

1. EN DEFINISJON - NYTT PERSPEKTIV PÅ NOE KJENT

Vi begynner med noe som er **typisk** i matematikk og skriver ned en **definisjon**. En definisjon er en presis måte å si hvordan vi bruker ord og hva vi snakker om.

Definisjon 1.1. En **kropp** er en *mengde* K sammen med *to operasjoner* $+: K \times K \rightarrow K$ som vi kaller **addisjon** og $\cdot: K \times K \rightarrow K$ som vi kaller **multiplikasjon** slik at følgende regler gjelder: For alle elementer $a, b, c \in K$ har vi

- $(a + b) + c = a + (b + c)$ og $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- $a + b = b + a$ og $a \cdot b = b \cdot a$,
- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,

og vi krever

- det finnes **to** elementer 0 og 1 slik at $0 \neq 1$ og $a + 0 = a$ og $a \cdot 1 = a$ for alle $a \in K$,
- for **hvert** $a \in K$ finnes det et element $-a$ slik at $a + (-a) = 0$,
- for **hvert** $a \neq 0$ i K finnes det et element a^{-1} , vi skriver også $\frac{1}{a}$, slik at $a \cdot a^{-1} = 1$.

2. EKSEMPLER

Vi er alle kjent med eksempler av kropp:

- Mengden $\mathbb{Q}$ av rasjonale tall er en kropp.
- Mengden $\mathbb{R}$ av reelle tall er en kropp.
- Det finnes en kropp $\mathbb{F}_p$ med p elementer for hvert primtall p .

Men noen andre mengder med addisjon og multiplikasjon er **ikke** kropp:

- Mengden $\mathbb{Z}$ av alle heltall er **ikke** en kropp fordi det finnes ikke noen inverse for multiplikasjonen, for eksempel $\frac{1}{2} \notin \mathbb{Z}$.
- Det **finnes ikke** en kropp med **6 elementer** fordi i en slik kropp måtte gjelde $2 \cdot 3 = 6 = 0$ selv om $2 \neq 0$ og $3 \neq 0$.

Typisk. I definisjonen av en kropp tok vi egenskapene av **kjente eksempler**, skrev ned det som er viktig for oss, nemlig regnereglene og eksistens av 0 og 1, og har sett bort fra alt annet. Og så finner vi mange flere eksempler. Faktisk finnes det **uendelig mange** andre kropp. Som matematikere kan vi nå sette oss målet med å prøve å forstå alle kropp som finnes. Men dette rekker vi ikke i dag. ;-)

3. Et tall er et element i en kropp

Vi bruker reglene i en kropp for å regne med tall. Faktisk kan vi si at et **tall** er rett og slett **et element i en kropp**. **For eksempel**, sier vi at et element i $\mathbb{Q}$ er et **rasjonalt** tall. Et element i $\mathbb{R}$ er et **reelt** tall.

Løse ligninger. En fundamental problemstilling i matematikk er å **løse ligninger** og det er ofte kropper som gir oss **løsningsmengder**. For eksempel kan vi løse ligningen

$$x^2 - 5 = 0$$

i kroppen $\mathbb{R}$ av alle reelle tall, dvs det finnes reelle tall $x = \pm\sqrt{5}$ som tilfredsstiller ligningen. **Men** vi kan ikke finne et **reelt** tall som er en løsning for ligningen

$$x^2 + 1 = 0.$$

Faktisk finnes det mange ligninger som er skrevet ved hjelp av reelle tall med $+$, $\cdot$ i $\mathbb{R}$ og én variabel x som vi **ikke** kan løse i $\mathbb{R}$.

Utvide $\mathbb{R}$. Vi har kanskje sett en gang før hvordan vi løser dette problemet. Ideen er at vi **utvider** kroppen $\mathbb{R}$ av reelle tall til kroppen $\mathbb{C}$ av alle **komplekse tall**. Dette gjør man vanligvis ved å **finne opp et nytt tall** i med egenskapen $i^2 = -1$. Så skriver man komplekse tall som $a + bi$ med reelle tall a, b . Men det **finnes også andre måter** å konstruere kroppen av alle komplekse tall. Det skal vi lære om nå...

4. UTFORDRING - NY MENGDE MED NYE REGNEREGLER

Vårt **mål** er nå å konstruere en ny kropp som inneholder løsninger for alle slike løsninger. Vi begynner med et første skritt i denne retningen.

Definisjon 4.1. Vi ser på mengden $\mathcal{M}$ gitt av

$$\mathcal{M} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}.$$

Vi kan tenke på elementer i $\mathcal{M}$ som 2×2 -tabeller. Som du kommer til å lære dette semesteret er $\mathcal{M}$ mengden av alle (reelle) 2×2 -**matriser**. For **eksempel** har vi at

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} e & \sqrt{3} \\ \pi & -\frac{1}{2} \end{pmatrix}, \dots$$

er elementer i $\mathcal{M}$ (uendelig mange andre).

