# Gruppeteori

Michael Knudsen

8. marts 2005

## 1 Motivation

For at motivere indførelsen af gruppebegrebet begynder vi med et eksempel.

**Eksempel 1.1.** Lad $\mathbf{Z}$ betegne mængden af de hele tal,

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

På $\mathbf{Z}$ har vi noget, vi kalder + (plus). Det er en regneoperation, der til to hele tal $m$ og $n$ knytter et nyt helt tal $m + n$. I mængden $\mathbf{Z}$ er der et tal, der opfører sig specielt. Det er tallet 0, der har egenskaben

$$m + 0 = 0 + m = m \text{ for alle } m \in \mathbf{Z}.$$

Ydermere har ethvert helt tal $m$ et *omvendt* tal, nemlig $-m$, som opfylder

$$m + (-m) = (-m) + m = 0.$$

Sidst men ikke mindst er det ligegyldigt, hvordan vi sætter parenteser, når vi lægger hele tal sammen. Der gælder, at

$$(m + n) + r = m + (n + r)$$

for alle $m, n, r \in \mathbf{Z}$.

Det forekommer måske mærkeligt, at vi i ovenstående eksempel fremhæver en række egenskaber, som vi ganske udmærket kender i forvejen, men prøv alligevel at have eksemplet i baghovedet ved gennemlæsningen af det næste eksempel. Prøv især at lægge mærke til, hvordan de tre centrede ligninger næsten går igen.

**Eksempel 1.2.** Lad $\mathbf{Q}$ betegne mængden af de rationale tal (brøker),

$$\mathbf{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbf{Z}\,, n \neq 0 \right\},$$

og sæt $\mathbf{Q}^\times = \mathbf{Q} \setminus \{0\}$. Det vil sige, at $\mathbf{Q}^\times$ er mængden af alle rationale tal undtagen 0. På $\mathbf{Q}^\times$ har vi regneoperationen $\cdot$ (gange), der til to tal $x, y \in \mathbf{Q}^\times$

knytter et nyt tal $x \cdot y \in \mathbf{Q}^\times$. Der er i $\mathbf{Q}^\times$ et særligt tal, nemlig 1, som har egenskaben

$$1 \cdot x = x \cdot 1 = x \text{ for alle } x \in \mathbf{Q}^\times.$$

Derudover har ethvert tal $x \in \mathbf{Q}^\times$ et *omvendt* tal, nemlig $\frac{1}{x}$, som opfylder

$$\frac{1}{x} \cdot x = x \cdot \frac{1}{x} = 1.$$

Bemærk, at det her er vigtigt, at det er $\mathbf{Q}^\times$, og ikke hele $\mathbf{Q}$, vi betragter. Tallet 0 har nemlig ikke noget omvendt tal. Til sidst bemærker vi, at det er ligegyldigt, hvordan vi sætter parenteser, når vi ganger tal i $\mathbf{Q}^\times$ sammen. Der gælder, at

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

for alle $x, y, z \in \mathbf{Q}^\times$.

Prøv at lade blikket glide ned over de to ovenstående eksempler. Rent typografisk er der ikke meget, der adskiller dem. I det store hele har vi i det andet eksempel blot erstattet $\mathbf{Z}$ med $\mathbf{Q}^\times$ og plus med gange.

## 2 Gruppebegrebet

Vi så i det foregående afsnit, at mængderne $\mathbf{Z}$ og $\mathbf{Q}^\times$ udstyret med henholdsvis $+$ og $\cdot$ havde meget til fælles. Disse observationer vil vi i dette afsnit forsøge at samle sammen i en abstrakt definition, som $\mathbf{Z}$ og $\mathbf{Q}^\times$ er specialtilfælde af.

**Definition 2.1.** Lad $M$ være en mængde. Ved en *sammensætning* på $M$ forstås en tilordning $*$, der til to elementer $a, b \in M$ knytter et nyt element $a * b \in M$.

Bemærk, at vi allerede er stødt på sammensætninger: Regneoperationerne $+$ og $\cdot$ på henholdsvis $\mathbf{Z}$ og $\mathbf{Q}^\times$ er eksempler på sammensætninger.

Vi er nu i stand til at formulere definitionen af en gruppe.

**Definition 2.2.** En mængde $G$ med en sammensætning $*$ kaldes en *gruppe*, hvis følgende tre punkter er opfyldt:

(1) For alle $a, b, c \in G$ er $a * (b * c) = (a * b) * c$.
(2) Der findes et element $e \in G$, så $e * a = a * e = a$ for alle $a \in G$.
(3) For alle $a \in G$ findes et $b \in G$, så $b * a = a * b = e$.

