2$. Da d_2 deler r og b, vil d_2 også dele $a = qb + r$. Men da har vi også $d_2 \mid d_1$, hvilket fuldfører beviset. □

Definition 15.7 (Euklids algoritme)**.** Lad heltallene a og b være givet. Per lemma 15.4 kan vi antage, at hverken a eller b er negative. Af hensyn til notation omdøber vi $a = r_0$ og $b = r_1$. Skriv $r_0 = q_1 r_1 + r_2$ med $0 \leq r_2 < r_1$. Gentag på følgende måde:

$$r_0 = q_1 r_1 + r_2 \quad \text{hvor } 0 \leq r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3 \quad \text{hvor } 0 \leq r_3 < r_2$$

$$\ldots$$

$$r_{n-1} = q_n r_n$$

indtil resten bliver 0. Den sidste ikke-nul rest r_n er lig $\text{sfd}(r_0, r_1) = \text{sfd}(a, b)$.

Vi skal naturligvis bevise, at denne fremgangsmåde er korrekt. Først er det dog på sin plads med et eksempel.

Eksempel 15.8. Vi ønsker at finde sfd(1957, 446). Vi følger proceduren ovenover:

$$\begin{aligned}
1957 &= 4 \cdot 446 + 173 \\
446 &= 2 \cdot 173 + 100 \\
173 &= 1 \cdot 100 + 73 \\
100 &= 1 \cdot 73 + 27 \\
73 &= 2 \cdot 27 + 19 \\
27 &= 1 \cdot 19 + 8 \\
19 &= 2 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Det ses, at den sidste rest forskellig fra 0 er 1. Dermed er sfd(1957, 446) = 1. ∘

Opgave 15.4:
Hvad kan vi nu sige om 1957 og 446?

- **Opgave 15.5:**
  Brug Euklids algoritme til at udregne:

  1) sfd(245, 135)

  2) sfd(−714, −356)

  3) sfd(5139, −481)

Sætning 15.9 (Korrekthed af Euklids algoritme)**.** Euklids algoritme anvendt på to ikke-negative heltal a og b giver den største fælles divisor sfd(a, b).

Bevis. Lad os først vise, at algoritmen faktisk terminerer (slutter). Når vi laver den beskrevne procedure, får vi en række rester $r_0, r_1, r_2, ...$ Disse rester er alle større end eller

lig 0, og vi har $r_0 > r_1 > r_2 > ....$ En vilkårlig rest bliver altså skarpt mindre end den forrige rest i hvert trin. Da de alle er ikke-negative, må proceduren stoppe på et tidspunkt, nemlig når resten bliver 0.

Algoritmen returnerer altså altid et output, nemlig r_n. Vi skal blot vise, at $r_n = \text{sfd}(a, b)$. Dette følger ved blot at benytte lemma 15.6 på hver opskrivning i algoritmen. Vi har nemlig

$$\begin{aligned}\text{sfd}(a, b) &= \text{sfd}(b, r_2) = \text{sfd}(r_2, r_3) = ... = \text{sfd}(r_n, r_{n+1}) \\ &= \text{sfd}(r_n, 0) = r_n,\end{aligned}$$

som ønsket. □

Bemærkning 15.10. At bevise korrekthed af en algoritme i datalogi eller matematik involverer altid at vise, at algoritmen slutter, og at algoritmen altid returnerer det korrekte output.

●● **Opgave 15.6:**
Lad p og q være forskellige primtal. Hvad er $\text{sfd}(p, q)$?

Vi er nu klar til at lære Bézouts lemma. Du kan bare springe beviset over, men vi har taget det med i tilfælde af nogen er interesseret.

Sætning 15.11 (Bézouts lemma)**.** Lad $d = \text{sfd}(a, b)$ for to heltal a og b ikke begge lig 0. Da eksisterer der hele tal x og y, så

$$d = ax + by.$$

Bevis. Vi starter med at bemærke, at sætningen oplagt gælder, hvis $a = 0$ eller $b = 0$. Lad os opskrive trinene i Euklids

algoritme på $a = r_0$ og $b = r_1$:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\ldots \\ r_i &= q_{i+1} r_{i+1} + r_{i+2} \\ &\ldots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \\ r_{n-1} &= q_n r_n. \end{aligned}$$

Beviset fungerer ved at trævle algoritmen op bagfra. Vi viser mere generelt, at hvis man har to rester r_{i-1} og r_i lige efter hinanden, da findes hele tal x_{i-1} og y_i, så $d = r_{i-1}x_{i-1} + r_i y_i$. Dette vil bevise det ønskede, da tilfældet $i = 1$ svarer til $d = ax + by$ hvor $x = x_0$ og $y = y_1$. Vi ved, at $d = r_n$, så fra det næstsidste trin i algoritmen fås $d = r_{n-2} + (-q_{n-1})r_{n-1}$. Altså er påstanden vist for det næstsidste trin. For det tredjesidste trin har vi:

$$r_{n-3} = q_{n-2} r_{n-2} + r_{n-1}.$$

Ved omrokering fås altså:

$$r_{n-1} = r_{n-3} - q_{n-2} r_{n-2}.$$

Indsættes dette i vores udtryk for d fra før fås:

$$\begin{aligned} d &= r_{n-2} + (-q_{n-1})(r_{n-3} - q_{n-2} r_{n-2}) \\ &= (-q_{n-1}) r_{n-3} + r_{n-2} + q_{n-1} q_{n-2} r_{n-2} \\ &= (-q_{n-1}) r_{n-3} + (1 + q_{n-1} q_{n-2}) r_{n-2}. \end{aligned}$$

Igen er d opskrevet på den ønskede form, men nu indgår der rester fra ét trin længere tilbage. Mere præcist ses det, at hvis $d = r_{i-1}x_{i-1} + r_i y_i$, hvor x_{i-1} og y_i allerede er kendt, da

kan man udtrykke d ud fra de foregående rester som

$$\begin{aligned} d &= r_{i-1}x_{i-1} + (r_{i-2} - q_{i-1}r_{i-1})y_i \\ &= r_{i-1}x_{i-1} + r_{i-2}y_i - q_{i-1}r_{i-1}y_i \\ &= y_i r_{i-2} + (x_{i-1} - y_i q_{i-1})r_{i-1}. \end{aligned}$$

Vi ved, at d kan opskrives ud fra tidligere rester i næstsidste og tredjesidste trin. Ligningerne ovenover giver en (endelig) procedure, vi kan følge for at komme tilbage til at opskrive d ud fra $r_0 = a$ og $r_1 = b$. Dette beviser sætningen. □

●● **Opgave 15.7:**
Lad a og b være heltal.

1) Vis, at hvis a og b er indbyrdes primiske, så findes heltal x og y, så $1 = ax + by$.

2) Antag nu omvendt, at der findes heltal x og y, så $1 = ax + by$. Vis, at $\text{sfd}(a, b) = 1$.

Vi har altså vist, a og b er indbyrdes primiske hvis og kun hvis der findes heltal x, y, så $1 = ax + by$.

Eksempel 15.12. Lad os finde en heltalsløsning (x, y) til ligningen $885x+360y = \text{sfd}(885, 360)$. Først bruger vi Euklids algoritme til at udregne $\text{sfd}(885, 360)$:

$$\begin{aligned} 885 &= 2 \cdot 360 + 165 \\ 360 &= 2 \cdot 165 + 30 \\ 165 &= 5 \cdot 30 + 15 \\ 30 &= 2 \cdot 15. \end{aligned}$$

Så $\text{sfd}(885, 360) = 15$. Vi trævler algoritmen op baglæns,

indtil vi finder heltallene x og y:

$$\begin{aligned}15 &= 165 - 5 \cdot 30 = 165 - 5 \cdot (360 - 2 \cdot 165) \\ &= 165 - 5 \cdot 360 + 10 \cdot 165 = -5 \cdot 360 + 11 \cdot 165 \\ &= -5 \cdot 360 + 11 \cdot (885 - 2 \cdot 360) \\ &= -5 \cdot 360 + 11 \cdot 885 - 22 \cdot 360 = -27 \cdot 360 + 11 \cdot 885.\end{aligned}$$

Vi aflæser, at en løsning er $(x, y) = (11, -27)$. At lave baglæns substitution kan være svært i starten, men tricket er at genkende resten i ligningerne og isolere den som udtryk af de to større rester, indtil man når til de to oprindelige tal (her var de 885 og 360). ∘

Lad os opsummere fremgangsmåden ovenover, da den er vigtig i mange sammenhænge:

Definition 15.13 (Baglæns euklidisk algoritme)**.** Vi ønsker at finde en heltalsløsning (x, y) til ligningen $\text{sfd}(a, b) = ax + by$, hvor a og b er heltal ikke begge lig 0. Først anvendes Euklids algoritme som sædvanligt for at finde $\text{sfd}(a, b)$:

$$\begin{aligned}r_0 &= q_1 r_1 + r_2 \quad \text{hvor } 0 \leq r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3 \quad \text{hvor } 0 \leq r_3 < r_2 \\ &\ldots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \\ r_{n-1} &= q_n r_n,\end{aligned}$$

hvor vi har omdøbt $a = r_0$ og $b = r_1$. Vi ved, at $r_n = \text{sfd}(a, b)$, og vi kan løse for $\text{sfd}(a, b)$ i den næstsidste ligning og få:

$$\text{sfd}(a, b) = r_{n-2} - q_{n-1} r_{n-1}.$$

Ligeledes kan vi løse for r_{n-1} ved at se på ligningen før:

$$r_{n-1} = r_{n-3} - q_{n-2} r_{n-2}.$$

Indsæt udtrykket for r_{n-1} i udtrykket for $\text{sfd}(a,b)$ i ligningen ovenover. På den måde har vi udtrykt $\text{sfd}(a,b)$ ud fra resterne r_{n-2} og r_{n-3}. Dette gentages, indtil man har udtrykt $\text{sfd}(a,b)$ ud fra et tal gange a plus et tal ganget b. Tallet ganget på a er vores x, og tallet ganget på b er vores y, og løsningen er fundet.

- **Opgave 15.8:**
  Find en heltalsløsning (x,y) til ligningen $245x + 135y = \text{sfd}(245,135)$.

Nu da vi har Bezouts lemma, er vi klar til at vise den sidste del af Proposition 4.10. Lad os bare state den del af sætningen vi mangler af vise her.

Proposition 15.14. $(\{[1]_p,\ldots,[p-1]_p\},\cdot)$ er en gruppe hvis p er et primtal.

Opgave 15.9:
Overbevis dig selv om at $\text{sfd}(a,p) = 1$ når p er et primtal, og $0 < a < p$.

Bevis. Givet et primtal p lad os betragte $(\{[1]_p,\ldots,[p-1]_p\},\cdot)$.

Den associative lov gælder, idet

$$([a]_p[b]_p)[c]_p = [abc]_p = [a]_p([b]_p[c]_p).$$

Vi har også $[1]_p$ som neutralelement, idet $[a]_p[1]_p = [1]_p[a]_p = [a]_p$.

At tjekke af vi har inverser er der hvor det bliver sværere, og hvor vi får brug for alt det arbejde vi har lavet i projektet.

Betragt et element $[a]_p$ i $\{[1]_p,\ldots,[p-1]_p\}$, hvor a er den repræsentant der ligger mellem 0 og p, altså $0 < a < p$. Vi har at $\text{sfd}(a,p) = 1$, fra opgave 15.9, og ved at bruge Bézouts lemma, får vi at der eksistere x og y så

$$\text{sfd}(a,p) = 1 = ax + py.$$

Betragter vi dette modulo p får vi nu at $1 \equiv ax + py \equiv ax$, så $[a]_p[x]_p = [1]_p$, så $[a]_p^{-1} = [x]_p$ er en invers til $[a]_p$ i $(\{[1]_p, \ldots, [p-1]_p\}, \cdot)$. □

●● **Opgave 15.10:**
Lad a og b være heltal og $c = \frac{a}{\text{sfd}(a,b)}$ og $d = \frac{b}{\text{sfd}(a,b)}$. Vis, at $\text{sfd}(c,d) = 1$.

●● **Opgave 15.11:**
En anvendelse af største fælles divisorer er i at forkorte brøker. En brøk a/b siges at være *uforkortelig* eller *reduceret*, hvis $\text{sfd}(a,b) = 1$. F.eks. er $1/7$ uforkortelig, mens $10/70$ ikke er det.

1) Omskriv $185/490$ til en uforkortelig brøk.

2) Omskriv $1244/2588$ til en uforkortelig brøk.

3) Vis, at $661/789$ er en uforkortelig brøk.

Hints til 'Multiplikative restklassegrupper'

15.1

Du kan søge inspiration i eksemplet.

15.2

Lad dig inspirere af beviset for lemmaet lige nedenfor.

15.3

Brug Lemma 15.4.

15.4

Se Definition 15.5.

15.5

Søg inspiration i Eksempel 15.8.

15.6

Hvilke tal findes der, som går op i både p og q?

15.7

Brug Bézouts lemma.

15.8

Brug Euklids algoritme baglæns.

15.9

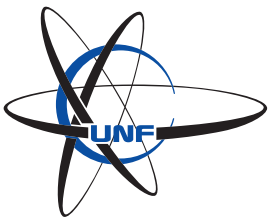
Hvilke tal går både op i p og a.

15.10

Brug Bézouts lemma og opgave 15.7 1).

15.11

Per opgave 15.10 skal vi blot dividere ud med den største fælles divisor i tæller og nævner.



3 Knudeteori

1 Introduktion

Knudeteori er en gren af algebraisk topologi, som beskæftiger sig med det såkaldte 'placement problem', som stiller spørgsmålet om, hvornår to topologiske rum ligger "inde i hinanden". Den matematiske teori om knuder blev for første gang beskrevet i 1771 af Alexandre Théophile Vandermonde og sidenhen glemt indtil 100 år senere, hvor blandt andet Gauß, Lord Kelvin og Peter Guthrie Tait byggede videre på teorierne. I dag findes utallige teorier, mængder og polynomier, der alle prøver på at forstå, hvad der gør en knude 'knudet'.

På trods af, at knudeteori er en undergren af topologi, kræver det nærmest ingen baggrundsviden at forstå emnet. Som læser vil du se, at knudeteori mest handler om at anvende mere grafiske, matematisk algoritmiske fremgangsmåder på tegninger og diagrammer.

Et andet interessant faktum er, at man i knudeteori i langt de fleste tilfælde arbejder via den deduktive metode. Dette betyder, at vi, i stedet for at observere specifikke egenskaber og beskrive dem med matematik, vælger at udlede lovene og teste disse på individuelle knuder. Det eneste problem er, at vi nærmest ingenting ved om knuder. Hvornår er en knude en knude? Hvordan 'udfolder' man en vilkårlig

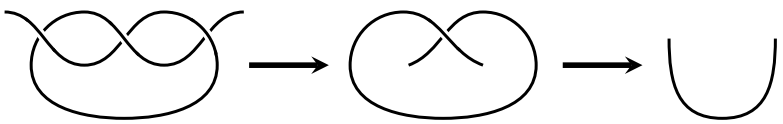
knude? Og hvordan konstruerer vi vilkårlige knuder og kæder? Den primære måde, vi takler disse problemer på, er ved at udlede såkaldte *knudeinvarianter*. En invariant er et tal, polynomium, eller et lignenede matematisk objekt, som ikke ændrer sig under visse transformationer. Med andre ord, hvis man beregner invarianterne for to knuder og får to forskellige resultater, må knuderne være forskellige.

At vise, at to knuder er forskellige, er meget nemt. Men det er meget svært at udlede, om to knuder er ens. Hvis to invarianter giver det samme resultat, kan man nemlig ikke altid med sikkerhed sige, at knuderne også må være ens. For at kunne gøre det, skal man bruge en *komplet* invariant, som har den egenskab, at den giver et forskelligt og unikt resultat for alle knuder. Sådan en invariant er dog meget svær at finde. Faktisk er det så svært, at det aldrig er blevet gjort før...

Man kan dog spørge sig selv, hvorfor studere knuder og kæder? På trods af vores meget 'indviklede' teorier om knuder, er vores behov for yderligere viden om knuder stadig stigende. Vi opdager nemlig knuder overalt i forskellige fagområder – alt fra mikrobiologi til kvantemekanik. For eksempel danner bakterier knuder i deres ringformede DNA, når de reproducerer. Dette skyldes, at de skærer DNA-molekylet midt over, når de replikerer. Bakterierne har derfor proteiner, som kan udføre "crossing switch"-operationer, som binder knuden op for at fortsætte replikeringen. Biologer arbejder derfor meget tæt sammen med matematikere for at forstå, hvordan bakterier binder knuder op. Det er nemlig lidt skræmmende at bakterier er bedre til det, end vi er.

2 Knuder og kæder

I knudeteori er en knude noget forskellig fra dem, som vi binder på vores sko. Inden for topologi er der nemlig intet begreb for 'længde'. Har man derfor en topologisk lineal, kan den udstrækkes og skrumpes til en vilkårlig længde og på samme tid bevare dens 'lineal-agtige' egenskaber. Hvis vi forestiller os et topologisk snørrebånd, kan vi derfor meget enkelt binde det op ved at forkorte båndet og bagefter trække det ud i en lige linje.



Figur 3.1: Et topologisk snørrebånd kan på enkelt vis bindes op ved at forkorte snoren.

Vi bliver derfor nødt til at definere knuder som 'snore', hvor enderne er klistret sammen. Hvis snoren forkortes, resulterer det ikke i, at knuden bindes op. Vi tilføjer derudover et par enkelte punkter for at sørge for, at vores snor opfører sig pænt.

Definition 2.1. En knude K er en lukket kurve (som vi kan betragte som en snor) i tre dimensioner, som ikke har nogen tykkelse og ikke skærer sig selv. Desuden må kurven ikke være "kantet", men skal opføre sig som en snor.

Ovenstående er en intuitiv definition. Nedenfor er den formelle definition til dem, som er interesserede.

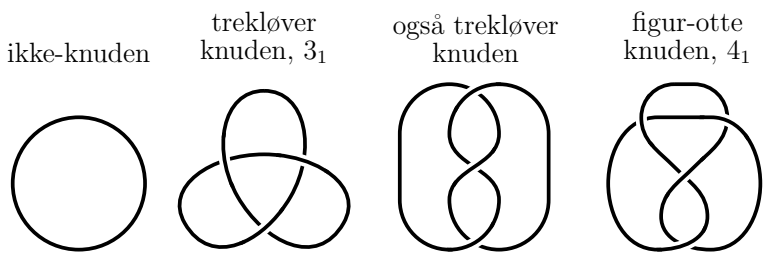
Definition 2.2. En knude $K \subseteq \mathbb{R}^3$ er en delmængde på formen $K = f(\mathbb{R})$, hvor $f : \mathbb{R} \to \mathbb{R}^3$ er en funktion med følgende egenskaber:

1. $f(t)$ er 'glat', så $\frac{\mathrm{d}^n}{\mathrm{d}t^n} f$ eksisterer for alle $n \in \mathbb{N}$.

2. $t\frac{\mathrm{d}f}{\mathrm{d}t} \neq 0$ for alle $t \in \mathbb{R} \setminus \{0\}$.

3. $f(t_1) = f(t_2)$ hvis og kun hvis $t_1 - t_2 \in \mathbb{Z}$.

Bemærkning 2.3. I realiteten vil man kun i meget få tilfælde arbejde med knuder som funktioner i $\mathbb{R}^3$, og i dette kompendium vil vi bruge Definition 2.1. Men Definition 2.2 er meget vigtig til at begrænse, hvordan vi må illustrere knuder. Punkt 1 og 2 beskriver, at knuden er 'glat', og at den ikke må indeholde 'skarpe hjørner'. Pinde limet sammen i enderne kan derfor aldrig danne en knude. Det sidste punkt beskriver, at alle knuder skal være lukkede, som vi ellers eksperimenterede med i Figur 3.1. For at forstå egenskaben skal du forestille dig, at du bevæger dig rundt på knuden i $\mathbb{R}^3$ og vælger et punkt $f(0)$. Hvis du bevæger dig en hel gang rundt om knuden, vil du nå til punktet $f(1)$. Efter to gange rundt når du til $f(2)$. Vi kan derfor sige, at $f(t) = f(t + z)$, hvor $z \in \mathbb{Z}$ er et antal gange, du bevæger dig rundt om knuden.