Notasjon 4.2. Vi bruker nå også bokstaver som M, N , eller X, Y for å betegne et element, dvs en tabell eller matrise, i $\mathcal{M}$.

Nå **definerer vi addisjonen** i $\mathcal{M}$ ved at

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}.$$

Dette ser ut som en ganske åpenbart måte å definere en addisjon: vi bare legger sammen elementer som vanlig i hver posisjon i tabellen ved å bruke addisjon av reelle tall.

Vi **definerer multiplikasjon** i $\mathcal{M}$ ved at

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}.$$

Vi kan **huske reglen** for multiplikasjonen sånn: for å få elementet i rad i og kolonne j må vi gange og legge sammen rad i fra den første tabellen med kolonne j fra den andre tabellen. Her er i og j enten 1 eller 2, men reglen fungerer også for større tabeller eller matriser.

Addisjon fungerer helt fint i $\mathcal{M}$. Vi har matrisen $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, som vi kaller **nullelementet** eller nullmatrisen, slik at

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for alle elementer $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ i $\mathcal{M}$. Vi har også:

Lemma 4.3. For alle X, Y og Z i $\mathcal{M}$ har vi

- (1) $(X + Y) + Z = X + (Y + Z)$,
- (2) $X + Y = Y + X$,
- (3) $(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$, og
- (4) $X \cdot (Y + Z) = (X \cdot Y) + (X \cdot Z)$.

Bevis. Vi lar X, Y og Z være elementer i $\mathcal{M}$ og bruker definisjonen av $+$ og $\cdot$:

(1)

$$\begin{aligned} (X + Y) + Z &= \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \\ &= \begin{pmatrix} (a+a')+a'' & (b+b')+b'' \\ (c+c')+c'' & (d+d')+d'' \end{pmatrix} \\ &= \begin{pmatrix} a+(a'+a'') & b+(b'+b'') \\ c+(c'+c'') & d+(d'+d'') \end{pmatrix} = X + (Y + Z), \end{aligned}$$

(2)

$$\begin{aligned} X + Y &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} \\ &= \begin{pmatrix} a'+a & b'+b \\ c'+c & d'+d \end{pmatrix} = Y + X, \end{aligned}$$

(3)

$$\begin{aligned} (X \cdot Y) \cdot Z &= \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) \cdot \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \\ &= \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix} \cdot \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \\ &= \begin{pmatrix} (aa'+bc')a''+(ab'+bd')c'' & (aa'+bc')b''+(ab'+bd')d'' \\ (ca'+dc')a''+(cb'+dd')c'' & (ca'+dc')b''+(cb'+dd')d'' \end{pmatrix} \\ &= \begin{pmatrix} aa'a''+bc'a''+ab'c''+bd'c'' & aa'b''+bc'b''+ab'd''+bd'd'' \\ ca'a''+dc'a''+cb'c''+dd'c'' & ca'b''+dc'b''+cb'd''+dd'd'' \end{pmatrix} \\ &= \begin{pmatrix} a(a'a''+b'c'')+b(c'a''+d'c'') & a(a'b''+b'd'')+b(c'b''+d'd'') \\ c(a'a''+b'c'')+d(c'a''+d'c'') & c(a'b''+b'd'')+d(c'b''+d'd'') \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a'a''+b'c'' & a'b''+b'd'' \\ c'a''+d'c'' & c'b''+d'd'' \end{pmatrix} = X \cdot (Y \cdot Z), \end{aligned}$$

(4)

$$\begin{aligned}
X \cdot (Y + Z) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a'+a'' & b'+b'' \\ c'+c'' & d'+d'' \end{pmatrix} \\
&= \begin{pmatrix} a(a'+a'')+b(c'+c'') & a(b'+b'')+b(d'+d'') \\ c(a'+a'')+d(c'+c'') & c(b'+b'')+d(d'+d'') \end{pmatrix} \\
&= \begin{pmatrix} aa'+aa''+bc'+bc'' & ab'+ab''+bd'+bd'' \\ ca'+ca''+dc'+dc'' & cb'+cb''+dd'+dd'' \end{pmatrix} \\
&= \begin{pmatrix} (aa'+bc')+(aa''+bc'') & (ab'+bd')+(ab''+bd'') \\ (ca'+dc')+(ca''+dc'') & (cb'+dd')+(cb''+dd'') \end{pmatrix} \\
&= (X \cdot Y) + (X \cdot Z).
\end{aligned}$$

Dermed har vi vist at alle påstandene er riktige for alle elementer i $\mathcal{M}$. $\square$

Eksempel 4.4. Men vi har

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Spørsmål: Hva viser oss dette eksemplet?

Svar: Eksemplet viser at $\mathcal{M}$ med operasjonen $\cdot$ **ikke** er en kropp fordi i det minste to av reglene ikke gjelder i $\mathcal{M}$.