Måske synes denne definition ved første øjekast at være lige lovlig abstrakt, men bemærk lige, hvad det er, vi har gjort: Vi har skåret eksemplerne $\mathbf{Z}$ med $+$ og $\mathbf{Q}^\times$ med $\cdot$ helt ind til benet. Hvis vi sætter $G = \mathbf{Z}$ og lader $*$ betegne $+$, så har vi jo allerede tjekket, at (1), (2) og (3) er opfyldt. Tilsvarende gør sig gældende for $G = \mathbf{Q}^\times$, hvor nu $\cdot$ spiller rollen som $*$.

Ideen med at abstrahere fra konkrete eksempler er et gennemgående tema i matematikken. Man forsøger at skære overflødig information væk i håbet om at skabe klarhed. Når vi beskæftiger os med grupper i den abstrakte forstand, har vi i forhold til eksemplerne $\mathbf{Z}$ og $\mathbf{Q}^\times$ givet afkald på en masse information. Det eneste, vi har beholdt, er spillereglerne (1), (2) og (3), og vi skal ikke længere bekymre os om, hvorvidt vi har med hele tal, brøker eller måske noget helt tredje at gøre. Hvem siger, at det i det hele taget skulle dreje sig om tal? Det står der ikke noget om i definitionen af en gruppe!

I det følgende vil vi med med udtrykket "$(G, *)$ er en gruppe" mene, at $G$ er en gruppe med sammensætning $*$.

Man skal være på vagt, når man beskæftiger sig med grupper i den abstrakte forstand. Mange af de egenskaber, som vi måske har taget for givet for konkrete grupper, er ikke altid så oplagte længere. De er måske oven i købet forkerte! Lad os se, hvor man for eksempel kunne gå galt i byen: Inspireret af eksemplerne $\mathbf{Z}$ og $\mathbf{Q}^\times$ kunne man måske fristes til at tro, at der i en vilkårlig gruppe $G$ med sammensætning $*$ altid gælder, at $a * b = b * a$ for alle $a, b \in G$. Dette er *ikke* tilfældet, og vi vil snart se et eksempel på dette fænomen.

Lad os se på et andet potentielt problem. I eksemplet med $\mathbf{Z}$ er det klart, at 0 er det eneste tal, der kan spille rollen som $e$ i definitionen af en gruppe. Tilsvarende gør sig gældende for tallet 1 i eksemplet med $\mathbf{Q}^\times$. Hvordan mon det forholder sig en vilkårlig gruppe? Punkt (3) siger, at et sådant element skal findes, men der står intet om, at der ikke kan findes flere. Denne gang har vi dog heldet med os.

**Sætning 2.3.** *Lad $(G, *)$ være en gruppe. Da findes præcis ét element $e \in G$, som opfylder $e * a = a * e = a$ for alle $a \in G$.*

*Bevis.* Vi ved i følge punkt (3), at et sådant element findes, så vi skal blot gøre rede for, at der ikke findes flere. Antag derfor, at $f$ opfylder $f * a = a * f = a$ for alle $a \in G$. Vi skal vise, at $f = e$.

Da $f * a = a$ for alle $a \in G$, gælder dette specielt, hvis vi sætter $a = e$.

Altså har vi

$$f * e = e. \tag{2.1}$$

Husk nu, at $e$ opfylder $a * e = a$ for alle $a \in G$. Så gælder det specielt for $a = f$, så vi ser, at

$$f * e = f. \tag{2.2}$$

Altså får vi ved at kombinere ligningerne 2.1 og 2.2, at

$$f = f * e = e.$$

Hermed har vi vist det ønskede. □

På helt tilsvarende vis kan man bevise den følgende sætning. Vi overlader beviset som en øvelse til læseren.

**Sætning 2.4.** *Lad $(G, *)$ være en gruppe, og lad $a \in G$. Da findes præcis ét element $b \in G$, som opfylder $b * a = a * b = e$.*

Vi ved nu, at alle elementer i en gruppe har et entydigt bestemt omvendt element. Det omvendte element af et element $a$ vil vi fremover betegne $a^{-1}$. Vi vil dog i særlige tilfælde, hvor der er tradition for at bruge en anden notation, bruge en anden betegnelse end $a^{-1}$. For eksempel i gruppen $\mathbf{Z}$ med $+$, hvor det er naturligt at skrive $-a$ for det omvendte element af et helt tal $a$.

**Definition 2.5.** Lad $(G, *)$ være en gruppe. En delmængde $H$ af $G$ kaldes en *undergruppe* af $G$, hvis $(H, *)$ er en gruppe.

Lad $(G, *)$ være en gruppe, og lad $H$ være en delmængde af $G$. Hvordan tjekker man, om $H$ er en undergruppe af $G$? Kravet er, at $(H, *)$ er en gruppe, så for det første skal $*$ være en sammensætning på $H$. Altså skal der gælde $g * h \in H$ for alle $g, h \in H$. For det andet skal punkterne (1), (2) og (3) i definitionen af en gruppe være opfyldt. Kravet i punkt (1) er stadig opfyldt, når vi holder os til $H$, så det er kun (2) og (3), der skal tjekkes.