Figur 3.2: Eksempler på forskellige knuder.

At snoren er lukket betyder også, at der eksisterer en stor (faktisk uendelig) mængde lukkede kurver – eller knuder –

som ikke direkte kan transformeres til hinanden ved at trække i dem. Figur 3.2 viser nogle eksempler på simple knuder, som vi kommer til at arbejde med. Vi vil også arbejde med kæder af knuder, som meget belejligt kaldes kæder. Før vi kan definere en kæde, har vi brug for nogle grundlæggende definitioner.

Definition 2.4. Lad J og K være to knuder. Den *disjunkte forening* af J og K, som skrives $J \sqcup K$, svarer til foreningsmængden $J \cup K$, men hvor knuderne ikke må have nogle punkter til fælles.

Definition 2.5. En kæde[1] L er en mængde på formen

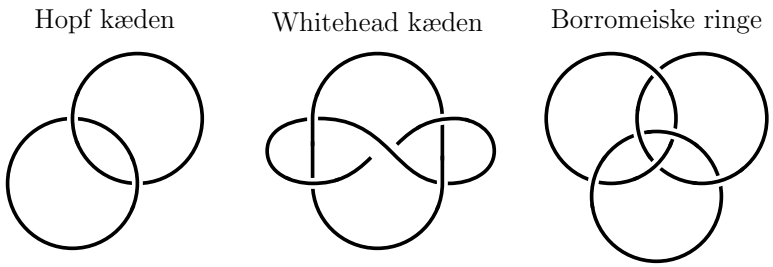
$$L = C_1 \sqcup \cdots \sqcup C_n,$$

hvor alle C_i hver især er knuder. De enkelte knuder kaldes også kædens *komponenter*.

Bemærk, at alle knuder er kæder med én komponent. Kæder er dog ikke knuder, medmindre de kun har én komponent. I dette kompendium vil vi oftest muligt prøve at skelne mellem knuder og kæder.

Figur 3.3 viser eksempler på forskellige kæder, som alle er konstrueret fra disjunkte foreninger af ikke-knuden. Det er tydeligt, at selv med få komponenter er der frihed til at konstruere uendelig mange kæder, som ikke kan omformes til hinanden ved at trække i dem. For at formalisere dette vil vi derfor gerne definere, hvad det vil sige for to knuder eller kæder at være ens.

[1] Kæder omtales med symbolet L fra det engelske ord *link*.



Figur 3.3: Forskellige kæder alle sammensat ud fra disjunkte foreninger af ikke-knuder. Bemærk, at kæder med samme komponenter og antal komponenter ikke behøver at være ækvivalente (se Definition 2.6).

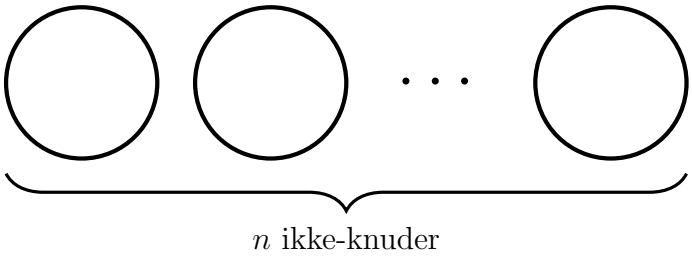
Vi holder os til en intuitiv definition af ækvivalens af kæder, da den formelle definition forudsætter ting, som I ikke har haft, og vi ikke skal bruge den ekstra information.

Definition 2.6. Kæderne L og L' er *ækvivalente*, hvilket skrives $L \simeq L'$, hvis L kan omformes til L' uden at klippe i snoren.

Bemærkning 2.7. Der gælder selvfølgelig også ækvivivalensrelationen, at hvis to kæder $L = C_1 \sqcup \cdots \sqcup C_n$ og $L' = C_1' \sqcup \cdots \sqcup C_n'$ er ækvivalente, så er $C_i \simeq C_i'$ for alle $i = 1, \ldots, n$ (under antagelse af at vi starter i samme ende af begge kæder).

Det følger også, at hvis to kæder ikke har lige mange komponenter, så kan de ikke være ækvivalente.

Definition 2.8. En knude er *triviel*, hvis den er ækvivalent med ikke-knuden. Ligeledes er en kæde *triviel med n komponenter*, hvis den er ækvivalent med følgende disjunkte forening af n ikke-knuder, hvor $n \in \mathbb{N}$.

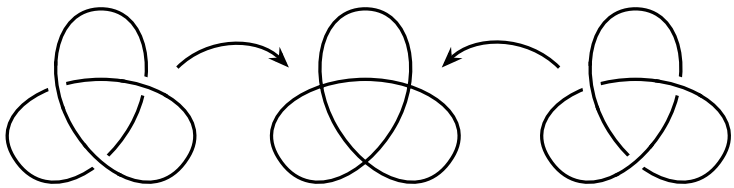


Figur 3.4: Den trivielle kæde, eller *ikke-kæden*, med n komponenter.

3 Diagrammer og Reidemeister-træk

Definition 2.6 er meget vigtig, da den fortæller os, hvornår to knuder er ens; en af de største udfordringer i knudeteori. Ligesom du kan binde snørrebånd eller slips på mange forskellige måder, så kan en knude også se ud på mange måder. Definitionen betyder også, at du ikke kan transformere knuder til hinanden ved at fx trække dem gennem den fjerde dimension eller andet snyd (som ville svare til at klippe snoren over). Til gengæld, når vi taler om knudeteori, foregår alt på et to-dimensionelt papir, og vi bliver derfor nødt til at diskutere, hvordan man må (og ikke må) tegne "diagrammer" af knuder.

Definition 3.1. Lad L være en kæde. Da er *skyggen* af L billedet, som vi får ved at projektere L ned på et vilkårligt plan. Skyggen har dog ikke informationer om, hvordan forskellige linjestykker krydser hinanden.



Figur 3.5: To forskellige knuder leder til samme skygge.

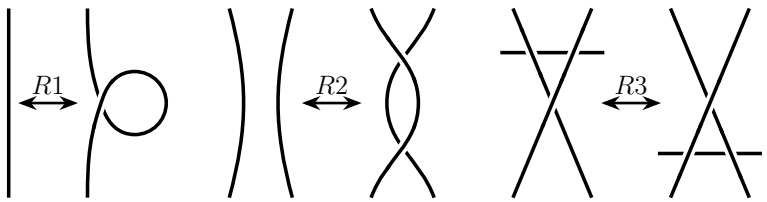
Definition 3.2. Et *diagram* D af en kæde L er en **god skygge** af L - altså en skygge, der også indeholder information om over- og underkrydsninger.

Som den skarpe læser har bemærket, illustrerer Figur 3.5, at ikke-knudens (venstre) og trekløverknudens (højre) skygger kan se ens ud. Så ved blot at vælge forskellige planer at projektere sit diagram på, kan man altså opnå, at to forskellige knuder ligner hinanden. Ligeledes kan en knude se forskellig ud alt efter hvilket perspektiv, som man kigger på den fra. Så hvordan kan vi vide, om vi kigger på den samme knude, når vi ændrer perspektiv? Kurt Reidemeister, som er en af de tidligste knudeteoretikere, udviklede i perioden 1920-1940 teorien om *Reidemeister-træk*, som forklarer, hvordan vi kan ændre på diagrammer og stadig bevare ækvivalens.

Definition 3.3. *Reidemeister-trækkene*, som skrives $R1$, $R2$, $R3$, er defineret som på Figur 3.6.

Normalt siger vi, at to kæder er *relaterbare* med et Reidemeister-træk, fx $R2$, hvis vi kan opnå den ene ved at udføre Reidemeister-træk på den anden. Det giver sig selv, at to diagrammer repræsenterer den samme kæde, hvis de er relaterbare med et endeligt antal Reidemeister-træk.

Sætning 3.4 (Reidemeister, 1932)**.** For alle knuder og kæder gælder der, at



Figur 3.6: De tre Reidemeister-træk, der relaterer ækvivalente segmenter af knudediagrammer.

1. vi kan tegne deres diagrammer.

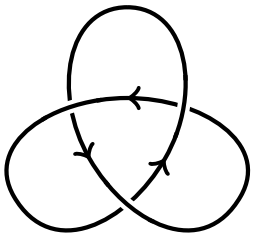
2. to kæder L_1 og L_2 er ækvivalente, hvis og kun hvis deres diagrammer D_1 og D_2 er relaterbare med endeligt mange Reidemeister træk.

I praksis er Sætning 3.4 fuldstændig nytteløs for at beslutte, om to diagrammer viser ækvivalente kæder, fordi det kan være meget ikke-intuitivt at vise ækvivalens mellem to diagrammer, som er relaterbare med rigtig mange Reidemeister-træk. Til gengæld vil vi anvende sætningen til at bevise relationer mellem knudeinvarianter, som kan bruges til meget hurtigere at bevise ækvivalens.

4 Orienteringer og Knudefunktioner

Definition 4.1. En *orienteret knude* er en knude, hvor snoren har en retning. Vi angiver dette ved at tegne en pil oven på linjestykkerne i diagrammet.

En orienteret kæde er en kæde, hvor alle komponenterne er orienterede. Det viser sig, at orienterede diagrammer er meget forskellige fra diagrammer uden en orientering, hvilket I vil se på i de tilhørende opgaver. For at to orienterede knuder

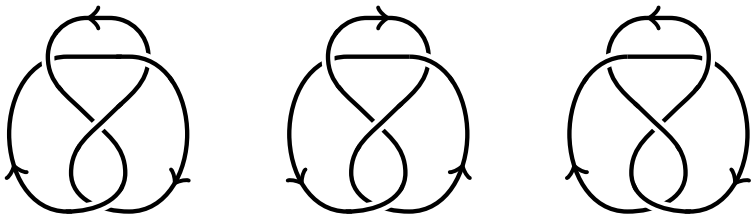


Figur 3.7: Et diagram af en orienteret trekløverknude. Her kan man teknisk set vælge to forskellige orienteringer af diagrammet – positiv eller negativ omløbsretning (matematikersprog for 'mod' eller 'med' uret). Men faktisk er disse ens, hvis man ser knuden fra 'bagsiden' af papirets plan.

skal være ækvivalente, skal diagrammerne udover at være relaterbare også have samme orientering. Selvom de to mulige orienteringer i Figur 3.7 giver den samme orienterede knude, så kan andre diagrammer have to ikke-ækvivalente orienteringer! Derfor kan det være relevant at se på forskellige funktioner, som laver orienterede knuder om til andre.

Definition 4.2 (Modsætning)**.** Lad L være en orienteret kæde. *Modsætningen* af L, som vi skriver rL, er en orienteret kæde, som fås ved at vende orienteringen af alle komponenter i L.

Definition 4.3 (Spejlbillede)**.** Lad L være en kæde (kan være orienteret). *Spejlbilledet* af L, som vi skriver mL, er kæden, som fås af at spejle L i et vilkårligt plan.



Figur 3.8: Et orienteret diagram af figur-otte knuden 4_1 samt dens tilsvarende modsætning $r4_1$ hvor orienteringen er vendt, og spejlbilledet $m4_1$ taget i papirets plan.

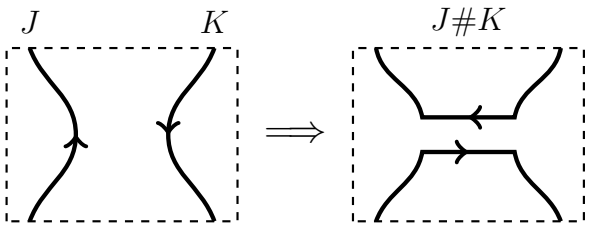
Bemærkning 4.4. En smart måde at konstruere spejlbilledet mL af kæden L er ved at placere spejlplanet i papiret. Når alle krydsninger spejles, svarer det derfor til, at overkryds bliver til underkryds og vice versa. I kan overbevise jer selv om, at lige meget, hvor man placerer spejlplanet, vil man altid opnå den samme kæde.

Ved hjælp af modsætning og spejlbillede kan vi, givet en kæde L, opskrive tre nye kæder:

$$L, \quad rL, \quad mL, \quad mrL \text{ (eller } rmL).$$

Disse vil ikke nødvendigvis være ækvivalente, men det er tilfældet for nogle simple knuder. For eksempel er trekløverknuden ækvivalent med dens modsætning, men ikke dens spejlbillede. På nuværende tidspunkt er det måske en smule vagt, hvorfor vi introducerer disse koncepter. Men senere vil vi se på, hvordan knudeinvarianter kan hjælpe os med at bestemme, hvorvidt de forskellige knuder er ækvivalente.

Definition 4.5 (Knudesummen)**.** Lad J og K være to orienterede knuder. *Summen* af J og K, som skrives $J\#K$, fås ved at sammensætte de to knuder på en måde, så deres samlede orientering er konsistent.



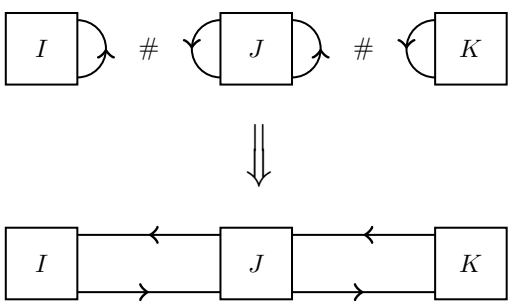
Figur 3.9: Illustration af udsnittet, hvor to knuder J og K summeres. Linjerne forbindes således at orienteringen er bevaret i resten af diagrammet.

Summen af knuder er kun defineret for orienterede knuder. Uden denne betingelse vil der ikke kunne være enighed om, hvordan man skal forbinde dem.

Sætning 4.6. Lad I, J og K være orienterede knuder, og $\bigcirc$ være en orienteret ikke-knude. Summen af disse opfylder følgende egenskaber:

1. Associativitet $(I\#J)\#K \simeq I\#(J\#K)$;
2. Kommutativitet $J\#K \simeq K\#J$;
3. Neutralitet $K\#\bigcirc \simeq K$.

Bevis. For at vise de tre dele gør vi brug af boksdiagrammer for de tre knuder.



Vi ser, at lige meget hvilken rækkefølge vi summerer knuderne, $(I\#J)\#K$ eller $I\#(J\#K)$, så vil det resultere i den samme knude.

Ligeledes er det nødvendigt for at kunne danne knuden $J\#K$, at J og K eksisterer i samme rum og er disjunkte. Trivielt er $J \sqcup K \simeq K \sqcup J$, så hvis vi antager, at j og k er to linjer i henholdsvis J og K, gør det ingen forskel, om vi forbinder $j \to k$ eller $k \to j$. Fordi rækkefølgen ikke påvirker noget, så må $J\#K \simeq K\#J$.

Beviset for punkt 3 overlades til læseren (se Opgave 6.6). □

Sumoperationen på knuder opfører sig faktisk meget ligesom multiplikation over de naturlige tal. Det er en kommutativ regneoperation, som har ikke-knuden som sin identitet. Et oplagt spørgsmål er derfor, om der også eksisterer en invers? Det vil sige, kan man på en eller anden måde addere to knuder, så summen er ækvivalent med ikke-knuden? Overraskende nok viser det sig ikke at være muligt, hvilket der arbejdes mere med i projektet om Seifert Overflader og Genus. Knuder danner dermed en *halvgruppe* (en gruppe uden inverser) under addition. Ligesom de naturlige tal med multiplikation har primfaktorisering, vil knuder også have en form for *knudefaktorisering*.

Definition 4.7. En orienteret knude er en *primknude*, hvis den ikke kan skrives på formen $K_1\#K_2$, hvor K_1,$K_2 \not\simeq \bigcirc$.

Derfor vil vi gerne bestemme alle de mulige primknuder, eftersom vi ud fra dem kan konstruere alle andre knuder. Jagten efter disse stammer helt tilbage fra 1800-tallet, hvor Gaußvar den første, som matematisk definerede knuder. Men motivationen for knudeteori kom først efter, Lord Kelvin kom på ideen om, at atomer er knuder af hvirvler i den kosmiske æter, hvilket var inspireret af den skotske fysiker Peter Taits

observationer om røgringe. Tanken var, at kemikalier og molekyler svarede til mere komplekse knuder og kæder. For eksempel troede Kelvin, at natrium svarede til Hopf-kæden på grund af dens dobbeltlinjer i dets emissionsspektrum.

Tait begyndte derfor at opskrive alle de unikke knuder i håb om at forudse en form for 'periodisk system' og skrev sidenhen *Taits formodninger*[2], som hjælper med at beskrive, hvornår vi har opnået en knude på dens simpleste form.

5 Jones-polynomiet

I sidste afsnit udforskede vi, hvad det vil sige for to knuder at være ens, samt hvordan Reidemeister-trækkene bevarer ækvivalens. Vi definerede også funktioner på orienterede knuder, som kun nogle gange bevarer ækvivalens, men som til gengæld kan benyttes til at lave nye knuder! Vigtigst af alt fandt vi ud af, at det faktisk ikke altid er nemt at afgøre, hvorvidt to knuder er ens. Dette er stadig et af de uløste problemer inden for knudeteori; hvordan kan vi definere en komplet knudeinvariant, som giver et forskelligt resultat for **alle** knuder?

I dette afsnit vil vi prøve kræfter med vores første knudeinvariant, som er en af de mere moderne og tværfaglige tilgange til knudeteori.

Definition 5.1. Et *Laurent polynomium* i variablene $X_1, \ldots, X_N$, som skrives $f \in \mathbb{Z}[X_1, \ldots, X_N]$ er et polynomium med heltalskoefficienter $a_{n,m} \in \mathbb{Z}$, hvor kun endeligt mange af koefficienterne er forskellige fra nul.

$$f = \sum_{n=1}^{N} \sum_{m=0}^{\infty} a_{n,m} X_n^m \in \mathbb{Z}[X_1, \ldots, X_N] \tag{3.1}$$

Eksempel 5.2. Følgende er eksempler på Laurent-polynomier:

[2]Som først blev bevist over 100 år senere!

- $f \in \mathbb{Z}[x,x^{-1}]$: $f = 4x^{-3} + x^{-2} - 6 + 2x^2 - 9x^5$
- $g \in \mathbb{Z}[p,q]$: $g = p - q + p^3 + 2q^6$

Følgende er ikke eksempler på Laurent-polynomier:

- $h \in \mathbb{Z}[w]$: $h = w^{-1} + w$ (Fordi: $m \geq 0$, så w^{-1} kan ikke forekomme)
- $l \in \mathbb{Z}[y,y^{-1}]$: $l = 2.5y^{-3} + 3 + 7y^2$ (Fordi: $2.5 \notin \mathbb{Z}$)

$\circ$

Sætning 5.3 (V. Jones, 1985)**.** Jones-polynomiet af en orienteret kæde L er et Laurent-polynomium $V(L) \in \mathbb{Z}\left[t^{1/2},t^{-1/2}\right]$, som er en knudeinvariant, der er defineret ved, at

- $V(\bigcirc) = 1$, hvor $\bigcirc$ er ikke-knuden.
- den opfylder *skein-relationen*[3]

$$t^{-1}V(L_+) - tV(L_-) + \left(t^{-1/2} - t^{1/2}\right)V(L_0) = 0. \quad (3.2)$$

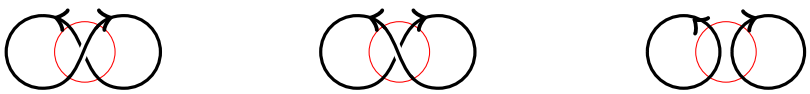
Her bruges notationen L_+, L_-, L_0 for de tre orienterede kæder, hvor en krydsning i diagrammet af L omskrives til en af følgende:

L_+ L_- L_0

"Venstrehåndet" "Højrehåndet"

[3]Skein-relationen er ikke opkaldt efter en Hr. eller Fru Skein. Ordet kommer fra den engelske betegnelse, som beskriver et 'bundt' garn (også kaldet fed på dansk). Det er dog her blevet valgt ikke at oversætte ordet, da det kan være en smule forvirrende, hvis vi kalder det en 'fed relation' – selvom matematikken er ret fed.

