AALBORG UNIVERSITET

Endelige legemer

Olav Geil
Institut for Matematiske Fag, Aalborg Universitet

Opgaver:

Når vi indfører talsystemer, så starter vi med at definere plus og gange. For nogle talssystemers vedkommende giver det så anledning til, at vi også kan trække fra og dividere. Men sådan er det ikke altid. De talsystemer, som ligner de rationale tal og de reelle tal (og for den sags skyld de komplekse tal), og hvor vi derfor automatisk får subtraktion og division med i købet, kaldes legemer. De opfylder følgende definition.

Definition
Lad L være en mængde og $+$ og $\cdot$ være to regnearter herpå. Da siges L at være et legeme, hvis

L.1: $a+b=b+a$ for alle a,b

L.2: $a+(b+c)=(a+b)+c$ for alle a,b,c

L.3: Der findes et element kaldet 0, så $a+0=a$ for alle a

L.4: For alle a findes der et element kaldet $-a$ således at $a+(-a)=0$

L.5: $a\cdot b=b\cdot a$ for alle a,b

L.6: $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ for alle a,b,c

L.7: Der findes et element kaldet 1, så $a\cdot 1=a$ for alle a

L.8: For alle $a\neq 0$ findes der et element kaldet a^{-1}, således at $a\cdot a^{-1}=1$

L.9: $a\cdot(b+c)=a\cdot b+a\cdot c$ for alle a,b,c

Læsevejledning til nedenstående opgavesæt:
I opgave 1 arbejdes der med legemet med 5 elementer. Opgave 2 behandler dernæst legemet med 8 elementer. Opgave 3 handler om systemet af to gange to matricer, som udgør et vigtigt eksempel på et talsystem, der ikke opfylder alle 9 regler L.1, . . . , L.9 ovenfor, og som derfor ikke er et legeme. Dette talsystem er ikke endeligt, men det er medtaget i opgavesættet, fordi det på en fin måde illustrerer, at man ikke kan tage reglerne ovenfor for givet, herunder at den kommutative lov for multiplikation holder. I opgave 4 vises det, hvordan enhver funktion på et endeligt legeme kan udtrykkes som et polynomium. Disse er altså de eneste eksempler på funktioner over endelige legemer. Endelig gives der i opgave 5 et eksempel på en talstruktur, hvor et polynomium af grad 2 har 4 nulpunkter. Dette er alene muligt, fordi denne talstruktur ikke er et legeme. Opgaverne kan regnes uafhængigt af hinanden, men det vil være hensigtsmæssigt at regne opgave 1 før opgave 2 og opgave 4.

Opgave 1
Betragt legemet $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ med regnereglen $5 = 0$. Vi har altså $3 + 4 = 2$ (fordi $7 = 5 + 2$) og $3 \cdot 4 = 2$ (fordi $12 = 2 \cdot 5 + 2$).

(a)
Udfyld alle indgange i nedenstående additionstabel

$+$	0	1	2	3	4
0					
1					
2					
3					
4					

(b)
Vi har $-1 = 4$, da $1 + 4 = 0$. Bestem værdierne af -2, -3 og -4.

(c)
Hvis vi fortolker $a - b$ som $a + (-b)$, hvad bliver så $3 - 4$ i $\mathbb{F}_5$?

(d)
Udfyld alle indgange i nedenstående multiplikationstabel

$\cdot$	0	1	2	3	4
0					
1					
2					
3					
4					

(e)
Ved at kigge i tabellen ser vi, at $2^{-1} = 3$ fordi $2 \cdot 3 = 1$. Hvad er 3^{-1} og 4^{-1}?

(f)
Hvis vi fortolker $\frac{a}{b}$ som $a \cdot b^{-1}$, hvad er $\frac{3}{4}$ så lig i talsystemet $\mathbb{F}_5$?

Opgave 2
I denne opgave betragter vi legemet med otte elementer, nemlig

$$\mathbb{F}_8 = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+\alpha, \alpha^2+1, \alpha^2+\alpha+1\}$$

med regnereglerne $2 = 0$ og $\alpha^3 = \alpha + 1$.
Således har vi $(\alpha+1) + (\alpha^2+1) = \alpha^2 + \alpha$, fordi $1 + 1 = 0$. Og vi har

$$\begin{aligned}(\alpha+1)\cdot(\alpha^2+1)) &= \alpha^3 + \alpha + \alpha^2 + 1 \\ &= \alpha + 1 + \alpha + \alpha^2 + 1 \\ &= \alpha^2\end{aligned}$$

ligesom vi har $\alpha^2 \cdot \alpha^2 = \alpha^4 = \alpha \cdot \alpha^3 = \alpha \cdot (\alpha+1) = \alpha^2 + \alpha$.