## Øvelser

**Øvelse 1.** Lad $G$ være en gruppe med sammensætning $*$, og lad $a, b, c \in G$ opfylde $a * b = a * c$. Vis, at $b = c$.

**Øvelse 2.** Lad $G$ være en gruppe med sammensætning $*$, og lad $a, b, c \in G$. Vis, at $(a * b)^{-1} = b^{-1} * a^{-1}$.

**Øvelse 3.** En gruppe $G$ kaldes *abelsk*, hvis $a * b = b * a$ for alle $a, b \in G$. Vis, at hvis $G$ er en gruppe, hvor $a * a = e$ for alle $a \in G$, så er $G$ abelsk.

**Øvelse 4.** Lad $(G, *)$ og $(H, \circ)$ være grupper, og lad $G \times H$ betegne det cartesiske produkt af $G$ og $H$. Det vil sige

$$G \times H = \{(g, h) \mid g \in G, h \in H\}.$$

Vis, at $(G \times H, \diamond)$, hvor $\diamond$ er givet ved

$$(g, h) \diamond (g', h') = (g * g', h \circ h'),$$

er en gruppe.

**Øvelse 5.** Lad $n \in \mathbf{Z}$, og sæt $n\mathbf{Z} = \{n \cdot m \mid m \in \mathbf{Z}\}$. Vis, at $n\mathbf{Z}$ er en undergruppe af $\mathbf{Z}$.

**Øvelse 6.** Lad $G$ være en undergruppe af $\mathbf{Z}$. Vis, at der findes et $n \in \mathbf{Z}$, så $G = n\mathbf{Z}$.

**Øvelse 7.** Lad $G = \{a, b\}$ være en mængde med to elementer, og definer en sammensætninger $*$ og $\circ$ på $G$ ved

| $*$ | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $b$ |
| $b$ | $b$ | $a$ |

og

| $\circ$ | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $a$ |
| $b$ | $a$ | $b$ |

og vis, at $(G, *)$ og $(G, \circ)$ er grupper.

Bemærk, at sammensætningerne $*$ og $\circ$ ikke adskiller sig meget fra hinanden. Elementerne $a$ og $b$ har blot skiftet roller.

Prøv med mængder med 3 og 4 elementer og se, om hvor mange sammesætninger, du kan lave på dem. Vil du kalde nogle af dem - som for eksempel $*$ og $\circ$ ovenfor - ens?

# 3 Symmetriske grupper

Lad $\mathcal{S}_n$ betegne mængden af alle ombytninger af tallene i mængden

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

Lad $\sigma \in \mathcal{S}_n$ være en ombytning. Da betegner vi for alle $i = 1, 2, \ldots, n$ med $\sigma(i)$ det tal, som $\sigma$ ombytter $i$ til, og givet to ombytninger $\sigma, \tau \in \mathcal{S}_n$ skriver vi $\sigma \circ \tau$ for den *sammensatte* ombytning, som er givet ved

$$(\sigma \circ \tau)(i) = \sigma(\tau(i))$$

for alle $i = 1, 2, \ldots, n$. Det vil altså sige *først* $\tau$ og *derefter* $\sigma$.

Det er ikke svært at vise, at $(\mathcal{S}_n, \circ)$ er en gruppe, og det overlader vi til øvelserne.

**Definition 3.1.** En ombytning $\sigma \in \mathcal{S}_n$ kaldes en *$k$-cykel*, hvis der findes $k$ forskellige tal $1 \leq i_1, i_2, \ldots, i_k \leq n$, så

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \ldots \quad , \quad \sigma(i_{k-1}) = i_k, \quad \sigma(i_k) = i_1,$$

og så $\sigma(i) = i$, hvis $i \notin \{i_1, i_2, \ldots, i_k\}$. Vi benytter notationen

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_k \end{pmatrix}.$$

Vi må vist hellere illustrere definitionen af en $k$-cykel med et eksempel!

**Eksempel 3.2.** Betragt ombytningen $\sigma \in \mathcal{S}_4$, som er givet ved $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 2$ og $\sigma(4) = 4$. Bemærk, at

$$\sigma(1) = 3, \quad \sigma(3) = 2, \quad \sigma(2) = 1,$$

og da $\sigma(4) = 4$, vil det sige, at $\sigma$ er en 3-cykel. Med notationen fra definitionen har vi $\sigma = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$. Denne notation er meget overskuelig, idet vi undgår at skrive det ene $\sigma$ efter det andet, og idet vi ikke noterer de tal, som $\sigma$ alligevel ikke gør noget ved. I dette eksempel drejer det sig om tallet 4.

**Sætning 3.3.** *Enhver ombytning i $\mathcal{S}_n$ kan skrives som en sammensætning af cykler.*

Vi vil ikke bevise denne sætning, som vi i stedet nøjes med at illustrere med et eksempel. Ideen i eksemplet kan bruges til at give et konstruktivt bevis for sætningen.