Eksempel 5.4. Lad os beregne Jones polynomiet $V(T)$ af den trivielle kæde med to komponenter $T = \bigcirc\bigcirc$. Først vælger vi en krydsning i diagrammet og udjævner den på de tre forskellige måder.



T_+ T_- T_0

Det er let at se, at både T_+ og T_- er ækvivalente med ikke-knuden, samt at T_0 svarer til den trivielle kæde med to komponenter, som vi starterede med. Vi kan derfor skrive skein relationen som

$$t^{-1}V\left(\bigcirc\right) - tV\left(\bigcirc\right) + \left(t^{-1/2} - t^{1/2}\right)V\left(\bigcirc\bigcirc\right) = 0. \tag{3.3}$$

Sætning 5.3 definerer ikke-knuden til at have Jones-polynomiet $V\left(\bigcirc\right) = 1$, så

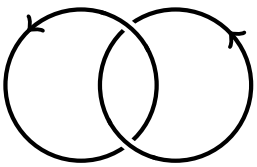
$$t^{-1} - t + \left(t^{-1/2} - t^{1/2}\right)V\left(\bigcirc\bigcirc\right) = 0. \tag{3.4}$$

Omskrives $t^{-1} - t = \left(t^{-1/2} - t^{1/2}\right)\left(t^{-1/2} + t^{1/2}\right)$, får vi, at

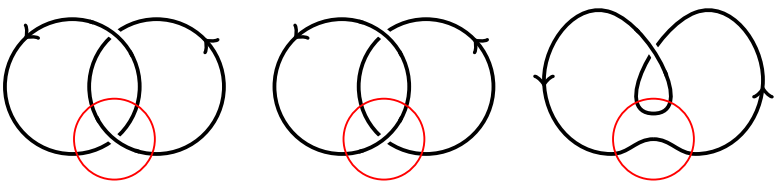
$$V(T) = -\left(t^{-1/2} + t^{1/2}\right), \tag{3.5}$$

hvilket er Jones-polynomiet af den trivielle kæde med to komponenter. ∘

Eksempel 5.5. Lad os beregne Jones-polynomiet af Hopf-kæden $V(\text{Hopf})$ med følgende orienterede diagram:



Igen opskriver vi diagrammerne for Hopf_+, Hopf_- og Hopf_0, hvor vi tegner en vilkårligt valgt krydsning på forskellige måder.



Hopf_+ Hopf_- Hopf_0

Da er skein relationen

$$t^{-1}V(\text{Hopf}_+) - tV(\text{Hopf}_-) + \left(t^{-1/2} - t^{1/2}\right) V(\text{Hopf}_0) = 0. \tag{3.6}$$

Ved brug af Reidemeister-trækkene kan vi vise, at Hopf_- er ækvivalent med den orienterede trivielle kæde med to komponenter, som vi i Eksempel 5.4 viste var $V\left(\bigcirc\bigcirc\right) = -\left(t^{-1/2} + t^{1/2}\right)$. Derudover er Hopf_0 ækvivalent med ikke-knuden, så $V(\text{Hopf}_0) = 1$. Bemærk også, at $\text{Hopf} \simeq \text{Hopf}_+$. Fra skein relationen får vi, at

$$t^{-1}V(\text{Hopf}) - t\left(-t^{-1/2} - t^{1/2}\right) + \left(t^{-1/2} - t^{1/2}\right) = 0. \tag{3.7}$$

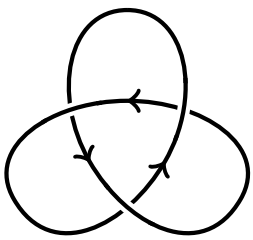
Vi løser udtrykket for $V(\text{Hopf})$:

$$V(\text{Hopf}) = -t^{5/2} - t^{1/2}. \tag{3.8}$$

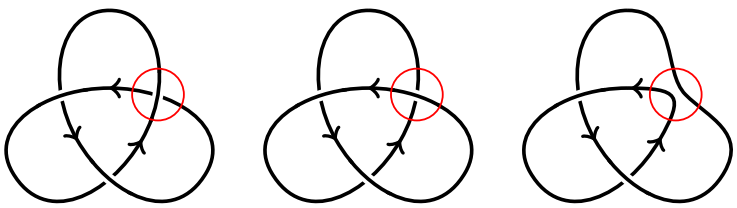
$\circ$

Bemærkning 5.6. Hvis vi havde valgt en anden orientering af Hopf-kæden ville udregningerne være anderledes, hvilket havde påvirket det endelige resultat. Med andre ord ***afhænger Jones polynomiet af en orienteret kæde af de enkelte komponenters orientering***.

Eksempel 5.7. Lad os beregne Jones-polynomiet af en orienteret, spejlvendt trekløverknude, $m3_1$. Bemærk, at $r3_1 \simeq 3_1$, hvilket betyder, at trekløverknuden er invertibel, samt at valget af orientering er ligegyldig.



Først tager vi udgangspunkt i den højre øverste krydsning. Herfra fås tre forskellige orienterede diagrammer.



3_{1_+} er præcis den orienterede knude, vi startede med, 3_{1_-} kan vi vise er ækvivalent med ikke-knuden, og 3_{1_0} viser samme orienterede Hopf-kæde som i Eksempel 5.5. Skein-relationen

bliver dermed

$$t^{-1}V(3_1) - tV\left(\bigcirc\right) + \left(t^{-1/2} - t^{1/2}\right)V(\text{Hopf}) = 0, \quad (3.9)$$

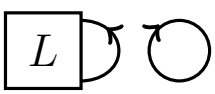
hvor $V(\bigcirc) = 1$ og $V(\text{Hopf}) = -t^{5/2} - t^{1/2}$. Da har vi, at

$$V(3_1) = -t^4 + t^3 + t. \quad (3.10)$$

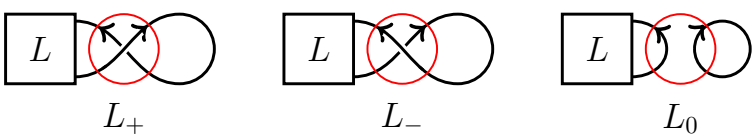
$\circ$

Proposition 5.8. Lad L være en vilkårlig orienteret kæde. Da er relationen mellem Jones polynomiet af L og dens disjunkte forening med ikke-knuden givet ved $V(L \sqcup \bigcirc) = -\left(t^{1/2} + t^{-1/2}\right)V(L)$.

Bevis. Først tegner vi $L \sqcup \bigcirc$ ved brug af følgende boksdiagram:



Herfra opskrives de tre diagrammer, som opstår ved at tegne de forskellige krydsninger:



Observér, at L_+ og L_- begge er ækvivalente med L, mens L_0 er ækvivalent med $L \sqcup \bigcirc$. Skein relationen bliver dermed

$$t^{-1}V(L) - tV(L) + \left(t^{-1/2} - t^{1/2}\right)V\left(L \sqcup \bigcirc\right) = 0. \quad (3.11)$$

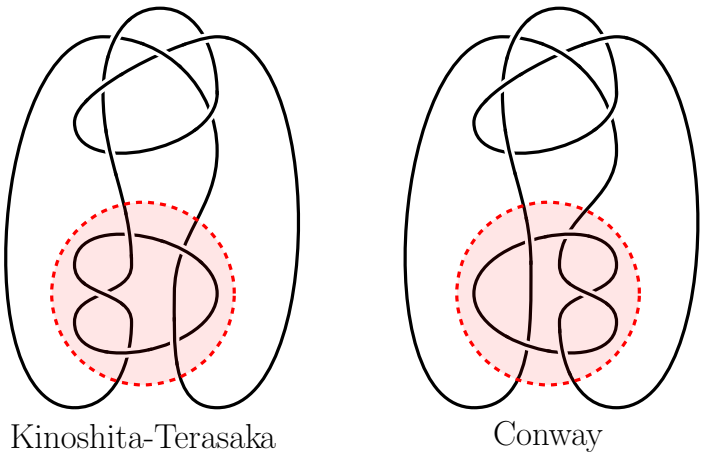
Dette kan vi omskrive til

$$\begin{aligned} V\left(L \sqcup \bigcirc\right) &= -\frac{t^{-1}-t}{t^{-1/2}-t^{1/2}} V(L) \\ &= -\frac{(t^{-1/2}+t^{1/2})(t^{-1/2}-t^{1/2})}{t^{-1/2}-t^{1/2}} V(L) \\ &= -\left(t^{-1/2}+t^{1/2}\right) V(L), \end{aligned}$$

som var hvad, vi skulle vise. □

I de ovenstående eksempler har vi ikke kun set på, hvordan man beregner Jones-polynomiet for forskellige orienterede knuder og kæder, men også hvordan det bliver til en rekursiv proces. For at beregne Jones-polynomiet af trekløverknuden er det nyttigt at kende Jones-polynomiet af Hopf-kæden, og for Hopf-kæden er det bedst at kende til polynomiet for den trivielle kæde med to komponenter. Langsomt ved at ændre på krydsningerne bygger man kæder, som er simplere og simplere, indtil man ender med den trivielle $V(\bigcirc) = 1$.

Selvom det er meget usandsynligt, er det faktisk muligt for forskellige knuder og kæder at have samme Jones polynomium. Et klassisk eksempel er Conway-knuden og Kinoshita-Terasaka knuden, som begge har 11 krydsninger og samme Jones-polynomium, men de er ikke ækvivalente! Det specielle ved disse er, at de er adskilt af et såkaldt "mutanttræk", hvilket betyder, at en sektion af diagrammet kan roteres for at opnå den anden knude. Disse knuder kaldes derfor også for *mutantknuder*.



Figur 3.10: Diagrammer af mutantknuderne 11n42 (Kinoshita-Terasaka knuden) og 11n34 (Conway knuden), og hvordan de er relaterbare med et mutanttræk.

Kauffman-parentesen

Måden, som vi har introduceret og taklet Jones-polynomiet, virker som om, det er trukket ud af den blå luft. Resultaterne af de gennemgåede eksempler stemmer overens, og skein-relationen ser ud til at være konsistent. Men hvordan er vi sikre på, at to ækvivalente orienterede kæder altid har samme Jones-polynomium, uanset hvilket diagram vi vælger? Og hvordan kan vi vise, at skein-relationen faktisk er opfyldt? Jones-polynomiet bygger i virkeligheden på et par forskellige værktøjer. Disse er *Kauffman-parentesen* og *vridningen*, som vi vil introducere i dette afsnit. Kauffman-parentesen har samme form som Jones-polynomiet, idet det er et Laurent-polynomium, dog i en ny variabel, som vi kalder A i stedet for t. Der findes dog to forskelle mellem de to:

1. Kauffman-parentesen er defineret for *ikke-orienterede* diagrammer, hvorimod Jones-polynomiet kun er defineret for orienterede kæder.

2. Vi kan nøjes med at beregne Kauffman-parentesen for dele af et diagram i stedet for hele kæden.

Definition 5.9. *Udjævningen* af en venstre krydsning ⤫ i et diagram D er et nyt diagram, hvor den valgte krydsning er ændret til en af følgende.

Vi skriver den negative udjævning som ⤬ og den positive udjævning som ⟩⟨.

Definition 5.10. Lad D være diagrammet af en knude. *Kauffman-parentesen* er et Laurent-polynomium $\langle D \rangle \in \mathbb{Z}[A,A^{-1}]$, som opfylder *Kauffman-aksiomerne*:

K1: $\langle \bigcirc \rangle = 1$

K2: $\langle D \sqcup \bigcirc \rangle = (-A^{-2} - A^2) \langle D \rangle$

K3: $\langle \rangle\!\!\diagup\!\!\langle \rangle = A \langle \rangle \langle \rangle + A^{-1} \langle \rangle\!\!\diagdown\!\!\langle \rangle$

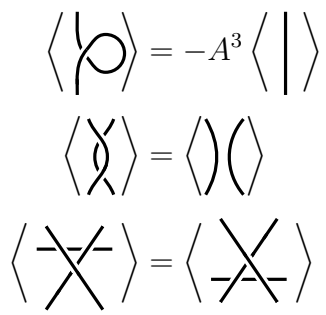
Her er $\bigcirc$ ikke-knuden, og de tre symboler ⤫, ⟩⟨ og ⤬ repræsenterer en krydsning i tre diagrammer af D, hvor de er forskellige med hensyn til udjævningen.

Bemærkning 5.11. For en "højrehåndet" krydsning ser K3 ud på følgende måde:

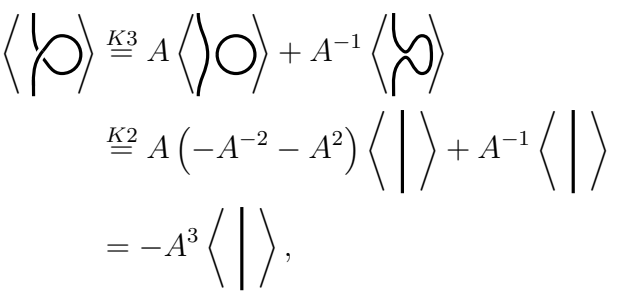
$$\langle \rangle\!\!\diagdown\!\!\langle \rangle = A \langle \rangle\!\!\diagup\!\!\langle \rangle + A^{-1} \langle \rangle \langle \rangle . \tag{3.12}$$

Kauffman-aksiomerne $K1$, $K2$, $K3$ tillader os at udregne Kauffman-parentesen af et vilkårligt diagram, uanset om det blot indeholder sektioner af et diagram eller komplette knuder og kæder. Hvis et diagram D har n krydsninger, så kan man skrive $\langle D \rangle$ som en sum af 2^n udtryk ved udelukkende at anvende K3. Når man ikke kan udføre operationerne længere, vil ens diagram bestå af lukkede kurver uden krydsninger. Herefter udregnes Kauffman-parentesen ved brug af K1 og K2. Om udregningerne bliver besværlige afhænger meget af, hvilken krydsning man først vælger at udjævne. Hvilken krydsning, som man starter med, vil dog ikke påvirke resultatet.

Lemma 5.12. Reidemeister-trækkene R1, R2 og R3 har følgende indflydelse på Kauffman-parentesen.

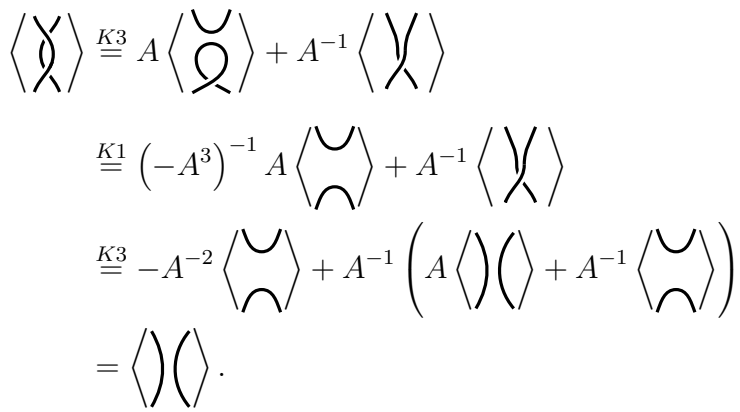


Bevis. For R1 har vi, at

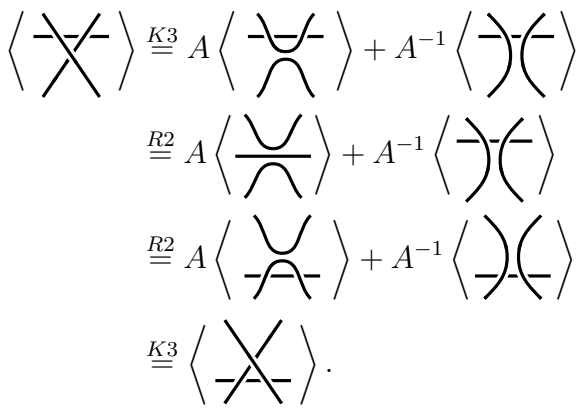


hvor vi benytter Kauffman aksiomerne K2 og K3. Herefter

udledes for R2:



Og for R3 er

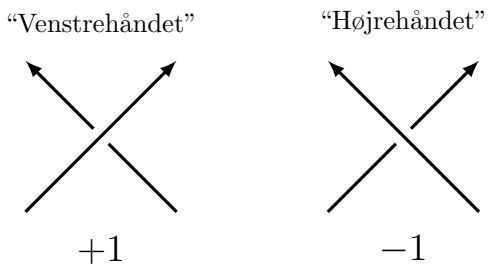


Dette fuldender beviset. □

Definition 5.13. Lad D være diagrammet af en orienteret kæde. *Vridningen* af D er

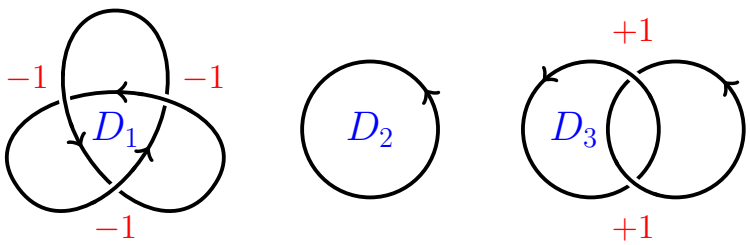
$$w(D) = \sum_c \text{sign}(c), \tag{3.13}$$

hvor vi summere over alle krydsninger c i D og sign(c) er krydsningens fortegn (se figuren nedenfor). Bemærk dog, at sign(c) her summerer over **alle** krydsninger og ikke kun dem, hvor forskellige komponenter krydser.



Figur 3.11: Krydsningers fortegn.

Eksempel 5.14. For de tre orienterede diagrammer



har vi, at $w(D_1) = -3$, $w(D_2) = 0$ og $w(D_3) = 2$. ∘

Hvorfor virker Jones-polynomiet?

Jones' sætning (Sætning 5.3) beskriver, hvordan et Laurent-polynomium, der opfylder specifikke regler, i virkeligheden også er en knudeinvariant. Med vores viden om Kauffman-parentesen og vridningen vil vi først definere Jones-polynomiet på en alternativ måde. Dernæst vil vi bruge dette til at vise, at Jones-polynomiet er en invariant.

Definition 5.15 (Jones polynomiet)**.** *Jones-polynomiet* af en orienteret kæde L er et Laurent polynomium $V(L) \in$

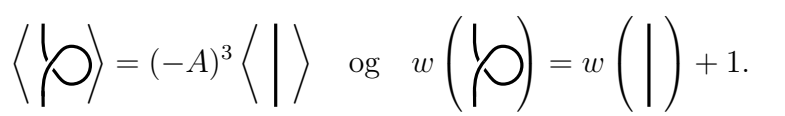
$\mathbb{Z}[t^{1/2},t^{-1/2}]$ givet ved

$$V(L) = \left[(-A)^{-3w(D)} \langle D \rangle\right]_{t^{1/2}=A^{-2}}, \tag{3.14}$$

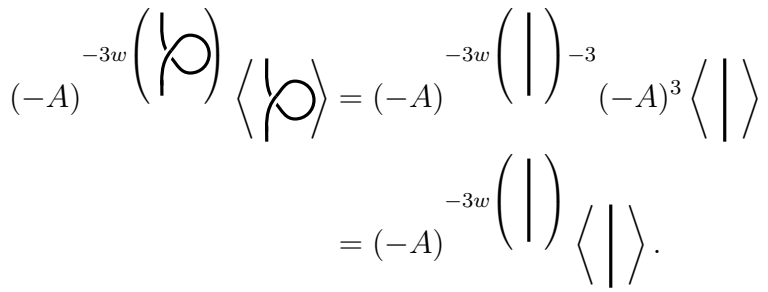
hvor D er et vilkårligt diagram af L. Subskriptet betyder, at vi skifter variable, så $t^{1/2} = A^{-2}$.