(a)
Udfyld alle indgange i nedenstående additionstabel

$+$	0	1	α	$\alpha+1$	α^2	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$
0								
1								
α								
$\alpha+1$								
α^2								
$\alpha^2+\alpha$								
α^2+1								
$\alpha^2+\alpha+1$								

(b)
Hvad er $-(\alpha^2+\alpha+1)$ lig (hvad skal vi lægge til $\alpha^2+\alpha+1$ for at få 0)?

(c)
Tænk på $a - b$ som $a + (-b)$. Argumenter for, at der i $\mathbb{F}_8$ gælder, at $a + b = a - b$ (plus og minus er det samme).

(d)
Udfyld alle indgange i nedenstående multiplikationstabel

$\cdot$	0	1	α	$\alpha+1$	α^2	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$
0								
1								
α								
$\alpha+1$								
α^2								
$\alpha^2+\alpha$								
α^2+1								
$\alpha^2+\alpha+1$								

(e)
Bestem følgende syv værdier ved at kigge i tabellen: 1^{-1}, α^{-1}, $(\alpha+1)^{-1}$, $(\alpha^2)^{-1}$, $(\alpha^2+\alpha)^{-1}$, $(\alpha^2+1)^{-1}$ og $(\alpha^2+\alpha+1)^{-1}$.

(f)
Hvis vi fortolker $\frac{a}{b}$ som $a \cdot b^{-1}$, hvad er $\frac{\alpha}{\alpha+1}$ så lig i talsystemet $\mathbb{F}_8$?

(g)
Udregn i rækkefølge følgende:

- α^3
- $\alpha^4 = \alpha \cdot \alpha^3 = \cdots$
- $\alpha^5 = \alpha \cdot \alpha^4 = \cdots$
- $\alpha^6 = \alpha \cdot \alpha^5 = \cdots$
- $\alpha^7 = \alpha \cdot \alpha^6 = \cdots$.

Konkluder at udregningerne herefter kører i ring: $\alpha^8 = \alpha$, $\alpha^9 = \alpha^2$, $\alpha^{10} = \alpha^3 = \cdots$ osv.

(h)
Kontroller vha. indsigten fra delopgave (g) dine udregninger i delopgave (d).

Opgave 3

Matricer spiller en helt central rolle i mange applikationer. I denne opgave betragter vi systemet bestående af 2 gange 2 matricer (over de reelle tal $\mathbb{R}$). Det vil sige elementer af formen

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

hvor $a, b, c, d \in \mathbb{R}$.
Vi indfører $+$ som følger

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

og $\cdot$ som følger

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}.$$

(a)
Udregn

$$\begin{bmatrix} 1 & 2 \\ 4 & -2 \end{bmatrix} + \begin{bmatrix} 0 & 7 \\ 1 & 3 \end{bmatrix}$$

(b)
Udregn

$$\begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 7 & 0 \end{bmatrix}$$

(c)
Argumenter for, at hvis vi tænker på

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

som 0-elementet, så er L.3 opfyldt.

(d)
Hvis

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

hvad er $-A$ så lig?

(e)
Argumenter for, at hvis vi tænker på

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

som 1-elementet, så er L.7 opfyldt.

(f)
Lad

$$B = \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix} \quad \text{og} \quad C = \begin{bmatrix} 0 & 1 \\ \frac{1}{2} & -\frac{1}{2} \end{bmatrix}$$

og udregn $B \cdot C$. Hvis ellers du har regnet rigtigt, så har du nu vist, at $B^{-1} = C$.

(g)
Udregn

$$\begin{bmatrix} 2 & 1 \\ 7 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}$$

Sammenlign med delopgave (b), og konkluder, at systemet af 2 gange 2 matricer ikke opfylder L.5.