**Eksempel 3.4.** Betragt ombytningen $\sigma \in \mathcal{S}_6$ givet ved

$$\sigma(1) = 3, \quad \sigma(2) = 6, \quad \sigma(3) = 1, \quad \sigma(4) = 2, \quad \sigma(5) = 5, \quad \sigma(6) = 4.$$

Vi går frem på følgende måde: Først skriver vi

$$\begin{pmatrix} 1 & ? \end{pmatrix}$$

og spørger, hvad $\sigma$ gør ved 1. Da $\sigma(1) = 3$, skriver vi

$$\begin{pmatrix} 1 & 3 & ? \end{pmatrix}$$

og ser, hvad $\sigma$ gør ved 3. Da $\sigma(3) = 1$, afsluttes cyklen, og vi begynder en ny cykel med et tal, som ikke indgår i den foregående.

$$\begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & ? \end{pmatrix}.$$

Da $\sigma(2) = 6$, skriver vi

$$\begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 6 & ? \end{pmatrix}$$

og spørger, hvad $\sigma$ gør ved 6. Idet $\sigma(6) = 4$, skriver vi

$$\begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 6 & 4 & ? \end{pmatrix},$$

og da $\sigma(4) = 2$, afsluttes parentesen.

$$\begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 6 & 4 \end{pmatrix}.$$

Til sidst har vi

$$\begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 6 & 4 \end{pmatrix} \circ \begin{pmatrix} 5 & ? \end{pmatrix},$$

og da $\sigma(5) = 5$, afsluttes parentesen. Resultatet er altså

$$\begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 6 & 4 \end{pmatrix} \circ \begin{pmatrix} 5 \end{pmatrix}.$$

Hvis vi tror på, at denne fremgangsmåde virker, har vi fundet frem til, at

$$\sigma = \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 6 & 4 \end{pmatrix}.$$

## Øvelser

**Øvelse 8.** Vis, at $(S_n, \circ)$ er en gruppe.

**Øvelse 9.** Find ombytninger $\sigma, \tau \in S_3$, som opfylder $\sigma \circ \tau \neq \tau \circ \sigma$. Her ser vi dette første eksempel på en ikke-abelsk gruppe.

**Øvelse 10.** Lad $\sigma \in \mathcal{S}_7$ være givet ved

$$\sigma(1) = 4,\ \sigma(2) = 6,\ \sigma(3) = 5,\ \sigma(4) = 1,\ \sigma(5) = 3,\ \sigma(6) = 7,\ \sigma(7) = 2.$$

Skriv $\sigma$ som en sammensætning af cykler. Kan det gøres på flere måder?

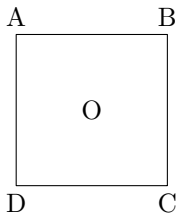
**Øvelse 11.** En 2-cykel, altså en cykel på formen $\begin{pmatrix} i & j \end{pmatrix}$, hvor $i \neq j$, kaldes en *transposition*. Skriv cyklen $\begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \in \mathcal{S}_3$ som en sammensætning af transpositioner.

**Øvelse 12.** En transposition på formen $\begin{pmatrix} i & i+1 \end{pmatrix}$ kaldes en *simpel* transposition. Skriv cyklen $\begin{pmatrix} 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix} \in \mathcal{S}_6$ som en sammensætning af simple transpositioner.

**Øvelse 13.** Gør rede for - eventuelt ved at vifte lidt med armene - at enhver ombytning i $\mathcal{S}_n$ kan skrives som en sammensætning af simple transpositioner. Man siger, at $\mathcal{S}_n$ er *frembragt* af de simple transpositioner.

# 4 Diedergrupper

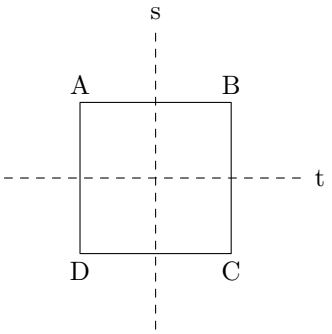
Betragt et kvadrat




i planen med centrum $O$ og hjørner $A$, $B$, $C$ og $D$.

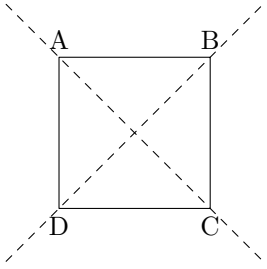
Lad $r_\theta$ betegne drejningen af kvadratet omkring $O$ gennem vinklen $\theta$ i positiv omløbsretning. Det vil altså sige *mod* uret.

Lad $s$ betegne spejlingen af kvadratet i linjen gennem midtpunkterne af de vandrette sider,




og lad $t$ betegne spejlingen i linjen gennem midtpunkterne af de lodrette sider.