Sætning 5.16. Jones-polynomiet er en invariant for orienterede kæder.

Bevis. Lad L være en orienteret kæde, og lad D være et vilkårligt diagram af L. Det er nok at vise, at $V(L)$ er invariant under anvendelse af Rediemeister-trækkene på D. Ifølge Lemma 5.12 og resultatet fra Opgave 6.16 ændrer $\langle D \rangle$ og $w(D)$ sig ikke under anvendelse af R2 eller R3. Derfor behøver vi kun at undersøge, hvordan R1 påvirker Jones polynomiet. Vi ved, at



Da har vi, at



Dermed er $(-A)^{-3w(D)} \langle D \rangle$ invariant under R1, hvilket fuldfører beviset. □

Sætning 5.17. Jones-polynomiet opfylder skein-relationen og egenskaben $V(\bigcirc) = 1$.

Bevis. Hvis vi indsætter Ligning (3.14) i skein-relationen og erstatter hvert t med A^{-4} får vi, at

$$A^4(-A)^{-3w(L_+)}\left\langle \times \right\rangle - A^{-4}(-A)^{-3w(L_-)}\left\langle)(\right\rangle + (A^2 - A^{-2})(-A)^{-3w(L_0)}\left\langle \right\rangle\left\langle \right\rangle = 0. \tag{3.15}$$

Bemærk, at $w(L_\pm) = w(L_0) \pm 1$, så det følger, at

$$-A\left\langle \times \right\rangle + A^{-1}\left\langle \times \right\rangle + (A^2 - A^{-2})\left\langle \right\rangle\left\langle \right\rangle = 0. \tag{3.16}$$

Nu hvor vi har konstrueret skein-relationen for vores nye definition af Jones-polynomiet, så skal vi også vise, at skein-relationen stadigvæk gælder. Fra definitionen af Kauffman-aksiom K3 har vi følgende to ligninger:

$$\left\langle \times \right\rangle = A\left\langle \right\rangle\left\langle \right\rangle + A^{-1}\left\langle) (\right\rangle \tag{3.17}$$

og (3.18)

$$\left\langle \times \right\rangle = A\left\langle) (\right\rangle + A^{-1}\left\langle \right\rangle\left\langle \right\rangle.$$

Ganger vi den første ligning med A og den anden med A^{-1}, og derefter trækker de to ligninger fra hinanden, får vi, at

$$A\left\langle \times \right\rangle - A^{-1}\left\langle \times \right\rangle = \left(A^2\left\langle \right\rangle\left\langle \right\rangle + \left\langle) (\right\rangle\right) \tag{3.19}$$

$$- \left(\left\langle) (\right\rangle + A^{-2}\left\langle \right\rangle\left\langle \right\rangle\right) \tag{3.20}$$

$$= \left(A^2 - A^{-2}\right)\left\langle \right\rangle\left\langle \right\rangle.$$

Ved at trække $A\left\langle \times \right\rangle - A^{-1}\left\langle \times \right\rangle$ fra på begge sider af udtrykket opnår vi relationen i Ligning 3.16. Vi har dermed vist, at Definition 5.15 og Kauffman-aksiomerne medfører skein-relationen. □

Modsætninger, spejlbilleder og summer

Vi vil nu også undersøge, hvordan Jones-polynomiet opfører sig, når vi anvender forskellige knudefunktioner på det.

Proposition 5.18. Lad L være en orienteret kæde.

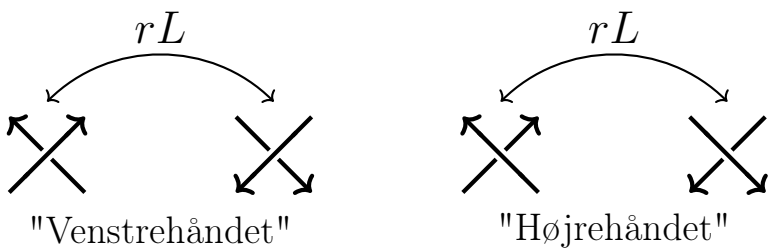
1. $V(rL) = V(L)$
2. $V(mL)(t) = V(L)(t^{-1})$

Notationen i punkt 2 betyder, at $V(mL)$ er lig $V(L)$, når vi i $V(L)$ erstatter t med t^{-1}.

Bevis. Punkt 1: Lad D være et diagram af L. Da har vi, at

$$V(L) = \left[(-A)^{-3w(D)} \langle D \rangle\right]_{t^{1/2}=A^{-2}}. \tag{3.21}$$

Siden $\langle D \rangle$ ikke afhænger af D's orientering, skal vi blot vise, at det samme gælder for $w(D)$. Modsætningen påvirker en given krydsning på følgende måde:



Vi kan se, at krydsningens fortegn ikke ændrer sig, når man tager modsætningen, så vridningen ændrer sig heller ikke. Jones-polynomiet af kæden og dens modsætning må dermed være ens.

Punkt 2: Lad D være et vilkårligt diagram af L. Da er $\overline{D}$ et diagram af spejlingen mL, hvor overkrydsninger er skiftet til underkrydsninger og vice versa. Fra det kan vi komme med to påstande:

1. $w(\overline{D}) = -w(D)$
2. $\left\langle \overline{D} \right\rangle = \overline{\langle D \rangle}$

Bemærk, at $\left\langle \overline{D} \right\rangle$ er Kauffman parentesen af diagrammet $\overline{D}$ af mL, mens $\overline{\langle D \rangle}$ er Kauffman parentesen af D, hvor vi har erstattet alle A med A^{-1} og omvendt. Første punkt giver sig selv, da når alle krydsninger skifter fortegn, så må vridningen også ændre fortegn. Det andet punkt vises ved at se, hvordan vi kan skrive Kauffman aksiomerne i Definition 5.10 for et spejlet diagram. Ikke-knuden er ækvivalent med dens spejling, så $\langle \bigcirc \rangle = \left\langle \overline{\bigcirc} \right\rangle = 1$. For K2 har vi, at

$$\left\langle \overline{D \sqcup \bigcirc} \right\rangle = \left\langle \overline{D} \sqcup \bigcirc \right\rangle = (-A^{-2} - A^2) \left\langle \overline{D} \right\rangle ; \tag{3.22a}$$

$$\overline{\left\langle D \sqcup \bigcirc \right\rangle} = \overline{(-A^{-2} - A^2) \langle D \rangle} = (-A^2 - A^{-2}) \overline{\langle D \rangle}. \tag{3.22b}$$

Tilsvarende har vi for K3, at

$$\left\langle \overline{\times} \right\rangle = A^{-1} \left\langle \overline{)(} \right\rangle + A \left\langle \overline{\smile\!\frown} \right\rangle ; \tag{3.23a}$$

$$\overline{\left\langle \times \right\rangle} = A \overline{\left\langle)(\right\rangle} + A^{-1} \overline{\left\langle \smile\!\frown \right\rangle}. \tag{3.23b}$$

Bemærk, at hvert par af ligninger, (3.22a) og (3.23a), samt (3.22b) og (3.23b), i virkeligheden er Kauffman-aksiomerne for henholdsvis $\left\langle \overline{D} \right\rangle$ og $\overline{\langle D \rangle}$. Fordi de overholder samme aksiomsæt, så må de også være lig hinanden.

Da har vi, at

$$(-A)^{-3w(\overline{D})} \left\langle \overline{D} \right\rangle = (-A)^{3w(D)} \overline{\langle D \rangle} = \overline{(-A)^{-3w(D)} \langle D \rangle}. \tag{3.24}$$

Sæt $A^{-2} = t^{1/2}$. Da har vi, at $V(mL)(t) = \overline{V(L)}(t) = V(L)(t^{-1})$. □

Korollar 5.19. Hvis K er en knude, så afhænger $V(K)$ ikke af orienteringen af K. Med andre ord er Jones polynomiet en invariant af ikke-orienterede knuder.

Bevis. Dette følger direkte fra punkt 1 i propositionen. □

Det følger dog ikke, at Jones polynomiet er en invariant af ikke-orientede *kæder*. En knude har nemlig maksimalt to mulige orienteringer. En kæde med m komponenter kan derimod have op til 2^m forskellige orienteringer.

Korollar 5.20. Lad L være en orienteret kæde. Hvis $V(L)(t) \neq V(L)(t^{-1})$, så er L og mL ikke ækvivalente.

Eksempel 5.21. Jones polynomiet for trekløverknuden fandt vi i Eksempel 5.7 til at være

$$V(3_1) = -t^4 + t^3 + t.$$

Erstattes t med t^{-1}, så får vi ikke det samme polynomium! Så $3_1 \not\simeq m3_1$, hvilket vi også diskuterede i Afsnit 4. Derimod er

$$V(4_1) = t^2 - t + 1 - t^{-1} + t^{-2}.$$

Dette kunne få en til at konkludere, at de er ækvivalente. Men faktisk siger korollaren ikke noget om dette! Dog ved vi fra Opgave 6.2, at de er ækvivalente, $4_1 \simeq m4_1$, hvilket stemmer overens med, at vi får samme Jones-polynomium. ∘

Sætning 5.22. Lad J og K være orientede knuder, og lad L og M være orienterde kæder. Følgende egenskaber gælder for Jones-polynomiet:

1. $V(J\#K) = V(J)V(K)$
2. $V(L \sqcup M) = (-t^{1/2} - t^{-1/2})V(L)V(M)$

Bevis. Punkt 1: Lad D_J og D_K være diagrammer af henholdsvis J og K. Forestil dig nu, at vi fuldkomment ignorerer den del af diagrammet af $J\#K$, som originalt bestod af K og gentagne gange udfører skein-relationen på diagrammet D_J. Jones polynomiet af J kan vi skrive på formen

$V(J) = f_1(t)V\left(\bigcirc\right) + f_2(t)V\left(\bigcirc\bigcirc\right) + \cdots + f_m(t)V\left(\bigcirc^{m}\right),$ (3.25)

hvor $f_1, \ldots, f_m$ er Laurent-polynomier, og $\bigcirc^m$ repræsenterer ikke-kæden med m komponenter for et passende $m \in \mathbb{N}$. Nu betragter vi D_K. Efter vi har anvendt skein-relationen på D_J så mange gange, som er muligt, vil der i hvert diagram være en af ikke-knuderne, som er sammensat med K. Når vi i stedet betragter $V(J\#K)$, så vil diagrammerne $\bigcirc^n$ i Ligning (3.25) for $1 \leq n \leq m$ svare til den disjunkte forening $K \sqcup \bigcirc^{n-1}$. Når vi opskriver $V(J\#K)$, skal vi derfor lave følgende ændring i $V(J)$:

$$V\left(\bigcirc^n\right) \mapsto V\left(K \sqcup \bigcirc^{n-1}\right). \tag{3.26}$$

Da er

$$\begin{aligned} &V(J\#K) = \\ &f_1(t)V(K) + f_2(t)V\left(K \sqcup \bigcirc\right) + \cdots + f_m(t)V\left(K \sqcup \bigcirc^{m-1}\right). \end{aligned} \tag{3.27}$$

Fra Proposition 5.8 og resultatet fra Opgave 6.12 har vi, at

$$\begin{aligned} V\left(K \sqcup \bigcirc^n\right) &= (-1)^n \left(t^{1/2} + t^{-1/2}\right)^n V(K) \\ &= V\left(\bigcirc^{n+1}\right) V(K). \end{aligned} \tag{3.28}$$

Kombinerer vi Ligning (3.27) og (3.28) får vi, at

$$\begin{aligned} V(J\#K) =& f_1(t)V\left(\bigcirc\right) V(K) + f_2(t)V\left(\bigcirc\bigcirc\right) V(K) + \cdots \\ &+ f_m(t)V\left(\bigcirc^m\right) V(K) \\ =& \left[f_1(t)V\left(\bigcirc\right) + f_2(t)V\left(\bigcirc\bigcirc\right) + \cdots \right. \\ &\left. + f_m(t)V\left(\bigcirc^m\right)\right] V(K) \\ =& V(J)V(K). \end{aligned} \tag{3.29}$$

Punkt 2: Lad os tegne kæderne L og M som boksdiagrammer og anvende skein-relationen.

$(L \sqcup M)_+$

$(L \sqcup M)_-$

$(L \sqcup M)_0$

Vi ser, at $(L \sqcup M)_+ \simeq L\#M$, $(L \sqcup M)_- \simeq L\#M$ og $(L \sqcup M)_0 \simeq L \sqcup M$. Dermed er skein-relationen

$$t^{-1}V(L\#M) - tV(L\#M) + (t^{-1/2} - t^{1/2})V(L \sqcup M) = 0. \tag{3.30}$$

Vi kan isolere for $V(L \sqcup M)$ ved at benytte resultatet $V(L\#M) = V(L)V(M)$ fra forrige bevis:

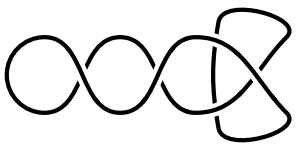
$$\begin{aligned} V(L \sqcup M) &= \frac{t^{-1} - t}{t^{-1/2} - t^{1/2}} V(L\#M) \\ &= \frac{(t^{1/2} - t^{-1/2})(-t^{1/2} - t^{-1/2})}{t^{-1/2} - t^{-1/2}} V(L)V(M) \\ &= (-t^{1/2} - t^{-1/2})V(L)V(M) \end{aligned} \tag{3.31}$$

□

6 Opgaver

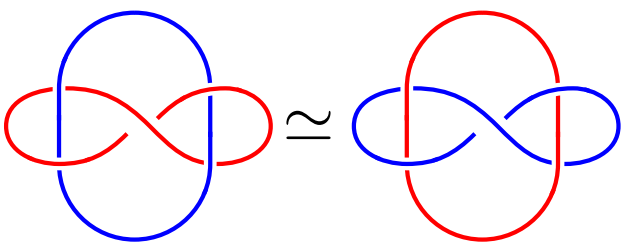
Knuder og kæder

Opgave 6.1:
Find en følge af Reidemeister træk, der viser, at nedenstående knude er ækvivalent med ikke-knuden.



Opgave 6.2:
Er $4_1 \simeq m(4_1)$?

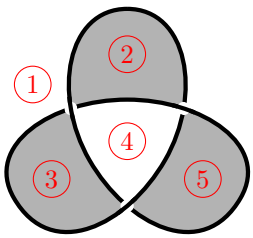
Opgave 6.3:
Vis, at Whitehead-kæden har en komponent-symmetri. Med andre ord, vis, at den er ækvivalent med Whitehead-kæden, hvor komponenterne er byttet rundt, som vist på Figur 3.12.



Figur 3.12: Komponent-symmetri af Whitehead-kæden.

Opgave 6.4:
Argumenter for, at der ikke eksisterer nogle knuder $K \not\simeq \bigcirc$ med 1 eller 2 krydsninger.

Opgave 6.5:
Vis, at antallet af områder (se Figur 3.13) i et kædediagram er lig antallet af krydsninger plus 2.



Figur 3.13: I et diagram med tre krydsninger er der fem områder.

Opgave 6.6:
Vis punkt 3 i Sætning 4.6: For enhver knude K, så er $K\#\bigcirc \simeq K$, hvor $\bigcirc$ er en orienteret ikke-knude.

Opgave 6.7:
En *kringle* $P(p,q,r)$ er en kæde på samme form som vist på Figur 3.14.

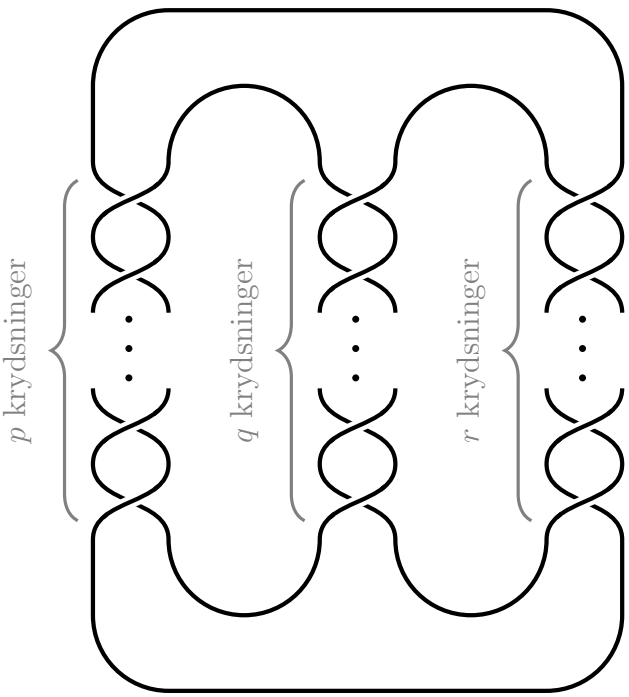
a) Tegn kringlerne $P(2,2,2)$, $P(-3,0,-3)$ og $P(-2,3,7)$.

b) Bestem hvilke kendte kæder følgende kringler er ækvivalente med:

- $P(0,0,0)$
- $P(0,-2,0)$
- $P(1,1,1)$
- $P(2,1,1)$

- $P(1,2,2)$

c) Hvor mange komponenter har $P(p,q,r)$ som funktion af p, q og r? Hvornår er det en knude?



Figur 3.14: Et generelt diagram af en kringle $P(p,q,r)$, hvor $p,q,r \in \mathbb{Z}$. Her lader vi positive p,q,r betyde venstre krydsninger og negative betyde højre krydsninger.

Nedenstående opgaver handler om *lænketallet*, som er en invariant for orienterede kæder.

Definition. Lad L være en orienteret kæde med diagram D, og lad c være alle krydsninger i D, hvor forskellige kompo-

nenter krydser. Her definerer vi *lænketallet* af L til at være

$$lk(L) = \frac{1}{2}\sum_{c} \text{sign}(c), \tag{3.32}$$

hvor vi husker Definition 5.13 af sign.

Opgave 6.8:

a) Beregn $lk(L)$ for figur-otte knuden, Hopf kæden og Whitehead kæden (se Figur 3.2 og 3.3).

b) Vi vil bevise, at $lk(L)$ er en invariant. Argumenter for, at det er tilstrækkeligt at vise, at $lk(L)$ ikke ændrer sig under anvendelse af Reidemeister træk.

c) Vis, at $lk(L)$ er invariant under R1 og R2. (Se evt. hint efter opgaverne.)

d) Gør det samme for et par tilfælde af R3 og overbevis dig selv om, at $lk(L)$ er invariant under R3.

e) Lad L_1 og L_2 være to orienterede kæder. Argumenter for, at hvis $lk(L_1) \neq lk(L_2)$, så er $L_1 \not\simeq L_2$.

f) Hvis $lk(L_1) = lk(L_2)$ gælder det så altid, at $L_1 \simeq L_2$? (Se evt. hint efter opgaverne.)

Opgave 6.9:
Byg de Borromeiske ringe med fire komponenter. Vis, at den har lænketal $lk(B_n) = 0$.
(Svær, valgfri) Kan du konstruere de Borromeiske ringe med n komponenter?

Opgave 6.10:
Vis, at for de orienterede kæder med to komponenter $L = K_1 \sqcup K_2$ og $L' = K_1 \sqcup rK_2$, så er $lk(L) = -lk(L')$.

Jones-polynomiet

Opgave 6.11:
Vis, at Jones-polynomiet af figur-otte knuden er

$$V(4_1) = t^2 - t + 1 - t^{-1} + t^{-2}.$$

Hvad kan vi konkludere om 4_1 i forhold til andre kendte knuder?

Opgave 6.12:
Find et generelt udtryk for Jones-polynomiet af den trivielle kæde med n komponenter.

