

Note om legemer

Leif K. Jørgensen

Definition 1 Ved et legeme (engelsk: field) $(F, +, \cdot)$ forstås en mængde F med to kompositioner $+$ og $\cdot$ som opfylder følgende:

1. $+$ er associativ

2. $+$ er kommutativ

3. der findes et element $0 \in F$, så $0 + x = x$, for alle $x \in F$

4. for ethvert element $x \in F$ findes et element $-x \in F$, så

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

5. $\cdot$ er associativ

6. $\cdot$ er kommutativ

7. der findes et element $1 \in F$, så $1 \cdot x = x$ for alle $x \in F$
($1 \neq 0$)

8. for ethvert element $x \in F \setminus \{0\}$ findes et element $x^{-1} \in F$, så

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

9. $\cdot$ er distributiv over $+$, dvs

$$x \cdot (y + z) = x \cdot y + x \cdot z, \text{ for alle } x, y, z \in F$$

Vi bruger den sædvanlige notation og skriver: $a + (-b) = a - b$ og $a \cdot b^{-1} = \frac{a}{b}$.

Eksempel 2

- $(\mathbb{Q}, +, \cdot)$ er et legeme.
- $(\mathbb{R}, +, \cdot)$ er et legeme.
- $(\mathbb{C}, +, \cdot)$ er et legeme.

Opgave 1 Lad $(F, +, \cdot)$ være et legeme. Vis at $(F, +)$ er en abelsk gruppe.

Opgave 2 Lad $(F, +, \cdot)$ være et legeme. Vis at $(F^*, \cdot)$ er en abelsk gruppe, hvor $F^* = F \setminus \{0\}$.

Opgave 3 Lad $(F, +, \cdot)$ være et legeme. Vis at $0 \cdot x = 0$ for alle $x \in F$. (Udnyt f.eks. at $0 = 0 + 0$.)

Opgave 4 Lad $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$, hvor i er det velkendte komplekse tal.

Vis at $(\mathbb{Q}[i], +, \cdot)$ er et legeme. Skriv den multiplikative inverse til $a + bi$ på formen $c + di$.

Opgave 5 Lad $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Vis at $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ er et legeme. Skriv den multiplikative inverse til $a + b\sqrt{2}$ på formen $c + d\sqrt{2}$.

Det fremgår af definitionen at et legeme har mindst to elementer. Der findes faktisk et legeme med præcis to elementer:

Lad $\mathbb{F}_2 = \{0, 1\}$ og lad kompositionerne $+$ og $\cdot$ være defineret ved

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Opgave 6 Vis at $(\mathbb{F}_2, +, \cdot)$ er et legeme.

Læs definition B.0.9 og eksempel B.0.10 i Lauritzen, side 230–231.

Opgave 7 Lad $(E, +, \cdot)$ være et legeme, og lad $F \subseteq E$ være en delmængde, som opfylder at $(F, +, \cdot)$ er et legeme. (F siges da at være et dellegeme af E .)

Vis at E er et vektorrum over F .

F.eks. er $\mathbb{C}$ et vektorrum over $\mathbb{R}$ og $\mathbb{R}$ er et vektorrum over $\mathbb{Q}$.

Opgave 8 Lad $\mathbb{F}_q$ være et endeligt legeme med q elementer. Hvor mange vektorer er der i vektorrummet $\mathbb{F}_q^n$ fra eksempel B.0.10?

Eksempel 3 Lad G være mængden af (reelle) $n \times n$ diagonalmatricer, hvor der på hver diagonalplads står enten 1 eller -1 . Så er G med matrixmultiplikation en abelsk gruppe med neutralt element I_n og med orden 2^n . Denne gruppe opfylder den betingelse, der undersøges i næste opgave.

Opgave 9 Lad $(G, \circ)$ være en gruppe med neutralt element e , som opfylder at $g \circ g = e$ for alle $g \in G$.

Vis at G er en abelsk gruppe. (Vink: udregn $x \circ x \circ y \circ x \circ y \circ y$ på to forskellige måder.)

Vi skriver nu komposition i denne gruppe som $+$ i stedet for $\circ$ og det neutrale element betegnes 0 .

Vis at G er et vektorrum over $\mathbb{F}_2$.

Man kan bevise at hvis gruppen G i opgave 9 er endelig så har vektorrummet G en basis. G 's orden er da 2^n , hvor n er antallet af vektorer i basen. (Se eventuelt: afsnit B.1.)