Hvis $x$ og $y$ er spejlinger eller drejninger, skriver vi $x \circ y$ for sammensætningen af $x$ og $y$. Det vil altså sige *først* $y$ og *derefter* $x$. Bemærk, at $t \circ r_{\pi/2}$ er spejlingen af kvadratet i linjen gennem $A$ og $C$,




mens $s \circ r_{\pi/2}$ er spejlingen i linjen gennem $B$ og $D$.

Sæt $\mathcal{D}_4 = \{r_0, r_{\pi/2}, r_\pi, r_{3\pi/2}, s, t, s \circ r_{\pi/2}, t \circ r_{\pi/2}\}$. Da er $(\mathcal{D}_4, \circ)$ en gruppe! Vi vil ikke vise dette, som forhåbentligt er til at tro på ud fra de geometriske betragtninger ovenfor.

Gruppen $\mathcal{D}_4$ er et eksempel på en *diedergruppe*. Genrelt defineres $\mathcal{D}_n$ som gruppen af drejninger og spejlinger af en regulær $n$-kant.

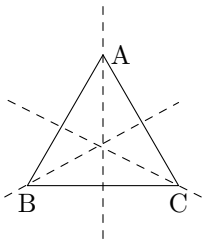
## Øvelser

**Øvelse 14.** Vis, at $\{r_0, r_{\pi/2}, r_\pi, r_{3\pi/2}\}$ er en undergruppe i $\mathcal{D}_4$.

**Øvelse 15.** Hvad er de omvendte elementer af elementerne i $\mathcal{D}_4$?

**Øvelse 16.** Vis, at alle drejningerne $r_0$, $r_{\pi/2}$, $r_\pi$ og $r_{3\pi/2}$ kan skrives som sammensætninger af spejlingerne $s$, $t$, $s \circ r_{\pi/2}$ og $t \circ r_{\pi/2}$. Dette udtrykkes ofte ved at sige, at $\mathcal{D}_4$ er *frembragt* af spejlinger.

**Øvelse 17.** Opskriv elementerne i $\mathcal{D}_3$. De relevante spejlingsakser er indtegnet nedenfor.




**Øvelse 18.** Er $\mathcal{D}_3$ også frembragt af spejlinger? Er alle $\mathcal{D}_n$ frembragt af spejlinger?

# 5 Division med rest

De to grupper $\mathbf{Z}$ og $\mathbf{Q}^\times$ er begge eksempler på *uendelige* grupper, mens $\mathcal{S}_n$ og $\mathcal{D}_n$ er *endelige* grupper. Fra nu af vil vi fokusere på endelige grupper. Ved *ordenen* af en endelig gruppe forstås antallet af elementer i gruppen.

Vi indleder med at repetere begrebet *division med rest*.

**Sætning 5.1.** *Lad $n$ og $d$ være hele tal, og antag $d > 0$. Da findes entydigt bestemte tal $q, r \in \mathbf{Z}$, som opfylder*

$$n = qd + r \quad og \quad 0 \leq r < d.$$

Tallet $r$ kaldes *resten* af $n$ ved division med $d$. Hvis $r = 0$, er $n = qd$, så $d$ går op i $n$. Dette skrives kort $d \mid n$. Vi vil ikke bevise Sætning 5.1, men nøjes i stedet med at illustrere den med et eksempel.

**Eksempel 5.2.** Sæt $n = 33$ og $d = 7$. Da $4 \cdot 7 = 28$ og $5 \cdot 7 = 35$, ser vi, at det højeste antal gange, som 7 går op i 33, er 4. Tilbage er $33 - 4 \cdot 7 = 5$. Altså kan vi sætte $q = 4$ og $r = 5$.

Lad nu $d$ være et helt tal, og antag $d > 0$. I følge Påstand 5.1 findes der til ethvert $n \in \mathbf{Z}$ entydigt bestemte tal $q_n$ og $r_n$, som opfylder $n = q_n d + r_n$ og $0 \leq r_n < d$. For ethvert $m \in \mathbf{Z}$ definerer vi

$$[m]_d = \{n \in \mathbf{Z} \mid r_n = r_m\}.$$

Det vil altså sige, at $[m]_d$ er mængden af de hele tal, der har samme rest som $m$ ved division med $d$. Vi vil nu finde en lidt mere bekvem beskrivelse af mængden $[m]_d$.

**Sætning 5.3.** *Lad $m, d \in \mathbf{Z}$ og antag $d > 0$. Da er*

$$[m]_d = \Big\{ n \in \mathbf{Z} \;\Big|\; d \mid (n - m) \Big\}.$$

*Bevis.* Når man skal vise, at to mængder er ens, viser man, at den første er indeholdt i den anden, og at den anden er indeholdt i den første.

Lad $n \in [m]_d$. Vi skal vise, at $d \mid (n - m)$. At $n \in [m]_d$ betyder ifølge definitionen af $[m]_d$, at $r_n = r_m$, så idet $n = q_n d + r_n$ og $m = q_m d + r_m$, følger det, at

$$n - m = q_n d + r_n - (q_m d + r_m) = q_n d - q_m d = (q_m - q_n)d,$$

hvilket viser, at $d \mid (n-m)$.