Opgave 6.13:
Bevis ved brug af skein-relationen og resultatet i Opgave 6.12, at Jones-polynomiet af en orienteret kæde med n komponenter er

$$V(L)(t = 1) = (-2)^{n-1}, \tag{3.33}$$

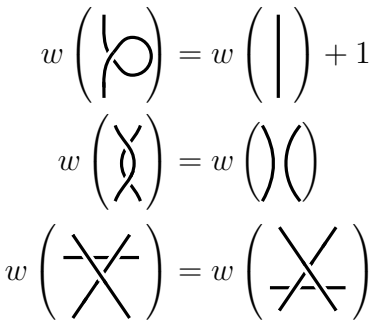
når $t = 1$. Argumenter for, at Jones-polynomiet aldrig kan være lig nul.

Opgave 6.14:
Lad L_+, L_- og L_0 være de tre kæder i skein-relationen, som er forskellige i én krydsning. Antag, at L_+ har n komponenter. Hvor mange komponenter kan L_- og L_0 have?

Opgave 6.15:
Vis, at Jones-polynomiet for kæder med et ulige antal komponenter (dvs. inklusiv knuder) kun har heltallige potenser af t (altså $\ldots, t^{-1}, 1, t, \ldots$). Vis ligeledes, at potenserne kun er halve heltal (altså $\ldots, t^{-1/2}, t^{1/2}, t^{3/2}, \ldots$), hvis der er et lige antal komponenter. (Se evt. hint efter opgaverne.)

Opgave 6.16:
Vis, at Reidemeister-trækkene R1, R2 og R3 har følgende

effekt på vridningen af et diagram:



Opgave 6.17:
Conway-polynomiet $\nabla_L(z) \in \mathbb{Z}[z]$ er en anden type invariant for orienterede kæder. Den opfylder en anden skeinrelation:

$$\nabla_{L_+}(z) - \nabla_{L_-}(z) = z\nabla_{L_0}(z), \tag{3.35}$$

hvor L_+, L_- og L_0 er de orienterede kæder, hvor en sektion i diagrammet af L omskrives ligesom for Jones-polynomiet. Antag, at $\nabla_{\bigcirc}(z) = 1$ og $\nabla_L(z) = \nabla_{rL}(z)$. Vis, at

a) Conway-polynomiet af de to mulige orienteringer af Hopf-kæden er $\pm z$.

b) Conway-polynomiet af den trivielle kæde med $n \geq 2$ komponenter er 0.

c) Conway-polynomiet af trekløverknuden er $z^2 + 1$.

d) Conway-polynomiet har aldrig negative potenser af z. (Se evt. hint efter opgaverne.)

e) Conway-polynomiet af enhver usammenhængende kæde er 0.

Opgave 6.18:
Lad $L = K_1 \sqcup K_2$ være en orienteret kæde. Vis, at $V(L') = V(L)$, hvor $L' = K_1 \sqcup rK_2$.

7 Hints til opgaverne

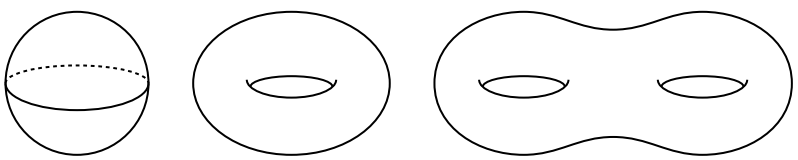
- Opgave 6.8c: Husk, at c er alle krydsninger, hvor forskellige komponenter krydser!
- Opgave 6.8f: Kan du finde en klasse af orienterede kæder som alle har lænketal $lk(L) = 0$?
- Opgave 6.15: Evt. bevis ved induktion.
- Opgave 6.17d: Brug induktion.

8 Projekt: Seifert-overflader og Genus

I dette projekt går vi tilbage til knudeteoriens rødder – nemlig til topologi. Tidligere har vi helt udeladt det faktum, at knuder rent faktisk er topologiske rum, og at man derfor i virkeligheden bør behandle dem ved brug af topologi. Derfor vil vi se på, hvordan vi ved at karakterisere knuder som overflader kan finde nye invarianter.

Først er det vigtigt at forstå, hvad *overflader* er, og hvordan vi kan arbejde med dem. Til vores formål er overflader todimensionelle objekter[4], hvor vi er ligeglade med længder, men rettere interesserer os for "nabolag" af punkter. Det vil sige, at vi jævnt kan transformere overflader så længe, at vi ikke tilføjer nye punkter eller fjerner eksisterende punkter.

Eksempel 8.1. Her er eksempler på tre overflader.



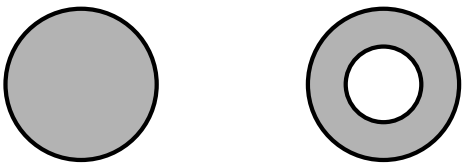
Sfære Torus Genus 2

○

I hvert af de ovenstående tilfælde udgør overfladerne et hult objekt. Men husk, at vi her kun diskuterer selve overfladerne – ikke det "indeni"!

[4] i virkeligheden er det en mængde med ekstra struktur – en "topologi" – som opfylder specifikke aksiomer

Eksempel 8.2. Her er eksempler på to 'flade' overflader.



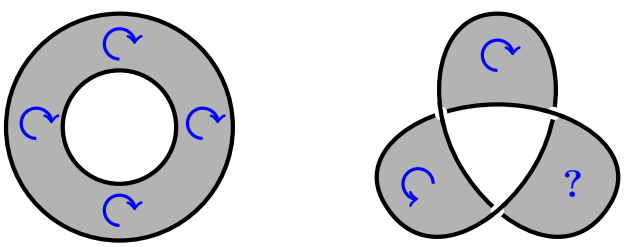
Disk Annulus

○

Definition 8.3. En overflade er *lukket*, hvis den ikke har nogle kanter.

Eksempel 8.4. Sfæren, torusen og genus 2 er alle lukkede. Derimod har disken og annulusen begge "kanter", hvorfor de ikke er lukkede. ○

Definition 8.5. En *orientering* af en overflade er et valg af "omløbsretning" ved hvert punkt på overfladen. Denne orientering skal kunne være det samme overalt på overfladen, når man bevæger sig rundt på den.



Figur 3.15: Annulusen er orienterbar, men overfladen til højre er ikke, fordi dens orientering ikke er entydig.

Omløbsretningen kan betyde enten "med uret" eller "mod uret". Ligesom, at man kan se overfladen fra to forskellige sider, så skal retningen også være konsistent, når man bevæger sig rundt på overfladen i tre dimensioner.

Hvis en overflade kan orienteres, så er den *orienterbar*. Overfladerne i Eksempel 8.1 og 8.2 er alle orienterbare. Til gengæld er overfladen med grænse tilsvarende trekløverknuden på Figur 3.15 ikke orienterbar.

Definition 8.6. Til enhver overflade Σ kan vi knytte et heltal $\chi(\Sigma)$ kaldet *Euler-karakteristikken*. Til vores formål er det blot en funktion, som opfylder følgende regler for vilkårlige overflader:

1. Ækvivalente overflader har samme Euler-karakteristik.

2. Disken har Euler karaktistk $\chi(\text{Disk}) = 1$.

3. $\chi(\Sigma_1 \sqcup \Sigma_2) = \chi(\Sigma_1) + \chi(\Sigma_2)$ for alle overflader Σ_1 og Σ_2.

4. Hvis Σ' fås ved at lime enderne af en strip til en overflade Σ, så vil $\chi(\Sigma') = \chi(\Sigma) - 1$.

5. Hvis Σ' fås ved at lime en disk til alle kanter af en overflade Σ, så vil $\chi(\Sigma') = \chi(\Sigma) + 1$.

Opgave 8.1:
Ved at bruge reglerne for Euler-karakteristikken i Definition 8.6, vis at

a) sfæren har Euler-karakteristik $\chi(\text{Sfære}) = 2$.

b) torusen har Euler-karakteristik $\chi(\text{Torus}) = 0$.

Definition 8.7. Hvis en overflade kan skrives som en disjunkt forening af to andre overflader, som kan adskilles af et plan, siges overfladen at være *usammenhængende*. Ellers er den *sammenhængende*.

Definition 8.8. *Genus* af en sammenhængende overflade Σ er

$$g(\Sigma) = \frac{2 - \chi(\Sigma) - k}{2}, \tag{3.36}$$

hvor k er antallet af 'kanter' i Σ.

Opgave 8.2:
Bestem genus for følgende overflader:

a) En sfære

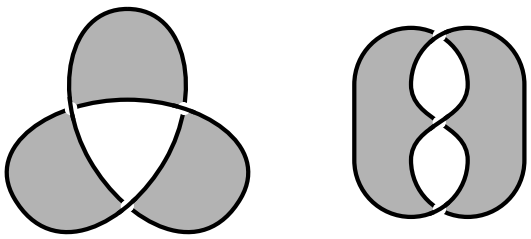
b) En torus

c) Genus 2

d) En lukket overflade med n huller ($n = 1$ og $n = 2$ for hhv. torussen og genus 2)

Sætning 8.9 (Klassificering af overflader)**.** To sammenhængende og orienterede overflader er ækvivalente, hvis og kun hvis, de har samme genus og samme antal kanter.

Ligesom knuder eksisterer overflader også som matematiske objekter i $\mathbb{R}^3$. Dog ses knuder som "linjestykker", hvorimod overflader har et to-dimensionelt spænd. Men i virkeligheden er overfladers kanter en fællesmængde af punkter, som danner en linje. Og ligeledes danner områderne mellem linjestykkerne på knudediagrammerne en overflade. For eksempel er kanten på følgende twistede overflade ækvivalent med hvad vi kender som trekløverknuden.



Figur 3.16: To forskellige overflader konstrueret ud fra trekløverknuden.

Dette motiverer oversættelsen af de begreber om overflader, vi lige har lært – Euler-karakteristikken og genus – til begreber om knuder og knudeinvarianter til at karakterisere egenskaber såsom ækvivalens.

Definition 8.10. En *Seifert-overflade* af en knude K er en sammenhængende og orienterbar overflade i $\mathbb{R}^3$, som har en kant svarende til K.

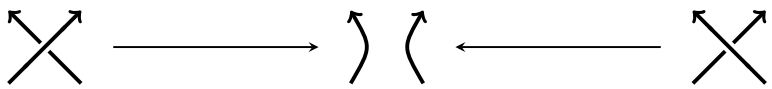
Opgave 8.3:
Overfladen til venstre på Figur 3.16 er ikke orienterbar og derfor ikke en Seifert-overflade. Overfladen til højre har også en kant svarende til et andet diagram af trekløverknuden (se Figur 3.2). Er den orienterbar? Er det en Seifert-overflade? Hvad kan du konkludere?

Sætning 8.11. Alle knuder udviser en Seifert overflade.

Metode 1 (Seiferts algoritme)**.** Vi konstruerer en overflade på følgende måde.

1. Vælg et diagram D af en knude. Vælg en orientering.

2. Udjævn alle krydsninger i forhold til orienteringen.



Diagrammet vil nu bestå af et antal ikke-knuder. Vi kalder disse *Seifert-cirkler*.

3. Konstruer nu en overflade ved at udfylde alle Seifert cirkler, så de bliver til diske. Hvis to cirkler ligger oven på hinanden, løftes den inderste "over" den yderste.

4. For hver krydsning i det originale diagram D tilføjes en twisted strip til hver disk med twist i henhold til krydsningen.

Resultatet vil være en orienterbar overflade, som vi betegner Σ_D.

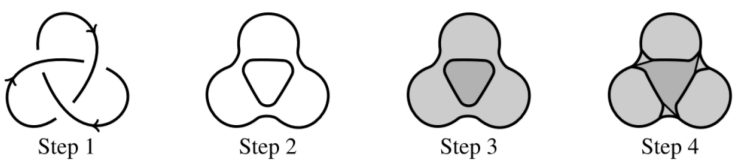
Opgave 8.4:
Lad K være en knude og D være et diagram af K. Vis, at

a) $\chi(\Sigma_D) = \mathcal{S} - n$,

b) $g(\Sigma_D) = \frac{1-\mathcal{S}+n}{2}$,

hvor n er antallet af krydsninger i D og $\mathcal{S}$ er antallet af Seifert-cirkler.

Eksempel 8.12. Hvis man anvender Seiferts algoritme til et diagram af trekløverknuden, giver det følgende overflade.



Her er $n = 3$ og $\mathcal{S} = 2$, så Seifert-overfladen har Euler-karakteristik $\chi(\Sigma_{3_1}) = 2-3 = -1$ og genus $g(\Sigma_{3_1}) = (1-2+3)/2 = 1$. Bemærk, hvordan denne overflade er forskellig fra den på Figur 3.15. Hvis overfladen er konstrueret via Seiferts algoritme, garanterer det, at den også er orienterbar. ∘

Hvis man implementerer et længdebegreb på vores overflader, så vi kan beregne "arealet" af Seifert-overfladerne, viser det sig faktisk også, at de minimerer arealet for enhver overflade med en kant svarende til knuden. Disse overflader kaldes også *minimalflader*. Samme fænomen ses faktisk på sæbebobler og sæbefilm: Overfladespændingen fra sæbevandet trækker i hinden, så det minimerer arealet. Dette tillader os faktisk eksperimentelt at bestemme Seifert-overfladerne for knuder ved brug af sæbevand:

1. Konstruer en vilkårlig knude K ud af ståltråd eller et lignende materiale.

2. Dyp knuden i sæbevand. Hinden vil danne en Seifert overflade af K.

! Bemærk at det ikke altid virker for større/komplekse knuder. Nogle gange skal de hjælpes på vej.

Overraskende nok, ligesom vi kan definere ækvivalens af overflader ved brug af Euler-karakteristikken og genus, kan vi også anvende dem som invarianter for knuder – ikke kun deres Seifert-overflader!

Definition 8.13. *Genus* af en knude K er

$$g(K) = \min\{g(\Sigma_D) \mid \Sigma_D \text{ er en Seifert-overflade af } K\}. \tag{3.37}$$

Bemærk, hvordan en knude kan have mange forskellige Seifert overflader, og at disse overflader kan have forskellige

genus. Hvis Σ_D er en vilkårlig Seifert overflade af K, så vil $g(K) \leq g(\Sigma_D)$, per definition.

Dog er der den udfordring, at for at bestemme $g(K)$, skal man i princippet kunne bestemme *alle* Seifert-overflader af K. Det er også derfor, at knudens genus er relativt svær at udlede, og hvorfor det ikke altid bliver brugt.

Opgave 8.5:
Bestem genus af ikke-knuden, $g\,(\bigcirc)$.

Opgave 8.6:
Bestem genus af Hopf-kæden.

Opgave 8.7:
I Eksempel 8.12 fandt vi en Seifert-overflade af trekløverknuden med genus 1. Brug Sætning 8.9 til at argumentere for, at $g(3_1) = 1$. Med andre ord, vis, at der ikke eksisterer en Seifert-overflade af trekløverknuden med genus 0.

Opgave 8.8:
Lad K være en knude med n krydsninger. Ved at betragte Seifert-overflader som en kombination af cirkler og bånd, vis, at genus af K har en øvre grænse $g(K) \leq n/2$.

Opgave 8.9:
I denne opgave vil vi vise, at $g(K)$ er en invariant.

a) Tegn Reidemeister-trækkene og deres mulige orienteringer.

b) Udjævn diagrammerne ved brug af Seiferts algoritme og sammenlign $g(\Sigma_D)$ for hvert træk.

c) Argumenter for, at $g(K)$ ikke ændrer sig.

Opgave 8.10:
Vis ud fra konklusionen i Opgave 8.9, at hvis $g(K) = 0$ for en knude K, så er $K \simeq \bigcirc$.

Opgave 8.11:
Lad J og K være knuder med Seifert-overflader Σ_J og Σ_K.

a) Vis ved brug af Definition 8.6, at

$$\chi(\Sigma_{J\#K}) = \chi(\Sigma_J) + \chi(\Sigma_K) - 1.$$

b) Antag, at vi vælger Σ_J og Σ_K således, at $g(\Sigma_J) = g(J)$ og $g(\Sigma_K) = g(K)$. Vis, at

$$g(\Sigma_{J\#K}) = g(J) + g(K).$$

c) Argumenter for, at $g(J\#K) \leq g(J) + g(K)$.

d) Antag nu i stedet, at $\Sigma_{J\#K}$ er en Seifert-overflade af $J\#K$ således, at $g(\Sigma_{J\#K}) = g(J\#K)$. Vis, at

$$g(J\#K) = g(\Sigma_J) + g(\Sigma_K).$$

e) Argumenter for, at $g(J\#K) \geq g(J) + g(K)$.

f) Brug resultaterne fra c) og e) til at vise relationen

$$g(J\#K) = g(J) + g(K). \tag{3.38}$$

Hvis vi husker tilbage til Definition 4.7, sagde vi, at en *primknude* var en knude, som ikke kan skrives på formen $K_1\#K_2$ for to andre knuder K_1,$K_2 \not\simeq \bigcirc$. Vi har lige set på, hvordan genus er en knudeinvariant, samt hvordan genus af en knudesum oversættes til de enkelte komponenter. Denne information kan derfor anvendes til at karakterisere, hvornår en knude er en primknude.

Opgave 8.12:
Lad K være en knude. Vis, at hvis $g(K) = 1$, så er K en primknude.

Opgave 8.13:
Det viser sig, at genus af en knude aldrig kan være negativ. Vis, at der ikke eksisterer en invers under knudeaddition. Med andre ord, for enhver knude $K \not\simeq \bigcirc$

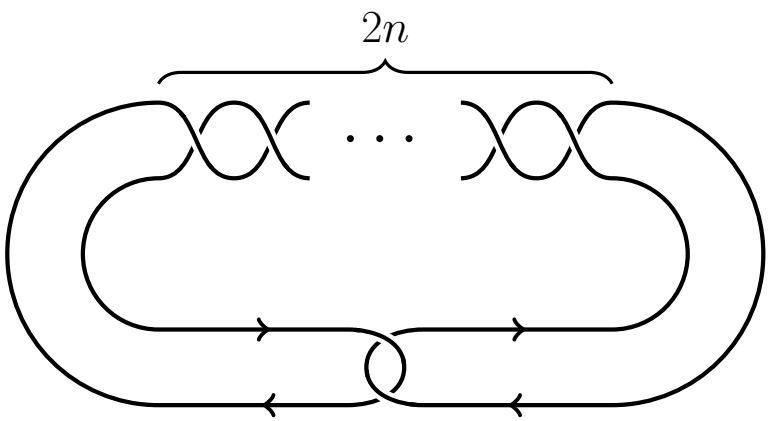
$$\nexists J\colon K\#J \simeq \bigcirc.$$

Opgave 8.14:
Vis, at

$$K \simeq K_1\#K_2\#\cdots\#K_r$$

for enhver knude K, hvor $g(K) \geq 2$ og K_1,K_2,$\ldots$,K_r er primknuder. Her siges K at have en *primknudeopløsning*. Kommenter på lighederne mellem primknudeopløsning og primtalsopløsning.

Opgave 8.15:
Betragt nedenstående orienterede knude, som vi vil kalde $(2n+2)_1$ for $n \geq 1$.



a) **(Valgfri)** Vis, at Conway-polynomiet (se Opgave 6.17) af $(2n+2)_1$ er $\nabla_{(2n+2)_1}(z) = 1 - nz^2$.

b) Argumenter ud fra a), at $(2n+2)_1 \not\simeq (2m+2)_1$ for $n \neq m$.

c) Anvend Seiferts algoritme og find et generelt udtryk for $g(\Sigma_{(2n+2)_1})$.

d) Vis, at der eksisterer uendelig mange primknuder.

Til den sidste opgave i dette projekt skal vi bruge et resultat, som desværre er alt for omfattende at vise her.

Definition 8.14. Lad $f \in \mathbb{Z}[X,X^{-1}]$ være et Laurentpolynomium. Da bruger vi følgende notation:

- $M(f)$ er den største potens i f.
- $m(f)$ er den laveste potens i f.
- *Spændet* af f defineres som $\text{span}(f) = M(f) - m(f)$.