På samme måde som vi betragter vektorrum over et vilkårligt legeme kan vi også se på matricer over et vilkårligt legeme F . Matrixprodukt for matricer over F udregnes på samme måde som for matricer over $\mathbb{R}$.

Her udregnes f.eks. et produkt af to matricer over $\mathbb{F}_2$:

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 0 \cdot 0 & 1 \cdot 1 + 0 \cdot 1 \\ 1 \cdot 1 + 1 \cdot 0 & 1 \cdot 1 + 1 \cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

idet udregningerne foretages med kompositionerne fra $\mathbb{F}_2$.

På samme måde som for matricer over $\mathbb{R}$ kan man vise at matrixmultiplikation er associativ. Vi giver her en formel definition af multiplikation af matricer over et vilkårligt legeme, og viser at den er associativ.

Definition 4 Mængden $M_n(F)$ består af $n \times n$ matricer $A = (a_{ij})$, hvor $a_{ij} \in F$, for $i, j = 1, \dots, n$. På denne mængde defineres kompositionen matrixmultiplikation ved at produktet af A og B er $n \times n$ matricen AB med indgang (i, j) givet ved:

$$(AB)_{ij} = \sum_{s=1}^n a_{is} b_{sj}.$$

Lemma 5 *Matrixmultiplikation i $M_n(F)$ er associativ og har neutralt element I hvor $(I)_{ij} = 1$ hvis $i = j$ og $(I)_{ij} = 0$ hvis $i \neq j$.*

Bevis Lad $A, B, C \in M_n(F)$. Så bestemmes indgang (i, j) i $A(BC)$ ved

$$(A(BC))_{ij} = \sum_{s=1}^n a_{is}(BC)_{sj} = \sum_{s=1}^n a_{is} \sum_{t=1}^n b_{st}c_{tj} = \sum_{s=1}^n \sum_{t=1}^n a_{is}b_{st}c_{tj},$$

hvor den sidste omskrivning udnytter at vi må gange a_{is} ind i “parentesen” $\sum_{t=1}^n$, p.g.a. den distributive lov.

Tilsvarende bestemmes indgang (i, j) i $(AB)C$:

$$((AB)C)_{ij} = \sum_{t=1}^n (AB)_{it}c_{tj} = \sum_{t=1}^n \left(\sum_{s=1}^n a_{is}b_{st} \right) c_{tj} = \sum_{t=1}^n \sum_{s=1}^n (a_{is}b_{st}c_{tj}) = \sum_{s=1}^n \sum_{t=1}^n a_{is}b_{st}c_{tj}.$$

Igen ganger vi ind i parentesen og bytter derefter om på summationerne. Dette svarer til at summere de n^2 led i en anden rækkefølge. Her udnyttes altså at $+$ er kommutativ.

Vi får altså at $A(BC) = (AB)C$.

Desuden ser vi at

$$(IA)_{ij} = \sum_{s=1}^n (I)_{is}a_{sj} = a_{ij},$$

hvor vi udnytter at $(I)_{is} = 0$ hvis $s \neq i$ og derfor kun får ledet hvor $s = i$. Dermed er $IA = A$ og tilsvarende er $AI = A$. $\square$

Opgave 10 Lad $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ være en matrix over legeme F .

Vis at hvis $ad - bc \neq 0$ så er $B = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$ en invers til A . (Altså

$$AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.)$$

Vis at hvis $ad - bc = 0$ så har A ikke nogen invers.

Vi betragter nu 2×2 matricer over $\mathbb{F}_2$. I $\mathbb{F}_2$ er $x = -x$. Den inverse til $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ er derfor matricen $\begin{pmatrix} \frac{d}{ad+bc} & \frac{b}{ad+bc} \\ \frac{c}{ad+bc} & \frac{a}{ad+bc} \end{pmatrix}$ forudsat at $ad + bc \neq 0$.

Opgave 11 Lad $GL_2(\mathbb{F}_2)$ betegne mængden af alle invertible 2×2 matricer over $\mathbb{F}_2$.

Gør rede for at $GL_2(\mathbb{F}_2)$ er gruppe med matrixmultiplikation som komposition.

Lav en liste med alle matricer i $GL_2(\mathbb{F}_2)$.

Opskriv en kompositionstavle for matrixmultiplikation i $GL_2(\mathbb{F}_2)$.

Lad $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$ og lad kompositionerne $+$ og $\cdot$ være defineret ved

$+$	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

$\cdot$	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

Man kan bevise at $(\mathbb{F}_4, +, \cdot)$ er et legeme.