Antag nu omvendt, at $d \mid (n-m)$. Vi skal vise, at $n \in [m]_d$. Idet $d \mid (n-m)$, findes et $k \in \mathbf{Z}$, så $n - m = kd$. Heraf følger, at

$$q_n d + r_n = n = m + kd = q_m d + r_m + kd = (q_m + k)d + r_m,$$

så entydigheden af $r_n$ giver, at $r_n = r_m$. Det vil sige, at $n \in [m]_d$. □

Lad os se på et eksempel.

**Eksempel 5.4.** Lad $d = 2$. Vi vil beskrive $[m]_2$ for $m \in \mathbf{Z}$. Sættes $m = 0$, giver Påstand 5.3, at

$$[0]_2 = \Big\{ n \in \mathbf{Z} \;\Big|\; 2 \mid n \Big\}.$$

Det vil sige, at $[0]_2$ er mængden af alle de tal, som 2 går op i. Disse er netop de lige tal, så

$$[0]_2 = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

Ved nu at sætte $m = 1$, giver Påstand 5.3, at

$$[1]_2 = \Big\{ n \in \mathbf{Z} \;\Big|\; 2 \mid (n-1) \Big\}.$$

Altså er $[1]_2$ mængden af de tal, $n$, der opfylder, at $n - 1$ er lige. Disse er netop de ulige tal, så

$$[1]_2 = \{\ldots, -3, -1, 1, 3, \ldots\}.$$

Lad nu $m \in \mathbf{Z}$ være vilkårligt. Da kan vi ved division med rest finde $q, r \in \mathbf{Z}$ med $0 \leq r < d$, så $m = qd + r$. Da $m$ og $r$ har samme rest, nemlig $r$, ved division med $d$, har vi $[m]_d = [r]_d$. Altså kan ethvert $[m]_d$ skrives på formen $[r]_d$, hvor $0 \leq r < d$. Det vil sige, at

$$\{[m]_d \mid m \in \mathbf{Z}\} = \{[0]_d, [1]_d, \ldots, [d-1]_d\}.$$

Denne mængde vil vi betegne $\mathbf{Z}_d$.

**Eksempel 5.5.** I det forrige eksempel fandt vi beskrivelser af mængderne $[0]_2$ og $[1]_2$. For et vilkårligt $m \in \mathbf{Z}$ er resten af $m$ ved division med 2 enten 0 eller 1, så $[m]_2 = [0]_2$ eller $[m]_2 = [1]_2$. Overvej, at det første er tilfældet, hvis $m$ er lige, og at det sidste er tilfældet, hvis $m$ er ulige.

## Øvelser

**Øvelse 19.** Find resten af 87 ved division med 9.

**Øvelse 20.** Beskriv mængderne $[m]_3$ for alle $m \in \mathbf{Z}$.

**Øvelse 21.** Lad $d > 0$. Vis, at $[n]_d = [m]_d$, hvis og kun hvis $d \mid (m - n)$.

# 6 Cykliske grupper

Vi skal nu se, at $\mathbf{Z}_d$ har struktur som en gruppe for alle $d > 0$.

**Sætning 6.1.** *Lad $d > 0$, og lad som ovenfor $\mathbf{Z}_d = \{[m]_d \mid m \in \mathbf{Z}\}$. Der findes en sammensætning $\oplus$ på $\mathbf{Z}_d$, som er givet ved*

$$[m]_d \oplus [n]_d = [m+n]_d$$

*for alle $m, n \in \mathbf{Z}$.*

*Bevis.* For at vise, at $\oplus$ på $\mathbf{Z}_d$ er en sammensætning, må vi vise, at dette $\oplus$ er veldefineret. Vi ved fra Eksempel 5.5, at vi sagtens kan have $[m]_d = [m']_d$, selv om $m \neq m'$. Definitionen

$$[m]_d \oplus [n]_d = [m+n]_d$$

ser ud til at afhænge af valget af *repræsentanterne* $m$ og $n$, og det er op til os at vise, at det ikke er tilfældet.

Antag derfor, at vi har et andet par repræsentanter $m'$ og $n'$. Det vil sige, at $[m]_d = [m']_d$ og $[n]_d = [n']_d$. Vi skal vise, at der gælder

$$[m+n]_d = [m'+n']_d.$$

Idet $[m]_d = [m']_d$, gælder $d \mid (m-m')$, og tilsvarende gælder $d \mid (n-n')$, da $[n]_d = [n']_d$. Heraf følger, da

$$(m+n) - (m'+n') = (m-m') + (n-n'),$$

at

$$d \mid ((m+n) - (m'+n')).$$

Altså er $[m+n]_d = [m'+n']_d$. □

**Sætning 6.2.** *Lad $d > 0$. Da er $(\mathbf{Z}_d, \oplus)$ en gruppe.*

*Bevis.* Vi skal tjekke, at punkterne (1), (2) og (3) i definitionen af en gruppe er opfyldt. Idet der for alle hele tal $m$, $n$, og $r$ gælder, at $(m+n)+r = m+(n+r)$, ser vi, at

$$\begin{aligned}([m]_d \oplus [n]_d) \oplus [r]_d = [m+n]_d \oplus [r]_d = [(m+n)+r]_d = [m+(n+r)]_d \\ = [m]_d \oplus [n+r]_d = [m]_d \oplus ([n]_d \oplus [r]_d)\end{aligned}$$

for alle elementer $[m]_d$, $[n]_d$ og $[r]_d$ i $\mathbf{Z}_d$. Dette viser punkt (1).