Hvilke regler gjelder ikke? Vi har ikke $X \cdot Y = Y \cdot X$ for alle $X, Y \in \mathcal{M}$, og ikke alle elementer i $\mathcal{M}$ har en invers med hensyn til $\cdot$. Her ser vi at det **ikke** finnes $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^{-1}$ og ikke $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^{-1}$ i $\mathcal{M}$. Vi skal lære mer om dette snart.

5. UTFORDRING - EN NY KROPP

For å oppnå vårt mål må vi altså forandre noe. La oss prøve å se på en litt mindre mengde. Kanskje blir den en kropp?

Vi definerer altså delmengden

$$\mathcal{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subseteq \mathcal{M}$$

og bruker **samme addisjon og multiplikasjon** som i $\mathcal{M}$. For eksempel har vi

$$\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} \in \mathcal{C}, \text{ og } \begin{pmatrix} \pi & -\sqrt{5} \\ \sqrt{5} & \pi \end{pmatrix} \in \mathcal{C}.$$

Notasjon 5.1. Vi kan se på $\mathbb{R}$ som en **delmengde** av $\mathcal{C}$ ved å **identifisere** et reelt tall a med $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Vi skal også skrive a for elementet $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ i $\mathcal{C}$ når a er et reelt tall.

(**Typisk** i matematikk: vi introduserer forkortende notasjoner som er enklere å bruke, men kan forvirre oss i første øyeblikket.)

Lemma 5.2. Når X og Y er elementer i $\mathcal{C}$, da er også $X + Y$ og $X \cdot Y$ elementer i $\mathcal{C}$.

Bevis. Vi lar X og Y være elementer i $\mathcal{C}$ og bruker definisjonen av $+$ og $\cdot$:

$$\begin{aligned} X + Y &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} a+a' & -(b+b') \\ b+b' & a+a' \end{pmatrix} \in \mathcal{C} \text{ og} \\ X \cdot Y &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa' - bb' & -ab' - ba' \\ ba' + ab' & -bb' + aa' \end{pmatrix} \\ &= \begin{pmatrix} aa' - bb' & -(ab' + ba') \\ ab' + ba' & aa' - bb' \end{pmatrix} \in \mathcal{C}. \end{aligned}$$

□

Dette viser at $+$ og $\cdot$ definerer operasjoner på $\mathcal{C}$. Vi gjør nå følgende påstand:

Teorem 5.1. *Mengden $\mathcal{C}$ sammen med de to operasjonene $+$ og $\cdot$ definert i $\mathcal{M}$ er en kropp.*

Spørsmål: Hva mangler vi for å bevise teoremet?

6. OPPGAVER

Vi skal nå jobbe med å svare på følgende spørsmål:

Oppgave 1: Er $X \cdot Y = Y \cdot X$ for alle $X, Y \in \mathcal{C}$?

Oppgave 2: Finnes det et element $Y \in \mathcal{C}$ slik at

$$Y \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

for alle $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathcal{C}$? Hvis det eksisterer, hva vil du kalle et slikt element?

Oppgave 3: For reelle tall a, b slik at $a^2 + b^2 > 0$ sjekk at vi har

$$\begin{pmatrix} \frac{a}{a^2+b^2} & \frac{b}{a^2+b^2} \\ \frac{-b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Oppgave 4: Forklar hvorfor vi har nå bevist Teorem 5.1.

Oppgave 5: Hva er

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}?$$

Kan vi løse ligningen $X^2 + 1 = 0$? (Her skriver vi $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ og $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.)

Oppgave 6: Vi kan lage en korrespondanse mellom planet $\mathbb{R}^2$ og $\mathcal{C}$ på følgende måte:

$$(a, b) \in \mathbb{R}^2 \longleftrightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathcal{C}$$

Vi har at $(0, 1) \longleftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Hva skjer når vi utfører multiplikasjonen

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

Tegn det i planet.

Oppgave 7: Når en vinkel α går fra 0 til 2π så beskriver $(\cos \alpha, \sin \alpha)$ en sirkel med radius 1 i $\mathbb{R}^2$. Hva skjer geometrisk når vi utfører multiplikasjonen:

$$\begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \cdot \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix}$$

Oppgave 8: Kan vi finne flere enn én løsning av ligningen $X^n = 1$ for positive heltall $n \geq 3$?

Oppgave 9: Ethvert punkt i planet kan uttrykkes som

$$(r \cos \alpha, r \sin \alpha)$$

for en vinkel α og et ikke-negativt reelt tall r . La

$$X = \begin{pmatrix} r \cos \alpha & -r \sin \alpha \\ r \sin \alpha & r \cos \alpha \end{pmatrix} \text{ og } Y = \begin{pmatrix} s \cos \beta & -s \sin \beta \\ s \sin \beta & s \cos \beta \end{pmatrix}$$

for ikke-negative reelle tall r, s og vinkler α og β . Hva er $X \cdot Y$?

Oppgave 10: Kan vi løse

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0$$

med $a_i \in \mathbb{R}$ (her skriver vi igjen a for elementet $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ i $\mathcal{C}$ som korresponderer til det reelle tallet a)?