Definition 8.15. Et diagram af en kæde siges at være

- alternerende: hvis krydsningerne langs hver komponent skiftevis er over- og underkrydsninger.
- reduceret: hvis det ikke er muligt at danne et ækvivalent diagram ved brug af Reidemeister-trækkene, som har færre krydsninger.
- sammenhængende: hvis der ikke eksisterer et ækvivalent diagram hvor man kan adskille kædens komponenter med en linje.

Eksempel 8.16. Alle knudediagrammer er selvfølgelig sammenhængende, fordi de kun har én komponent. Desuden er diagrammerne af primknuderne (se Definition 4.7) altid reduceret. Alle knuder op til 7 krydsninger er alternerende. Dog er knuderne 8_{19}, 8_{20} og 8_{21} ikke alternerende. ∘

Sætning 8.17. Lad L være en orienteret kæde med et sammenhængende diagram D med n krydsninger. Da vil

$$\text{span}\,(V(L)) \leq n \tag{3.39}$$

med lighed, hvis og kun hvis, D er alternerende og reduceret.

Opgave 8.16:
Betragt kringlen $P(p,q,r)$ på Figur 3.14 fra Opgave 6.7.

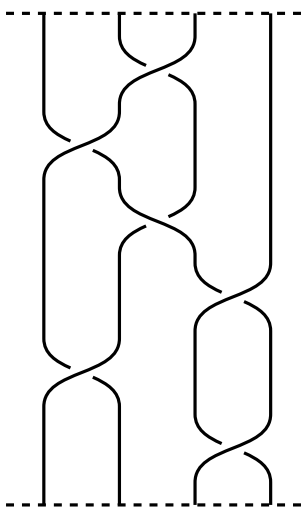
a) Vis, at når p, q og r er ulige, så er $P(p,q,r)$ en primknude.

b) Benyt Sætning 8.17 om spændet af Jones-polynomiet for en alternerende knude til at vise, at knuderne $P(3,5,r)$, for ulige r, alle er forskellige.

9 Projekt: Fletninger og Brunniske kæder

Dette projekt handler ikke nødvendigvis om knuder, men rettere om nogle matematiske objekter, som kan transformeres om til dem. Formålet er at introducere til konceptet om *fletninger*, som viser sig at være en nyttig og alternativ måde at løse problemer på inden for knudeteori. Derudover vil vi se på, hvordan vi kan bruge fletninger til problemet ophængning af billeder.

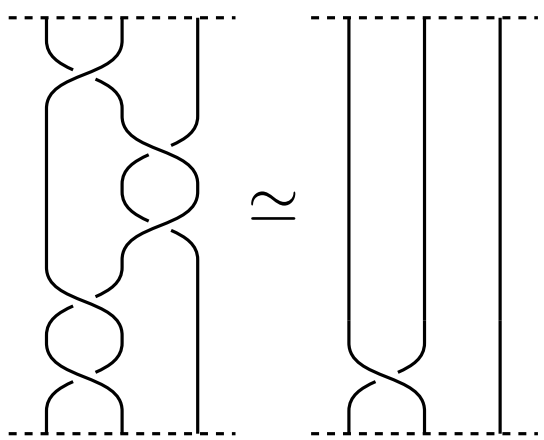
En *fletning* er en konstruktion af n strenge, som er limet fast på en vandret stolpe for oven og for neden (se Figur 3.17). Hver streng er altid rettet nedad, når vi bevæger os fra toppen og mod bunden. En anden måde at se dette på er, at en streng altid vil skære en horisontal linje mellem de to stolper, præcis én gang!



Figur 3.17: Eksempel på en kæde med 4 strenge.

Når vi tegner fletninger, skal der ligesom for knudediagram-

mer altid være information om, hvordan strengene krydser, og diagrammet skal være entydigt. Det bør derfor ikke være en særlig stor overraskelse, at vi kan knytte vores definitioner om ækvivalens af knudediagrammer til fletninger.



Figur 3.18: Eksempel på to fletninger som er ækvivalente med hinanden.

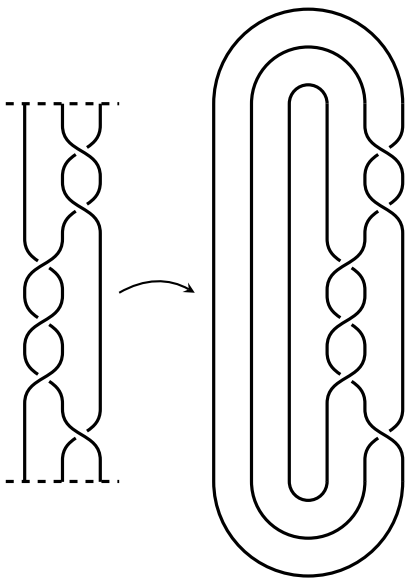
Sætning 9.1. Fletninger kan transformeres ved brug af Reidemeister-trækkene $R2$ og $R3$. To fletninger er ækvivalente, hvis den ene kan omformes til den anden med et endeligt antal Reidemeister-træk.

Opgave 9.1:
Argumenter for, hvorfor det ikke er muligt for en streng at krydse sig selv i en fletning.

Opgave 9.2:
Hvorfor kan fletninger ikke transformeres ved brug af $R1$?

Men hvad har fletninger at gøre med knuder og kæder? Forestil dig at vi trækker den nederste stolpe rundt og limer den fast på den øverste, så de resulterende strenge danner

en knude eller kæde. Hvis der eksisterer en orientering, så vi altid kan bevæge os i urets retning langs knuden eller kæden, siger vi, at den har en *lukket fletningsrepræsentation*.



Figur 3.19: Den lukkede fletningsrepræsentation af en kæde konstrueres fra en fletning ved at forbinde top og bund.

Sætning 9.2 (Alexanders Sætning)**.** Enhver orienteret kæde har en lukket fletningsrepræsentation.

Definition 9.3. Lad L være en vilkårlig kæde. *Fletningsindekset* $b(L)$ er det mindste antal strenge i en fletning, som er nødvendigt for at danne en lukket fletningsrepræsentation af L.

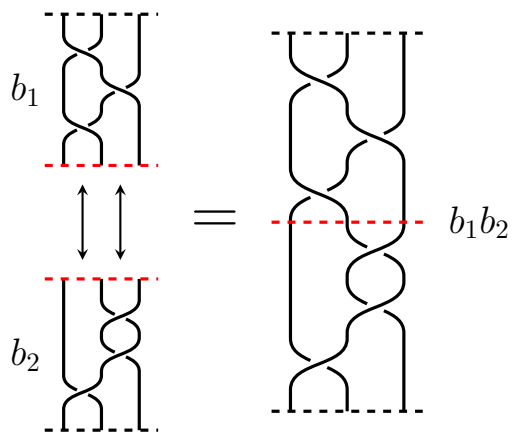
Opgave 9.3:
Bestem

a) kæde(r) L med $b(L) = 1$.

b) (eller beskriv) alle kæder L med $b(L) = 2$.

Opgave 9.4:
Argumenter for, hvorfor $b(L)$ er en invariant af L.

Det viser sig faktisk, at der er mange flere sammenhænge mellem fletningsindekset og fletningens associerede kæde. I Afsnit 8 beskrives konceptet om antallet af Seifert-cirkler for et kædediagram, som fås, når man udjævner diagrammet, så der ikke længere er nogle krydsninger. Shuji Yamada viste, at fletningsindekset af en kæde er lig det mindste antal af Seifert-cirkler over alle diagrammer af kæden. Ligeledes viste Yoshiyuki Ohyama, at hvis L er en sammenhængende kæde (se Definition 8.15), så er antallet af krydsninger n relateret til fletningsindekset ud fra uligheden $n \geq 2b(L) - 2$.



Figur 3.20: Produktet af to fletninger.

Antag, at B_n er mængden af alle fletninger med n strenge (som vi fra nu af vil kalde for en *n-fletning*). For to elementer i B_n, det vil sige to n-fletninger b_1 og b_2, er det muligt at danne et *produkt* b_1b_2 af b_1 og b_2. Dette gøres ved at lime den

ene fletning på enden af den anden. Ligeledes kan vi definere produktet b_2b_1, hvor fletningerne blot er limet sammen i modsat rækkefølge. Generelt er det ikke nødvendigvis sandt, at $b_1b_2 = b_2b_1$. **Opgave 9.5:**
Vis, at fletningsproduktet er associativt. Altså, at hvis b_1, b_2 og b_3 er fletninger, så er

$$(b_1b_2)b_3 = b_1(b_2b_3).$$

Opgave 9.6:
Bestem det 'neutrale element' for fletningsmultiplikation. Med andre ord, find en n-fletning e, så $be = eb = b$ for en arbitrær n-fletning b. Denne fletning kaldes også for den *trivielle fletning*.

Opgave 9.7:
Tegn en vilkårlig fletning b og den samme fletning men spejlet på den horisontale akse. Lad os kalde denne b^{-1}. Vis, at $b^{-1}b = e$ og $bb^{-1} = e$. Argumenter for, at alle fletninger har en "invers".

Opgave 9.8:
Argumenter for, at mængden af alle n-fletninger B_n i virkeligheden er en gruppe med fletningsprodukt som operation. Vi vil kalde B_n for *n-fletningsgruppen*.

Lad os bevæge os lidt i dybden med strukturen af disse fletningsgrupper. Først og fremmest har 1-fletningsgruppen B_1 kun ét element – nemlig den trivielle fletning – så $B_1 = \{e\}$. **Opgave 9.9:**
Hvorimod en 1-fletning ikke kan have nogle krydsninger, så kan elementerne i B_2 godt. Men vi ved, at det altid er mellem de samme to, og eneste, strenge.

a) Vis, at to 2-fletninger er ækvivalente, hvis og kun hvis, tallet $n_h - n_v$ er ens for dem begge, hvor n_h og n_v er henholdsvis antallet af højre og venstre krydsninger.

b) Vis derfra, at der findes uendelig mange ikke-ækvivalente 2-fletninger.

Vi vil gerne kunne beskrive en fletning uden, at vi er nødt til at tegne den. Det viser sig at være smart at skrive en fletning som en sekvens, der beskriver

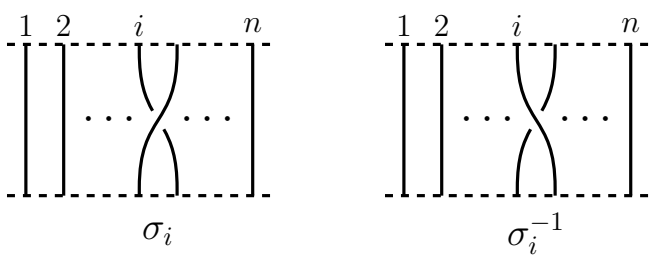
- hvilke strenge, som krydser hinanden,
- i hvilken rækkefølge, strengene krydser hinanden,
- og hvorvidt hver enkelt krydsning er en højre- eller venstrekrydsning.

To strenge kan kun krydse hinanden hvis de er naboer. Forestil dig derfor en n-fletning, hvor vi nummererer strengene fra venstre mod højre med tallene $1, \ldots, n$. Herfra indfører vi følgende notation

σ_i: Venstre krydsning mellem streng i og $i+1$

σ_i^{-1}: Højre krydsning mellem streng i og $i+1$

hvor $i = 1, \ldots, n-1$. Vi kan nu bruge denne notation til at danne ethvert element i en fletningsgruppe.



σ_i $\quad$ σ_i^{-1}

Eksempel 9.4. Fletningen på Figur 3.17 kan skrives på formen $b = \sigma_2\sigma_1\sigma_2^{-1}\sigma_3\sigma_1\sigma_3$. ∘

Man kan altså repræsentere enhver fletning ud fra et endeligt produkt af σ_i og σ_i^{-1}. Dette kalder vi også *ordet* for en fletning. Af den grund siges fletningerne $\sigma_1,\sigma_2,\ldots,\sigma_{n-1}$ også at være *frembringere* af fletningsgruppen B_n.

Opgave 9.10:
Tegn 5-fletningen givet ved ordet $\sigma_1\sigma_2\sigma_3\sigma_2^{-1}\sigma_4\sigma_1^{-1}$.

Opgave 9.11:
Find ordet af en fletning, så den lukkede fletningsrepræsentation giver trekløverknuden.

Opgave 9.12: Svær, valgfri
Vis, at den lukkede fletningsrepræsentation af n-fletningen $(\sigma_1\sigma_2\cdots\sigma_{n-1})^m$ er en knude, hvis og kun hvis, n og m er indbyrdes primiske.

Opgave 9.13:
Vis for en vilkårlig n-fletning, at

a) $\sigma_i^{-1}\sigma_i = \sigma_i\sigma_i^{-1} = e$,

b) $\sigma_i\sigma_{i-1}\sigma_i = \sigma_{i-1}\sigma_i\sigma_{i-1}$,

hvor $2 \leq i \leq n-1$, og at disse svarer til Reidemeister trækkene $R2$ og $R3$.

Opgave 9.14:
Vis, at $\sigma_i\sigma_j = \sigma_j\sigma_i$, hvis og kun hvis, $|i-j| \geq 2$.

Ved hjælp af resultaterne fra Opgave 9.13 og 9.14 kan vi skrive B_n ved brug af frembringerne $\sigma_1,\sigma_2,\ldots,\sigma_{n-1}$:

$$B_n = \left(\sigma_1,\sigma_2,\ldots,\sigma_{n-1}\middle|\begin{array}{cc}\sigma_i\sigma_j = \sigma_j\sigma_i & (|i-j|\geq 2)\\ \sigma_i\sigma_{i-1}\sigma_i = \sigma_{i-1}\sigma_i\sigma_{i-1} & (i = 1,2,\ldots,n-1)\end{array}\right). \tag{3.40}$$

Højre side af ligningen kaldes *repræsentationen* af B_n. **Opgave 9.15:**
Vis, at relationerne

a) $\sigma_{i-1}\sigma_i\sigma_{i-1}^{-1} = \sigma_i^{-1}\sigma_{i-1}\sigma_i$

b) $\sigma_i\sigma_{i-1}^{-1}\sigma_i^{-1} = \sigma_{i-1}^{-1}\sigma_i^{-1}\sigma_{i-1}$

gælder for enhver n-fletning, hvor $2 \leq i \leq n-1$.

Opgave 9.16:
Vis, at fletningerne b_1,$b_2 \in B_3$ beskrevet med ordene

$$b_1 = \sigma_1\sigma_2^2\sigma_1^{-1}\sigma_2^{-1}\sigma_1^2\sigma_2 \text{ og}$$
$$b_2 = \sigma_2^{-1}\sigma_1^4\sigma_2$$

er ens.

Ægte fletninger og at hænge billedrammer med søm

Hvis man hænger en billedramme i et stykke snor bundet om to søm og derefter fjerner et af sømmene, kan man måske forestille sig, at billedet stadig hænger på det andet søm? Dette er i hvert fald sandt, hvis man hænger billedet på den åbenlyse måde som vist på Figur 3.21. Spivak stillede i 1997 spørgsmålet om, hvorvidt det er muligt at hænge en billedramme på n søm, så hvis man fjerner ét vilkårligt søm, så falder rammen ned.

Figur 3.21: Til venstre ses den normale måde, som man ville hænge en billedramme op med to søm. Til højre ses en konstruktion, så rammen falder ned lige meget hvilket et af de to søm, man fjerner.

Sillke og Schwärzler observerede, at de Borromeiske ringe giver en løsning for $n = 2$, og at den generaliserede form af de Borromeiske ringe løser problemet for alle n. Resten af dette projekt vil gå på at bruge fletninger og fletningsnotation til at karakterisere de kæder, som "falder fra hinanden", når vi fjerner en komponent.

Definition 9.5. En n-fletning er *ægte*, hvis dens lukkede fletningsrepræsentation er en kæde med n komponenter.

Definition 9.6. Mængden af alle n-ægte fletninger P_n kaldes den *ægte fletningsgruppe* og er en undergruppe af fletningsgruppen $P_n \subset B_n$.

Lad os prøve at overveje, hvad det betyder for n-fletningen, hvis dens lukkede fletningsrepræsentation også har n komponenter. Hver streng i fletningen kan kun være en del af én komponent, og generelt er det muligt for flere strenge at

være en del af den samme komponent. Det vil sige, at antallet af komponenter i den lukkede fletningsrepræsentation har *maksimum* n komponenter. Hvis der er præcis n, så må det betyde, at ingen af strengene er fælles om en komponent. Fordi den lukkede fletningsrepræsentation fås ved at forbinde top og bund af fletningen, så skal den i'te indgang fra toppen være den samme streng som den i'te udgang fra bunden.

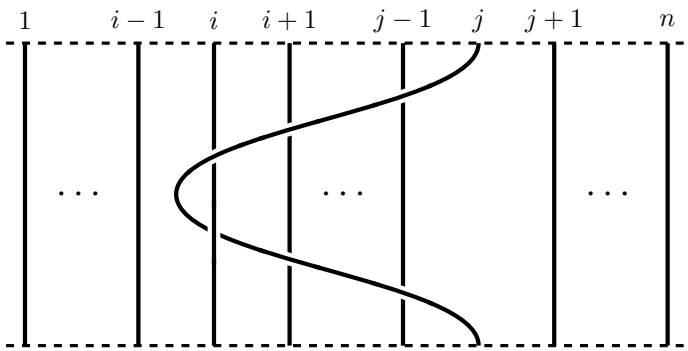
Hvad vil det betyde for frembringerne af P_n? Bemærk, at σ_i bytter rundt på to nabostrenge. Men σ_i kan tydeligvis ikke være en frembringer af den ægte fletningsgruppe, fordi den ikke bevarer strengenes rækkefølge. σ_i^2 er dog derimod en gyldig operation, fordi den bytter rundt på strengene to gange, og dermed bringer dem tilbage til deres originale rækkefølge.

Sætning 9.7. Den ægte fletningsgruppe P_n er frembragt af fletningerne

$$p_{ij} = \sigma_{j-1}\sigma_{j-2}\cdots\sigma_{i+1}\sigma_i^2\sigma_{i+1}^{-1}\cdots\sigma_{j-2}^{-1}\sigma_{j-1}^{-1}, \tag{3.41}$$

hvor $1 \leq i < j \leq n$.

Kort fortalt virker p_{ij} ved at binde den j'te streng rundt om den i'te streng ved at trække den hen over alle andre mellem dem. Dette er illustreret på Figur 3.22.



Figur 3.22: Frembringeren af den ægte fletningsgruppe.

Opgave 9.17:
Tegn eksempler på fletninger p_{ij} for forskellige værdier af i og j. Overbevis dig selv om, at de er ægte, og at deres lukkede fletningsrepræsentationer ikke er trivielle.

Opgave 9.18: Artins semidirekte produktdekomposition
Vælg som eksempel fire tal i,j,k,l, hvor $1 \leq i < j < k < l \leq n$, og tjek, at følgende relationer gælder:

a) $p_{ij}p_{ik}p_{jk} = p_{ik}p_{jk}p_{ij} = p_{jk}p_{ij}p_{jk}$,

b) $p_{ij}p_{kl} = p_{kl}p_{ij}$ og $p_{il}p_{jk} = p_{jk}p_{il}$,

c) $p_{ik}(p_{jk}^{-1}p_{jl}p_{jk}) = (p_{jk}^{-1}p_{jl}p_{jk})p_{ik}$.

Definition 9.8. Lad $S \subseteq N = \{1,2,\ldots,n\}$. En n-ægte fletning $P \in P_n$ er *monisk* i en mængde S, hvis $(n-1)$-fletningen, som man får ved at fjerne den s'te streng for ethvert $s \in S$, er ækvivalent med den trivielle $(n-1)$-fletning e_{n-1}. Hvis $S = N$ er P *fuldkommen monisk*. Med andre ord "falder fletningen fra hinanden", når man fjerner en vilkårlig streng i P.