For at vise punkt (2) bemærker vi, at $[0]_d$ opfylder

$$[0]_d \oplus [m]_d = [0+m]_d = [m]_d \quad \text{og} \quad [m]_d \oplus [0]_d = [m+0]_d = [m]_d$$

for alle elementer $[m]_d$ i $\mathbf{Z}_d$.

Lad nu $[m]_d$ være et element i $\mathbf{Z}_d$. Da er

$$[m]_d + [-m]_d = [m-m]_d = [0]_d \quad \text{og} \quad [-m]_d + [m]_d = [(-m)+m] = [0]_d,$$

hvilket viser, at $[m]_d$ har et omvendt element, nemlig $[-m]_d$. Dette viser punkt (3). □

Gruppen $\mathbf{Z}_d$ kaldes den *cykliske* gruppe af orden $d$.

# 7 Isomorfibegrebet

I dette afsnit vil vi diskutere, hvornår vi vil kalde to grupper ens.

**Definition 7.1.** Lad $(G, *)$ og $(H, \circ)$ være grupper. En funktion $f\colon G \to H$ kaldes en *gruppehomomorfi*, hvis $f(g * g') = f(g) \circ f(g')$ for alle $g, g' \in G$.

Bemærk, at betingelsen $f(g * g') = f(g) \circ f(g')$ i definitionen ovenfor betyder, at det er ligegyldigt, om man først sammensætter elementerne $g$ og $g'$ i $G$ og derefter anveder $f$, eller om man først anvender $f$ på $g$ og $g'$ og derefter sammensætter elementerne $f(g)$ og $f(g')$ i $H$.

**Eksempel 7.2.** Lad $d > 0$, og lad $f_d\colon \mathbf{Z}_d \to \mathbf{Z}_d$ være givet ved $f_d([m]_d) = [2m]_d$. Som tidligere, er der noget, der lige skal tjekkes: Er funktionen $f_d$ veldefineret? Hvis $[m]_d = [n]_d$, er så $[2m]_d = [2n]_d$? Ja, thi hvis $[m]_d = [n]_d$, så gælder $d \mid (m-n)$ og dermed også $d \mid (2m-2n)$, og dermed er $[2m]_d = [2n]_d$. Lad os vise, at $f_d$ er en gruppehomomorfi: For elementer $[n]_d$ og $[m]_d$ i $\mathbf{Z}_d$ gælder, at

$$\begin{aligned} f_d([n]_d \oplus [m]_d) &= f_d([n+m]_d) = [2(n+m)]_d = [2n+2m]_d \\ &= [2n]_d \oplus [2m]_d = f_d([n]_d) \oplus f_d([m]_d). \end{aligned}$$

**Definition 7.3.** Lad $G$ og $H$ være grupper. En gruppehomomorfi $f\colon G \to H$ kaldes en *gruppeisomorfi*, hvis følgende krav er opfyldt:

(1) Hvis $g, g' \in G$ opfylder $f(g) = f(g')$, så er $g = g'$.
(2) For ethvert $h \in H$ findes et $g \in G$, så $f(g) = h$.

Hvis der findes en gruppeisomorfi $f\colon G \to H$, siges grupperne $G$ og $H$ at være *isomorfe* grupper.

Vi vil tænke på to grupper som værende "ens", hvis de er isomorfe. Lad os overveje, hvorfor dette synes rimeligt: Lad $f\colon G \to H$ være en gruppeisomorfi. Definitionen af en gruppeisomorfi giver, at der er en 1-1 korrespondance mellem elementerne i $G$ og $H$, og da $f$ er en gruppehomomorfi viser diskussionen efter Definition 7.1, at der i princippet ikke er forskel på sammensætningerne i henholdsvis $G$ og $H$.

## Øvelser

**Øvelse 22.** Betragt gruppehomomorfierne $f_d$, hvor $d > 0$, fra Eksempel 7.2. Vis, at $f_3$ er en gruppeisomorfi. Er $f_4$ en gruppeisomorfi?

**Øvelse 23.** Vis, at $f\colon \mathbf{Z} \to \mathbf{Z}$, hvor $f(n) = n^2$, er en funktion, som *ikke* er en gruppehomomorfi.