(h)
Lad

$$D = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Argumenter for, at D^{-1} ikke findes. Hint: Gang D på

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

og vis, at dette aldrig kan blive lig

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Opgave 4
I denne opgave vises det på eksempelform, hvordan enhver funktion på et endeligt legeme kan beskrives som et polynomium. Metoden hedder Lagrange-interpolation.

Betragt $\mathbb{F}_3 = \{0, 1, 2\}$ med regnereglen $3 = 0$. Dvs. vi har:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Dvs. $-1 = 2$ og $-2 = 1$. Tilsvarende haves $2^{-1} = 2$, da $2 \cdot 2 = 1$.

I det følgende skriver vi $\frac{a}{b}$ i betydningen $a \cdot b^{-1}$.

Betragt funktionen f fra $\mathbb{F}_3$ ind i $\mathbb{F}_3$ givet ved

$$f(0) = 1, f(1) = 2 \text{ og } f(2) = 1.$$

Vi opbygger nu i et par step et polynomium, som svarer til netop denne funktion.

Step 1:
Først betragter vi

$$\begin{aligned} \frac{(x-1)\cdot(x-2)}{(0-1)\cdot(0-2)} &= \frac{x^2-3x+2}{2\cdot 1} = 2^{-1}\cdot(x^2+2) \\ &= 2\cdot(x^2+2) = 2x^2+1. \end{aligned}$$

Dette polynomium er konstrueret således, at hvis vi sætter 1 eller 2 ind, så får vi 0, men sætter vi 0 ind, så får vi 1. Kan du se, hvad der menes med, at det er "konstrueret således"?. Eftervis ved indsættelse i

sidste udtryk, at dette er korrekt.

Step 2:
Polynomiet

$$\begin{aligned}\frac{(x-0)\cdot(x-2)}{(1-0)\cdot(1-2)} &= \frac{x^2-2x}{-1} = \frac{x^2+x}{2} \\ &= (2^{-1})\cdot(x^2+x) = 2\cdot(x^2+x) = 2x^2+2x\end{aligned}$$

opfylder på samme måde, at sætter vi 0 eller 2 ind, så får vi 0, men sætter vi 1 ind, da får vi 1. Verificer dette ved indsættelse.

Step 3:
Polynomiet

$$\begin{aligned}\frac{(x-0)\cdot(x-1)}{(2-0)\cdot(2-1)} &= \frac{x^2-x}{2} = (2^{-1})\cdot(x^2+2x) \\ &= 2\cdot(x^2+2x) = 2x^2+x\end{aligned}$$

er konstrueret således at stopper vi 0 eller 1 ind, da får vi 0, men stopper vi 2 ind, da får vi 1. Verificer dette.

Sidste step:
Lad nu polynomiet $f(x)$ være givet som

$$f(x) = (2x^2+1)\cdot f(0) + (2x^2+2x)\cdot f(1) + (2x^2+x)\cdot f(2).$$

Indsæt værdierne for $f(0)$, $f(1)$ og $f(2)$ i dette udtryk og simplificer. Eftervis ved indsættelse, at der derved er fremkommet et polynomium $f(x)$ med de rigtige funktionsværdier.

Prøv med andre funktionsværdier. Forklar hvorledes metoden genereliserer til vilkårligt endeligt legeme.

Opgave 5
Betragt et polynomium $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, med $a_n \neq 0$ og alle $a_i \in \mathbb{F}$, hvor $\mathbb{F}$ er et legeme. Et centralt resultat i algebraen siger, at f højst kan have n nulpunkter i $\mathbb{F}$. I denne opgave ser vi, at et tilsvarende resultat ikke nødvendigvis gælder, når den givne talstruktur ikke er et legeme.

Betragt talstrukturen $\mathbb{Z}_4 = \{0,1,2,3\}$ med regnereglen $4 = 0$.

(a)
Udfyld nedenstående additions- og mulitiplikationstabelller:

+	0	1	2	3
0				
1				
2				
3				

$\cdot$	0	1	2	3
0				
1				
2				
3				

(b)
Gør rede for, at ikke alle ikke-nul elementer har en multiplikativ invers, og at Z_4, derfor ikke er et legeme.

(c)
Vis ved indsættelse, at $f(x) = 2x^2 + 2x$ har fire nulpunkter i $\mathbb{Z}_4$ (til trods for, at det alene har grad 2).