Opgave 9.19:
Vis, at $p_{ij} \in P_n$ og $p_{ij}^{-1} \in P_n$ er moniske i mængden $\{i,j\}$ for alle $1 \leq i < j \leq n$.

Definition 9.9. En n-kæde $L = C_1 \sqcup C_2 \sqcup \cdots \sqcup C_n$ er *Brunnisk*, hvis $L \setminus C_i \simeq \bigcirc^{n-1}$, hvor $i = 1,2,\ldots,n$ og $\bigcirc^{n-1}$ er ikke-kæden med $n-1$ komponenter.

Opgave 9.20:
Argumenter for, at alle kæder med to komponenter er Brunniske.

Opgave 9.21:
Har du set en Brunnisk 3-kæde tidligere? I så fald, hvad er den? *(HINT: Det har du...)*

Opgave 9.22:
Vis, at den lukkede fletningsrepræsentation af en fuldkommen monisk n-fletning er en Brunnisk n-kæde.

Opgave 9.23:
Lad os definere kommutatoren $[x,y] = x^{-1}y^{-1}xy$. Vis, at $[p_{ij},p_{kl}] \in P_n$ er monisk i mængden $\{i,j,k,l\}$ for alle $1 \leq i < j \leq n$ og $1 \leq k < l \leq n$.

Opgave 9.24:
Er følgende fletninger fuldkommen moniske?

a) $p_{13} \in P_3$

b) $[p_{13},p_{24}] \in P_4$

c) $[p_{12},p_{13}] \in P_4$

d) $[p_{12},p_{13}] \in P_3$

e) $[[p_{12},p_{13}],p_{14}] \in P_4$

f) $[[[p_{12},p_{23}],p_{34}],[p_{45},p_{56}]] \in P_6$

Lad os nu anvende alt den viden, som vi har lært om moniske fletninger og Brunniske kæder, til at løse problemet om at hænge billedrammer op med søm. For kort at opsummere hvad det går ud på, handler det om, at vi skal hænge en billedramme i et stykke snor om n søm således, at hvis man fjerner et vilkårligt søm, så falder rammen ned. Med det samme ser vi symmetrien mellem at fjerne søm og at fjerne strenge/komponenter i moniske fletninger/Brunniske kæder.

Vi kan derfor konstruere billedramme-problemet som en fletning ved at betragte hvert søm som en streng, der strækker sig vinkelret på papirets plan.

Opgave 9.25:
Find løsningen på billedramme-problemet med 2 søm ved at bestemme en fuldkommen monisk 3-ægte fletning. Test dit resultat ved enten at tegne fletningen eller bruge to arme og et stykke snor. *(Hint: Kun den tredje streng må passere over og under de andre)*

Opgave 9.26:
Skriv fletningsordene udtrykt i frembringerne p_{ij} for de fletninger, der løser følgende billedramme-problemer:

a) 3 søm

b) 4 søm

c) 5 søm

d) 4 søm og 2 billedrammer

Opgave 9.27:
Vis, at ordet

$$\Big[\Big[\cdots\Big[\Big[\,[p_{1n},p_{2n}]\,,p_{3n}\Big],p_{4n}\Big],\cdots p_{(n-2)n}\Big],p_{(n-1)n}\Big]$$

giver en fletning, der løser problemet for $n-1$ søm. Argumenter også for, at der findes $(n-1)!$ forskellige løsninger på sådan en form.

Kombinatorisk Spilteori 4

1 Hvilke spil kigger vi på?

I kombinatorisk spilteori arbejder man med spil, der falder indenfor følgende kriterier:

- **2 personer:** Vi kigger udelukkende på spil for to personer, der skiftes til at foretage træk. Konventionen indenfor kombinatorisk spilteori er at kalde de to spillere for "Venstre" og "Højre".
- **Deterministisk:** Der indgår ingen elementer af tilfældighed i spillet - spillets udvikling er fastlagt udelukkende ud fra spillernes valg. Terningkast eller tilfældigt blandede kortbunker er eksempler på spilelementer, som ikke indgår i et deterministisk spil.
- **Fuld information:** Alle spillere sidder med al information om spillets tilstand og om alle måder hvorpå spillet kan udvikle sig. Hvis spillere sidder med skjulte kort eller brikker på hånden, er der så ikke tale om et spil med fuld information.

Ludo og Matador er eksempler på spil med fuld information, men de er ikke deterministisk (og kan desuden have mere end 2 spillere). Spillet Sænke Slagskibe er et deterministisk spil for 2 personer, men spillere har ikke fuld information (hvis

de havde ville det også gøre spillet en del kedeligere). Af 2-personersspil, som rent faktisk er deterministiske og med fuld information, er der for eksempel Skak, Dam, Hex og Go.

Det ville være for vidtgående for denne Matematik Camp at skulle se på alle disse spil, der falder indenfor disse kategorier af spil, så vi indskrænker det yderligere:

- **Den, der ikke kan trække, har tabt:** Når en spiller får deres tur og ikke kan foretage et gyldigt træk, har spilleren tabt. Dette er desuden den eneste måde hvorpå en spiller kan tabe.

- **Endelighed:** De spil, vi kigger på, skal altid have en afslutning. Uanset hvad spillerne gør, kan et spil ikke fortsætte i uendelighed - så der vil altid være en vinder.

Spil, spilpositioner og regelsæt

I kombinatorisk spilteori benyttes ordet "spil" om mere end bare regelsættet for spillet. Med et "spil" mener vi en specifik spilposition. For et spil G er det desuden givet hvilke mulige træk de to spillere kan foretage fra positionen G. Ethvert af de mulige træk resulterer i en ny spilposition, dvs. et nyt spil.

2 Udfaldsklasser

Vi antager altid at begge spillere spiller optimalt efter at vinde. Hvis der, for eksempel findes en strategi hvormed Venstre kan sikre sig sejren, vil Venstre i sidste ende også være vinderen.

Der er altid én af de to spillere, der fra starten har en vindende strategi. Hvis ingen af de to spillere kunne sikre sig sejre, ville begge kunne undgå at tabe - dvs. begge spillere ville blive ved med at have gyldige træk. Vi ser dog kun på

	Venstre vinder når Venstre starter	Højre vinder når Venstre starter
Højre vinder når Højre starter	$\mathcal{F}$	$\mathcal{H}$
Venstre vinder når Højre starter	$\mathcal{V}$	$\mathcal{A}$

Figur 4.1: De fire udfaldsklasser

endelige spil, så dette kan ikke lade sig gøre. Altså er der altid en spiller, der har en vindende strategi.

For et givet spil G er det interessant at vide hvilken af de to spillere, det har en vindende strategi (og dermed vil vinde spillet). Vinderen kan dog afhænge af om det er Venstre eller Højre, der starter med at trække fra positionen G. Udfaldet af G består altså af to spørgsmål: "Hvem vinder, når Venstre trækker først?" og "Hvem vinder, når Højre trækker først?" Dette giver i alt fire muligheder for udfaldet af G.

Ved at se på udfaldet får vi en naturlig inddeling af alle spil i fire mængder $\mathcal{V}$ (Venstre vinder), $\mathcal{H}$ (Højre vinder), $\mathcal{F}$ (første spiller vinder) og $\mathcal{A}$ (anden spiller vinder).

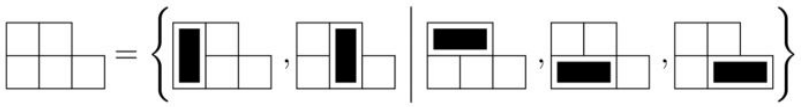
Definition 2.1.

- $\mathcal{V}$ består af alle de spil, hvor Venstre vinder uanset hvem, der trækker først.

- $\mathcal{H}$ består af alle de spil, hvor Højre vinder uanset hvem, der trækker først.

- $\mathcal{F}$ består af alle de spil, hvor den spiller, der trækker først, også er den spiller, der vinder (uanset om spilleren er Venstre eller Højre).

- $\mathcal{A}$ består af alle de spil, hvor den spiller, der trækker først altid taber spillet.



Figur 4.2: Eksempel på brug af mængdenotation for spil.

3 Notation af spil

Det kan være smart at have en standardiseret måde at opskrive spil på – så alle er enige om hvilket spil man taler om. Den første af disse opskrivningsstandarder andvendes i mange formelle definitioner og argumenter. Et spil G er en samling af mulige træk, som hver af de to spillere kan foretage i den spilposition. Ethvert træk fører til et nyt spil.

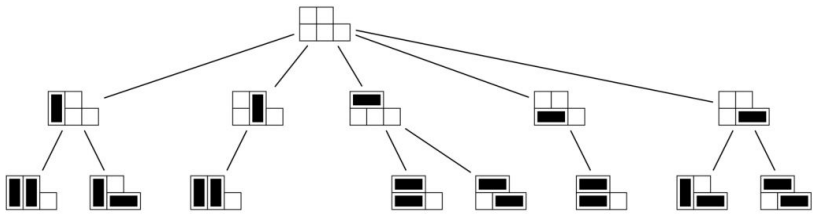
Mængden af spil, som Venstre kan trække til fra G, betegner vi med $\mathcal{G}^V$. På samme måde betegner vi, mængden af spil, som Højre kan trække til fra G, med $\mathcal{G}^H$. Spillet G er altså karakteriseret ved de to mængder $\mathcal{G}^V$ og $\mathcal{G}^H$ af mulige træk for de to spillere.

Spillet G noterer vi derfor på følgende måde ud fra de mulige træk:

$$\begin{aligned} G &= \{ \text{ mulig træk for Venstre } | \text{mulige træk for Højre } \} \\ &= \{\mathcal{G}^V | \mathcal{G}^H\} \end{aligned}$$

Figur 4.2 viser et eksempel på brugen af denne mængdenotation for spil.

Den anden måde hvorpå man noterer et spil G, er som et *spiltræ*. Et spiltræ giver en grafisk oversigt over et spil og alle dets positioner. Øverst i træet placeres selve spillet G. Til venstre nedenfor G placeres de træk som Venstre kan foretage fra G, og til højre nedenfor G placeres de træk som Højre kan foretage. For hver position fortsættes træet derefter nedad med de træk spillerne kan foretage fra positionen (igen med



Figur 4.3: Eksempel på et komplet spiltræ

Venstres træk til venstre og Højres til højre). Dette fortsættes indtil man har et forgrenet træ med alle de måder spillet kan udvikle sig - træet starter øverst med det oprindelige spil, og stopper nederst med alle de mulige slutpositioner (hvor ingen af spillerne kan trække). I figur 4.3 ses spiltræet for et konkret Dominering-spil.

4 De fire simpleste spil

Det simpleste spil er spillet 0, hvor ingen af spillerne kan trække. Dette spil hører naturligvis til klassen $\mathcal{A}$, da den første spiller taber øjeblikkeligt.

I klassen $\mathcal{V}$ er det simpleste spil, det spil, hvor Venstre kan trække til 0 og Højre ikke kan trække, altså spillet noteret som $\{0|\}$. Dette spil betegnes gerne 1. Helt tilsvarende er det simpleste spil i klassen $\mathcal{H}$ er spillet $-1 := \{|0\}$.

Endelig er det simpleste spil i klassen $\mathcal{F}$ er spillet $\{0|0\}$ hvor begge spillere kan trække til 0. Dette spil betegnes $*$ (udtales "stjerne").

5 Spiltræer og udfaldsklasser

Når man har tegnet det komplette spiltræ for et spil, kan man bestemme udfaldsklassen for spillet ved at arbejde sig

nedefra og op igennem træet.

For det første hører alle positionerne nederst i træet til klassen $\mathcal{A}$ da ingen af spillerne kan trække. Udfaldsklassen af en position højere oppe i træet kan afgøres ved at se på udfaldsklasserne af de mulige træk fra positionen.

Når man skal afgøre, hvem der vinder, når Venstre trækker først, ser man på udfaldsklasserne af Venstres mulige træk. Hvis Venstre kan trække til en position, hvor Højre taber, når han er i trækket, vinder Venstre. Venstre vinder altså hvis mindst et af deres træk tilhører $\mathcal{V}$ eller $\mathcal{A}$. Alternativt ligger samtlige Venstres træk i klasserne $\mathcal{H}$ eller $\mathcal{F}$. Dette dækker også muligheden at Venstre ingen træk har, og i det tilfælde kan Venstre ikke undgå at Højre vinder.

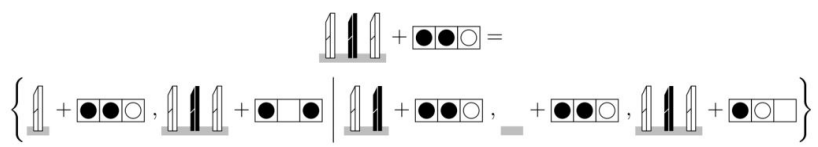
Tilsvarende kan man afgøre, hvem der vinder, når Højre starter ved at se på udfaldsklasserne af Højres mulige træk. Hvis Højre har mindst ét træk i $\mathcal{H}$ eller $\mathcal{A}$, vinder Højre. Alternativt ligger alle Højres træk i klasserne $\mathcal{V}$ eller $\mathcal{F}$ og her vinder Venstre.

Ved at kombinere disse to iagttagelser, finder man udfaldsklassen af en position ud fra de mulige træk fra positionen.

6 Addition af spil

Det sker ofte i løbet af et spil, at spillet spalter op i mindre dele, der ikke påvirker hinanden. I spillets videre forløb kan spillerne så kun trække i et enkelt af delspillene, når de har tur. Dette giver anledning til at definere summen af spil: Et spil i situationen ovenfor siges at være "summen" af de enkelte delspil.

Definition 6.1. Lad G og H være to spil. Sumspillet $G+H$ fungerer da på følgende måde: Når en spiller har tur, skal



Figur 4.4: En sum af to spil.

spilleren foretage enten et træk i G eller et træk i H, men ikke begge dele.

De mulige træk for Venstre i spillet $G+H$ er altså: G^V+H, hvor G^V er et Venstre-træk i G eller $G+H^V$, hvor H^V er et Venstre-træk i H. Situationen er tilsvarende for Højre.

I figur 4.4 ses en konkret sum af en positionen i Clobber og en position i Pushover.

7 Nulspil

Spillene i udfaldsklassen $\mathcal{A}$ opfører sig interessant i forhold til addition af spil:

Sætning 7.1. For ethvert spil $N \in \mathcal{A}$, gælder der at G og $G+N$ er i samme udfaldsklasse uanset spillet G. Det vil sige, at uanset hvem der starter, vil G have samme udfald som $G+N$.

Bevis. Antag at Venstre vinder spillet G. I spillet $G+N$ spiller Venstre som udgangspunkt efter sin vindende strategi i G. Hvis Højre på et tidspunkt trækker i N, svarer Venstre med den vindende strategi for anden spiller i N.

Fordi Venstre hele tiden trækker som anden spiller i N, kan Venstre svare på ethvert træk Højre foretager i N. Da Venstre har en vindende strategi i G, kan Venstre også svare på ethvert træk Højre foretager i G. Derfor må det være Venstre, der vinder i $G+N$.

Tilsvarende ser vi at hvis Højre vinder i G, vinder Højre i $G + N$. □

Dette resultat fortæller os, at det i bund og grund ikke gør nogen forskel, hvis man adderer med et spil fra $\mathcal{A}$. Dette er den samme egenskab som tallet 0 har i normal regning. Af den grund kalder vi spillene i klassen $\mathcal{A}$ for *nulspil*.

8 Negationen af et spil

De tal vi normalt arbejder med, altså hele tal eller reelle tal, har følgende egenskab: Til ethvert tal x findes et specielt tal, som vi kalder "negationen af x", og vi bruger notationen $-x$ for dette tal. De to tal x og $-x$ har da egenskaben at $x + (-x) = 0$.

Der gælder noget tilsvarende for spil. Vi skal nemlig nu se på, at der til ethvert spil G findes et spil, som vi kalder $-G$, sådan at $G + (-G)$ er et nulspil, dvs. $G + (-G) \in \mathcal{A}$.

Definition 8.1. Lad G være et spil. Negationen af G betegnes $-G$ og er fastlagt på følgende vis.

Spillet $-G$ spilles præcist som spillet G bortset fra, at de to spillere bytter roller. Hvis Højre kan trække fra G til H, kan Venstre trække fra $-G$ til $-H$ (idet spillerne også bytter roller i alle efterfølgende træk).

Vi kan også se $-G$, som at vi tager spiltræet for G og spejler det - herved fås spiltræet $-G$.

Udfaldsklassen for $-G$ er let at bestemme ud fra udfaldsklassen for G. Hvis Venstre vinder i G, når de er i trækket, vil Højre vinde i $-G$ når de er i trækket. Tilsvarende ser vi, at hvis Venstre vinder i G, når Højre er i trækket vil Højre vinde i $-G$, når Venstre er i trækket. Dermed haves det at hvis $G \in \mathcal{V}$, må $-G \in \mathcal{H}$. Analogt gælder der at

$$G \in \mathcal{H} \Rightarrow -G \in \mathcal{V}, \quad G \in \mathcal{F} \Rightarrow -G \in \mathcal{F}, \quad G \in \mathcal{A} \Rightarrow -G \in \mathcal{A}.$$

Med denne definition gælder det altid at $G + (-G)$ er et nulspil, dvs. anden spiller vinder. Hvis første spiller trækker i G, laver anden spiller blot det tilsvarende træk i $-G$. Med denne symmetri-strategi vil anden spiller vinde med sikkerhed, så $G + (-G)$ er et nulspil.

Bemærkning 8.2. På samme måde som med normale tal, skriver vi $G - H$ i stedet for $G + (-H)$.

9 Lighed af spil

For normale tal gælder der at $x = y$ netop når $x - y = 0$. Vi definerer lighed af spil på følgende måde:

Definition 9.1. Vi siger at to spil G og H er lig hinanden (skrives $G = H$) hvis de opfylder at $G - H$ er et nulspil - dvs $G - H \in \mathcal{A}$

Denne lighed vi har defineret er en ækvivalensrelation, hvilket vil sige at relationen opfylder følgende egenskaber:

- **Refleksivitet:** For ethvert spil G gælder der at $G = G$.
- **Symmetri:** Hvis $G = H$ gælder der også at $H = G$.
- **Transivitet:** Hvis $G = H$ og $H = K$, så gælder der også at $H = K$.

Hvis to spil opfylder $G = H$, vil de i langt af de fleste sammenhænge opføre sig fuldkommen ens:

Sætning 9.2. Vi kigger på sammenspillet mellem $+$, $-$ og $=$:

- Hvis $G = H$, er G og H i samme udfaldsklasse.
- G er et nulspil hvis og kun hvis $G = 0$. Her et 0 spillet, hvor ingen af spillerne kan trække.

- Hvis $G = H$, gælder der at $G + K = H + K$ for alle spil K - specielt har $G + K$ og $H + K$ samme udfald.
- Hvis $G = H$, har vi også $-G = -H$.
- Der gælder altid at $-(-G) = G$.
- Vi har at $-(G + H) = -G - H = (-G) + (-H)$

Spil der er lig hinanden er altså for alle praktiske formål ens. Vi vil derfor ofte heller ikke skelne mellem spil, der er lig hinanden; Vi betrager dem som forskellige udgaver af samme spil.

10 Heltallene

Nu har vi et par operationer på spil, og vi har en måde at afgøre om to spil er "ens". Vi skal nu se på en basal, men vigtig klasse af spil.

Spillet 0 er spillet, hvor ingen af spillerne kan trække og vi har tidligere set at 0 er et nulspil.

Spillet 1 defineres til at være spillet, hvor Venstre har et enkelt træk og Højre ikke kan trække. Som vi definerede tidligere har vi $1 := \{0|\}$. Da venstre vinder uanset hvem der starter, har vi $1 \in \mathcal{V}$. Tilsvarende definerer vi for ethvert naturligt tal $n > 0$ spillet n, som spillet, hvor Venstre kan foretage n træk og Højre på intet tidspunkt kan trække. Denne definition kan skrives op som

$$n := \{n - 1| \quad \} \text{ for } n > 0 \text{ og } n \in \mathbb{Z}$$

Ligesom for spillet 1, så har vi at $n \in \mathcal{V}$ for alle $n > 0$. Alle disse spil giver et godt mål for hvornår et spil er n træk værd for Venstre. Hvis $G = n$ kan vi sige at Venstre "har n træk til overs i G".