**Øvelse 24.** Gør rede for, at funktionen $f\colon \mathbf{Z} \to \mathbf{Z}_d$ givet ved $f(n) = [n]_d$ er en gruppehomomorfi.

**Øvelse 25.** Lad $f\colon G \to H$ være en gruppehomomorfi og definer *billedet* af $G$ under $f$ ved

$$\mathrm{im}(f) = \{f(g) \mid g \in G\}.$$

Vis, at $\mathrm{im}(f)$ er en undergruppe af $H$.

**Øvelse 26.** Lad $f\colon G \to H$ være en gruppehomomorfi og definer *kernen* for $f$ ved

$$\ker(f) = \{g \in G \mid f(g) = e\}.$$

Vis, at $\ker(f)$ er en undergruppe af $G$.

**Øvelse 27.** Lad $f\colon G_1 \to G_2$ og $g\colon G_2 \to G_3$ være gruppehomomorfier. Vis, at den sammensatte funktion $g \circ f\colon G_1 \to G_3$ er en gruppehomomorfi. Vis også, at $g \circ f$ er en gruppeisomorfi, hvis både $f$ og $g$ er gruppeisomorfier.

**Øvelse 28.** Vis, at grupperne $\mathcal{D}_3$ og $\mathcal{S}_3$ er isomorfe grupper. Hvorfor er $\mathcal{D}_n$ og $\mathcal{S}_n$ *ikke* isomorfe grupper, når $n \neq 3$?

**Øvelse 29.** Vis, at $\mathbf{Z}_2 \times \mathbf{Z}_3$ og $\mathbf{Z}_6$ er isomorfe grupper. Er $\mathbf{Z}_2 \times \mathbf{Z}_4$ og $\mathbf{Z}_8$ isomorfe? Hvornår mon $\mathbf{Z}_m \times \mathbf{Z}_n$ og $\mathbf{Z}_{mn}$ er isomorfe?

**Øvelse 30.** Lad $G$ og $H$ være grupper, og lad

$$s\colon G \to H$$

være en gruppeisomorfi. Vis, der er findes en funktion

$$t\colon H \to G,$$

som opfylder $t(s(g)) = g$ for alle $g \in G$ og $s(t(h)) = h$ for alle $h \in H$. Vis, at $t$ er en gruppeisomorfi.

# 8 Grupper af primtalsorden

Det er generelt svært at sige, hvor mange forskellige grupper - det vil sige grupper, der ikke er isomorfe - der findes af en given orden. Hvis $G$ er en gruppe af orden $p$, hvor $p$ er et primtal, er det derimod ikke så svært.

Der gælder følgende vigtige sætning, som vi ikke vil bevise her.

**Sætning 8.1** (Lagrange)**.** *Lad $G$ være en endelig gruppe, og lad $H$ være en undergruppe af $G$. Da gælder*

$$|H| \;\Big|\; |G|.$$

Lad $G$ være en endelig gruppe af orden $p$, hvor $p$ er et primtal, og vælg et element $g \neq e$ i $G$. Sæt $\langle g \rangle = \{g^n \mid n \in \mathbf{Z}\}$. Det overlades til læseren at vise, at $\langle g \rangle$ er en undergruppe af $G$.

Da $g \neq e$, er $|\langle g \rangle| > 1$, og i følge Sætning 8.1 går $|\langle g \rangle|$ op i $p$. Da $p$ er et primtal, må vi da have $|\langle g \rangle| = p$, så $G = \langle g \rangle$. Heraf følger, at

$$G = \{e, g, g^2, \ldots, g^{p-1}\}.$$

Vi er nu nået til hovedresultatet!

**Sætning 8.2.** *Lad $(G, *)$ være en endelig gruppe af orden $p$, hvor $p$ er et primtal. Da er $G$ isomorf med $\mathbf{Z}_p$.*

*Bevis.* I følge diskussionen ovenfor er $G = \{e, g, g^2, \ldots, g^{p-1}\}$. Definer nu en funktion

$$f \colon \mathbf{Z}_p \to G$$

ved $f([m]_p) = g^m$. Som sædvanlig skal vi lige tjekke, at funktionen $f$ er veldefineret. Hvis $[m]_p = [n]_p$, gælder $p \mid (m - n)$. Derfor $m - n = kp$ for et $k \in \mathbf{Z}$, og dermed er $m = n + kp$. Heraf følger, at

$$g^m = g^{n+kp} = g^n * g^{kp} = g^n * (g^p)^k = g^n * e^k = g^n * e = g^n,$$

så $f$ er veldefineret. Det overlades til læseren at tjekke, at $f$ er en gruppehomomorfi.

Definitionen af $f$ viser direkte, at $f$ rammer ethvert element i $G$, og da $G$ og $\mathbf{Z}_p$ indeholder lige mange elementer, bliver hvert element i $G$ ramt præcist én gang. Det betyder altså, at $f$ er en gruppeisomorfi. □