Vi har naturligvis et tilsvarende begreb for spillene, hvor Højre har et antal træk og Venstre på intet tidspunkt kan trække. Vi kan således bruge de positive tal til at betegne spillene, hvor Venstre vinder og de negative tal til at betegne spillene, hvor Højre vinder.

For et negativt heltal $-n$, lader vi spillet $-n$ være givet ved at Højre kan trække n gange og Venstre aldrig kan trække. Dette kan vi definere på følgende måde

$$-n := \{ \quad | -n+1\} \text{ for } -n < 0 \text{ og } -n \in \mathbb{Z}$$

Vi har naturligvis at $-n \in \mathcal{H}$ for alle de negative heltal.

Man kan nu overveje, hvad der sker, når man lægger heltal-spillene sammen og det viser sig at de opfører sig lige så pænt, som man kunne håbe på:

Sætning 10.1. For ethvert heltal $n \in \mathbb{Z}$, lader vi n betegne heltalsspillet n. Der gælder så, at

- Det negative af et spil $n \in \mathbb{Z}$ er spillet $-n$. Kort sagt er $-(n) = (-n)$.
- Summen af to heltal n,$m \in \mathbb{Z}$ er lig spillet knyttet til tallet $n+m$ (med vores definerede lighedsbegreb).

Når vi regner med heltalsspillene opfører de sig altså fuldstændig ligesom de normale heltal.

11 Fortegn på spil

Heltalsspillene blev defineret sådan, at de positive heltal er de heltal, hvor Venstre vinder og de negative heltal er de heltal, hvor Højre vinder. Dette begreb om positiv og negativ udvider vi nu til at omfatte alle spil:

Definition 11.1.
- G kaldes et *nulspil*, hvis $G \in \mathcal{A}$.

- G kaldes *positivt*, hvis $G \in \mathcal{V}$.
- G kaldes *negativt*, hvis $G \in \mathcal{H}$.
- G kaldes *uldent*, hvis $G \in \mathcal{F}$.

Vi ved allerede at summen af to nulspil igen er et nulspil. Det ses også let at summen af to positive spil giver et positivt spil og på samme måde at summen af to negative spil igen giver et negativt spil. Det tilsvarende gælder dog ikke for uldne spil: Spillet $*$ er uldent, men $* + * = 0$ er et nulspil.

12 Ordning af spil

Nu hvor vi har begreberne *positive* og *negative* spil, ligger det lige for at definere en ordning $>$ af spil. Ligesom vi definerede $G = H$ ved at $G - H$ er et nulspil, definerer vi nu $G > H$ ved

- $G > H \overset{def}{\Leftrightarrow} G - H$ er positiv.
- $G < H \overset{def}{\Leftrightarrow} G - H$ er negativ.

Dette ligner til forveksling den sædvanlige ordning af de reelle tal, hvor der også gælder at $x > y$ hvis $x - y$ er et positivt reelt tal. Til forskel fra de reelle tal, har vi dog spil, der hverken er positive, negative eller 0, nemlig de uldne spil. Det betyder, at der kan finde spil G og H, så der hverken gælder $G < H$, $G > H$ eller $G = H$. Dette forekommer netop, når $G - H$ er uldent og vi siger, da at G er *konfus med* H og det skriver vi $G \parallel H$. Vi har altså

$$G \parallel H \overset{def}{\Leftrightarrow} G - H \text{ er uldent.}$$

En ordning, hvor der altid gælder $x > y$, $x < y$ eller $x = y$, kaldes en *total ordning*. Ordningen af de reelle tal er altså

et eksempel på en total ordning, imens ordningen af spillene ikke er total - det er kun en *partiel ordning*.

Som med den normale ordning af tallene benytter vi det kombinerede symbol $G \geq H$, hvis $G = H$ eller $G > H$. Vi definerer desuden et nyt kombineret symbol $G \rhd H$, som betyder $G > H$ eller $G \parallel H$. Vi har de tilsvarende symboler $\leq$ og $\lhd$. Disse kombinerede symboler har også en simpel karakterisering ud fra $G - H$:

- $G \geq H \Leftrightarrow$ Venstre vinder $G - H$, når Højre starter.
- $G \leq H \Leftrightarrow$ Højre vinder $G - H$, når Venstre starter.
- $G \rhd H \Leftrightarrow$ Venstre vinder $G - H$, når Venstre starter.
- $G \lhd H \Leftrightarrow$ Højre vinder $G - H$, når Højre starter.

Så længe vi holder os til relationerne $=$, $>$ og $<$ opfører det sig "pænt":

Sætning 12.1 (Egenskaber ved ordningen)**.** Følgende resultater gælder også med $\leq$ og $\geq$ i stedet for henholdsvis $<$ og $>$:

- Hvis $G < H$ og $H < K$, så gælder $G < K$.
- Vi har $G < H$ hvis og kun hvis $H > G$.
- Hvis $G < H$ og $K < L$, er $G + K < H + L$.
- Hvis $G < H$, er $-G > -H$.

Man skal passe mere på med $\parallel$, $\lhd$ og $\rhd$. Der findes for eksempel G,H og K, så $G \lhd H$ og $H \lhd K$, men hvor der gælder $K < G$. Der gælder stadig at $G \lhd H$ hvis og kun hvis $H \rhd G$ og hvis og kun hvis $-G \rhd -H$ (og tilsvarende for $\parallel$).

Sammenspil mellem $\geq$ og $+$

Med heltallene har vi at jo større heltallet er, des flere ekstra træk har Venstre. Det viser sig også generelt, at jo større et spil er, des bedre er spillet for Venstre i alle sammenhænge:

Sætning 12.2. Antag at $G \geq H$. Der gælder da for ethvert spil K, at hvis Venstre vinder $H + K$ med en given startspiller, så vinder Venstre også $G + K$ med den samme startspiller.

Det kan altså aldrig skade Venstre, hvis H bliver skiftet ud med G - forudsat at $G \geq H$.

Tilsvarende gælder hvis $G \leq H$, at det aldrig kan skade Højre at der spilles spillet $G + K$ i stedet for spillet $H + K$.

Begrænsning af mulige træk

Ofte kan et spil blive lettere at overskue, hvis man ser bort fra et antal af den ene spillers mulige træk. Lad G og G' være to spil, hvor G' er fremkommet fra G ved at udelukke nogle af Venstres træk-muligheder. Da det aldrig kan være en ulempe at have flere muligheder, må vi forvente at G er mindst lige så godt for Venstre som G', altså at $G \geq G'$.

For at vise $G \geq G'$, skal vi bevise at $G - G' \geq 0$, dvs. at Venstre vinder $G - G'$, når Højre trækker først. Strategien som Venstre kan vinde med, er en simpel symmetri-strategi, for uanset hvad Højre trækker, kan Venstre foretage det tilsvarende træk i den anden summand. Venstre kan ikke komme i problemer på grund af de udelukkede træk, for disse træk er nu blevet udelukkede Højre-træk i $-G'$.

Helt analogt gælder der naturligvis, at hvis G' fremkommer fra G ved at udelade nogle af Højres træk er $G' \geq G$.

I nogle tilfælder kan man endda vise, at der gælder lighedstegn:

Sætning 12.3. (Udeladelse af dominerede træk). Lad der være givet et spil G hvori Venstre har to træk A og B, der opfylder $A \leq B$. Lad G' være det spil, der fremkommer ved at udelade trækket A fra G. Da er $G = G'$.

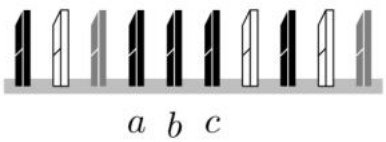
Bevis. For at gøre beviset mere overskueligt antager vi at Venstre netop har de to træk A og B og Højre har netop et træk C. Eventuelt ekstra træk ændrer ikke på bevisførelsen. Vi har altså $G = \{A,B|C\}$ og $G' = \{B|C\}$. Så er $-G' = \{-C|-B\}$ og $G - G' = A,B|C + \{-C|-B\}$. Vi skal vise at dette er et nulspil.

Hvis Højre starter har han to muligheder. Hvis han trækker til C i første summand, kan Venstre trække til $-C$ i anden summand. Da har Venstre trukket til $C + (-C) = 0$ og vundet. Hvis Højre trækker til $-B$ i anden summand, trækker Venstre tilsvarende til B i første summand og vinder derved. Altså vinder Venstre, når Højre starter.

Hvis Venstre starter, har de tre muligheder. Hvis de trækker til $-C$ i anden summand, trækker Højre til C og vinder. Hvis de trækker til B i første summand, trækker Højre til $-B$ og vinder. Hvis de trækker til A i første summand, trækker Højre til $-B$ i anden summand. Positionen er nu $A - B$ og Venstre er i trækket. Men idet $A \leq B$, er $A - B \leq 0$, dvs. $A - B$ er et spil, hvor Højre vinder, hvis Venstre er i trækket. Altså er Højre i en vindende position. Dermed vinder Højre $G - G'$, hvis Venstre starter. □

Den underliggende ide i sætningen er naturligvis at Venstres træk til A er irrelevant, da det altid vil være mindst lige så godt at trække til B. Dermed kan A fjernes uden at ændre på spillets værdi. Helt analogt kan man udelade et af Højres træk A, hvis Højre har et andet træk B, således at $B \leq A$.

Disse to egenskaber kan gøre det muligt at forenkle visse spilpositioner.



Figur 4.5: Eksempel på position i Pushover

Eksempelvis gælder følgende: Lad G være en position i Pushover, der består af en enkelt række af dominobrikker og lad G' være den position, der fremkommer ved at tilføje en sort domino for enden af rækken. Da er $G' \geq G$. Dette er fordi Højres trækmuligheder ikke ændrer sig, når man tilføjer en sort dominobrik, mens Venstres trækmuligheder bliver udvidet.

Det bliver herved let at fjerne en hel del dominerede træk fra Pushover-positioner. Betragt en position i Pushover, der består af en enkelt række og hvori, der optræder et antal sorte dominobrikker lige efter hinanden. Tag foreksempel positionen set i figur 4.5

I denne position har Venstre bland andet de tre mulige træk at vælte enten a,b eller c mod højre. I alle tre tilfælde vil de tre brikker til venstre for a blive stående, mens de fire brikker til højre for c bliver væltet. Den eneste forskel ligger i hvor mange af de tre brikker a,b og c bliver stående. Hvis Venstre vælter a, vil ingen af de tre blive stående, men hvis de vælter b, vil a bliver stående, så trækket at vælte a mod højre er domineret. Tilsvarende ses, at hvis Venstre vælgter c mod højre, vil både a og b blive stående, hvilket er bedre end kun at lade a blive stående. Altså er trækket at vælte b mod højre også domineret, så det eneste af de tre træk, der er værd at undersøge er trækket at vælte c mod højre. Helt tilsvarende kan vi se, at hvis Venstre vil vælte en af de tre brikker mod venstre, vil det altid være bedre at vælte a end

at vælte b eller c.

13 Rationale tal

Vi kan definere spil hørende til alle rationale tal med en 2-potens i nævneren. Vi nøjes med at definere de positive spil, for de negative defineres analogt.

De positive heltal har vi allerede defineret, så vi nøjes med at se på de ikke-hele tal. Enhver positiv brøk med en 2-potens i nævneren kan skrives som $\frac{u}{2^k}$, hvor $u > 0$ er ulige. Det rationale spil $\frac{u}{2^k}$ defineres da ved at spillerne kan rykke $\frac{1}{2^k}$ i hver retning:

$$\frac{u}{2^k} := \left\{ \frac{u-1}{2^k} \middle| \frac{u+1}{2^k} \right\}$$

Fordi u er ulige, kan de to brøker $\frac{u-1}{2^k}$ og $\frac{u+1}{2^k}$ forkortes, så spillerne rykker hele tiden til spil med lavere nævner indtil spillet når et heltal. [1]

Eksempelvis er de rationale spil $\frac{1}{2}$, $\frac{5}{4}$ og $\frac{7}{16}$ givet ved

$$\frac{1}{2} := \{0|1\}, \quad \frac{5}{4} := \left\{1 \middle| \frac{3}{2}\right\}, \quad \frac{7}{16} := \left\{\frac{3}{8} \middle| \frac{1}{2}\right\}$$

Alle disse nye rationale spil opfører sig endnu engang som man kunne ønske: Summen af rationale spil x og y er spillet knyttet til $x + y$. Negationen af et rationalt spil er spillet hørende til negationen af tallet. Et rationalt spil er positivt/nul/negativt netop når det tilhørende tal positivt/nul/negativt.

Bemærk at i ethvert tal er Venstres træk til et lavere tal og Højres træk er til et højere tal. Dette er relateret til et mere generelt resultat: Hvis alle trækkene fra et spil G er tal og alle Venstres træk er mindre end alle Højres træk, så er G selv et tal, der ligger mellem Venstres største og Højres mindste træk.

[1] Dette heltal vil være et af de to heltal nærmest $\frac{u}{2^k}$

14 Spil der ikke er tal

Når nu vi har fået et hav af positive spil, nemlig de positive rationale tal (med 2-potens i nævneren), er det naturligt at spørge sig om alle positive spil er at finde blandt de rationale tal. Som vi skal se, er dette *ikke* tilfældet.

Vi vil vise at spillet $\uparrow := \{0|*\}$ (udtales "pil op") er positivt, men mindre end ethvert positivt rationalt tal. Denne egenskab har et navn - vi siger at $\uparrow$ er *infinitesimalt*.

Definition 14.1. Et spil G kaldes infinitesimalt, hvis $x > G > -x$ for alle positive rationale tal x.

Spillet 0 ses umiddelbart at være infinitesimalt, men der er mange andre infinitesimale spil.

Spillet $*$ er infinitesimalt: Lad $x > 0$ være et rationalt tal. Da skal vi vise at $x > * > -x$. Vi nøjes her med at vise $x > *$, dvs. $x - * > 0$. Vi skal altså se, at Venstre vinder $x - * = x + *$ (idet $-* = *$) uanset hvem der starter. Hvis Venstre starter, kan de rykke fra $x + *$ til x, der er positivt, så Venstre vinder. Hvis Højre starter, kan de enten rykke til x eller til $y + *$, hvor $y > x$. Begge træk taber Højre på, da $y > x > 0$.

Vi har altså fundet et infinitesimalt spil $*$, der ikke er et tal (idet $*$ er uldent og ingen tal er uldne). Spillet $*$ er dog ikke positivt.

Lad os nu se $\uparrow$. Lad $x > 0$ være rationalt; da vil vi vise at $x > \uparrow > 0 > -x$. Det ses hurtigt at $\uparrow > 0$, dvs. at Venstre vinder uanset startspilleren. Vi ser derfor på spillet $x - \uparrow = x + \downarrow$, som vi skal vise at Venstre vinder. Hvis Venstre starter, rykker de til $x + *$, der er positivt, idet $*$ er infinitesimalt. Hvis Højre starter, kan han enten rykke til $x > 0$ eller til $y + \downarrow$, hvor $y > x$. Det efterlader Venstre i trækket i enten et positivt spil x, eller et spil $y + \downarrow$ med $y > x > 0$ - uanset hvad,

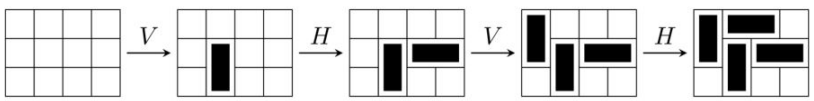
vinder Venstre. Dermed har vi $x > \uparrow > +$ for alle positive tal x, så $\uparrow$ er et infinitesimalt positivt spil (og altså ikke et tal).

15 Regler for spillene

Her præsenterer vi regelsæt for seks topersonersspil. De to spillere betegnes "Venstre" og "Højre". I alle spillene gælder der, at en spiller, der er i trækket, men ikke kan foretage et træk, har tabt.

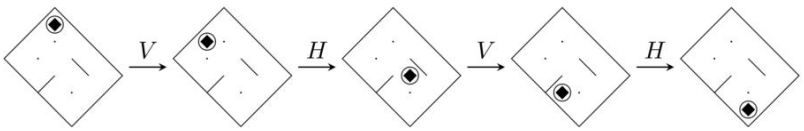
Domineering

Domineering spilles på et rektangulært bræt, hvor nogle af felterne er blokerede. Et træk består i at placere en dominobrik, så den blomerer to nabofelter. Venstre placerer sine brikker lodret, Højre placerer deres vandret. En typisk startposition er et $n \times m$-bræt, hvor alle felter er tomme. Et eksempel på dette spil ses i figuren nedenfor.



Maze

Maze spilles på et rektangulært gitter roteret 45°, hvor nogle kanter er tegnet op. En brik er placeret på et af felterne. Et træk består i at rykke brikken et antal felter i lige linje, uden at den krydser nogle af de optegnede kanter. Venstre rykker nedad og til venstre, Højre rykker nedad og til højre. Et eksempel på dette spil ses i figuren på næste side.

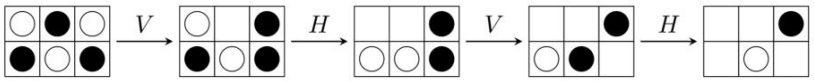


Pushover

En position i Pushover består i et antal rækker af dominobrikker, hvor hver brik er enten sort, hvid eller grå. Et træk består af at vælge en dominobrik og vælte den mod højre eller venstre. Alle dominobrikker, der herved bliver væltet fjernes fra spillet. Venstre må vælte sorte og grå brikker, Højre må vælte hvide og grå brikker. Et eksempel på et spil Pushover ses i figuren nedenfor.

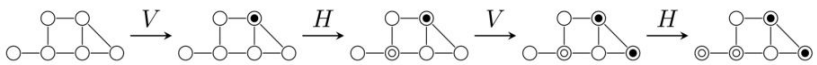
Clobber

Clobber spilles på et bræt med kvadratiske felter, hvor hvert felt kan indeholde en sort eller hvid brik. Venstre spiller sort, Højre spiller hvid. Et træk består i at flytte en af sine egne brikker til et tilstødende felt (vandret eller lodret), som indeholder en af modstanderens brikker. Modstanderens brik fjernes så fra spillet. En typisk startposition er et rektangulært bræt, hvor alle felter indeholder en brik, med farverne lagt som på et skakbræt. Et eksempel på dette spil ses i figuren på næste side.



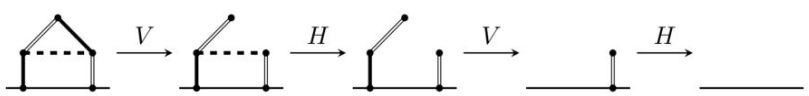
Snort

Snort spilles på en graf, hvor hver knude kan være farvet sort eller hvid. Venstre spiller sort, Højre spiller hvid. Et træk består i at vælge en ufarvet knude og farve den med sin egen farve. Man må ikke farvelægge en knude således at to forbundne knuder får forskellig farve. Et eksempel på spillet Snort kan ses i figuren nedenfor.



Hackenbush

En position i Hackenbush består i en graf, hvis kanter er farvet sort, hvid eller grå (her afbildet som stiplede kanter). Én af knuderne er speciel; den kaldes jorden og tegnes som regel som en lang vandret linje. Et træk består i at fjerne en kant i grafen og derefter fjerne alle dele af grafen, der ikke længere er forbundet til jorden. Venstre ,å fjerne sorte og grå kanter, Højre må fjerne hvide og grå kanter. Ofte anvendes farverne blå, rød og grøn i stedet for sort, hvid og grå. Der ses et eksempel på spillet Hackenbush i figuren nedenfor.



Indeks