Facit til udvalgte opgaver i note om legemer

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

Opgave 2 *Lad* $(F, +, \cdot)$ *være et legeme. Vis at* $(F^*, \cdot)$ *er en 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* $0 = 0 + 0$.*)*

Bevis: $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$. Hvis vi adderer $-(0 \cdot x)$ på begge sider får vi $0 = 0 \cdot x$.

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* $c + di$.

Løsning: se næste opgave.

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* $c + d\sqrt{2}$.

Bevis: vi skal først vise at $\mathbb{Q}[\sqrt{2}]$ er lukket under $+$ og $\cdot$: $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}$ og $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$.

Regnereglerne 1, 2, 5, 6 og 9 er opfyldt for alle komplekse tal og dermed specielt for tal der ligger i $\mathbb{Q}[\sqrt{2}]$. Vi bemærker desuden at 0 og 1 ligger i $\mathbb{Q}[\sqrt{2}]$, så 3. og 7. er opfyldt. 4. er opfyldt da $-(a + b\sqrt{2}) = -a - b\sqrt{2}$. 8. er opfyldt da $a + b\sqrt{2} \neq 0$ har invers $\frac{1}{a+b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$ (Tæller og nævner ganges med $a - b\sqrt{2}$. Vi ved at $a^2 - 2b^2 \neq 0$, for ellers er $\sqrt{2} = \pm\frac{a}{b}$, som er rational men vi ved at $\sqrt{2}$ er irrational.)

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

Bevis for 9.: Vi bemærker at hvis $x = 0$ så får vi $0 \cdot (y + z) = 0 = 0 \cdot y + 0 \cdot z$ og hvis $x = 1$ er $1 \cdot (y + z) = y + z = 1 \cdot y + 1 \cdot z$.

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 E.) Vis at E er et vektorrum over F.*

Bevis: Fra opgave 1 ved vi at $(E, +)$er en abelsk gruppe. (i), (ii), (iii) og (iv) i definition B.0.9 er opfyldt da de gælder for alle $a, b, v, w \in E$.

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?*

Svar: q^n

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 element betegnes 0.
Vis at G er et vektorrum over $\mathbb{F}_2$.

Bevis: $x \circ x \circ y \circ x \circ y \circ y = (x \circ x) \circ y \circ x \circ (y \circ y) = e \circ y \circ x \circ e = y \circ x$.
Desuden er $x \circ x \circ y \circ x \circ y \circ y = x \circ ((x \circ y) \circ (x \circ y)) \circ y = x \circ e \circ y = x \circ y$.
Altså $x \circ y = y \circ x$.

$(G, +)$ er nu en abelsk gruppe. Vi definerer $0 \cdot v = 0$ og $1 \cdot v = v$.
(i): vi skal vise $(ab)v = a(bv)$. Hvis $a = b = 1$ står der $v = v$. Hvis enten a eller b er 0 står der $0 = 0$.
(iii) undersøg de forskellige kombination af a og b.
(iv) hvis $a = 0$ står der $0 = 0$, og hvis $a = 1$ står der $v + w = v + w$.

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.

Bevis for 2. del: Antag $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ og $ad - bc = 0$. Hvis $a \neq 0$ så er $d = \frac{bc}{a}$ og $ax + bz = 1$ medfører at $\frac{c}{a}(ax + bz) = \frac{c}{a} \neq 0$ altså $cx + dz \neq 0$, modstrid. Hvis $a = 0$ så ...

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 $GL_2(\mathbb{F}_2)$.

Løsning: $\mathrm{GL}_2(\mathbb{F}_2)$ er lukket under multiplkation, for hvis A og B er invertible så er AB invertibel med invers $B^{-1}A^{-1}$. Det neutrale element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ligger i $\mathrm{GL}_2(\mathbb{F}_2)$.

$$\mathrm{GL}_2(\mathbb{F}_2) = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\}.$$

Hvis disse matricer benævnes henholdvis e, a, d, b, c, f så kan kompositionstavlen læses på side 55 i Lauritzen.

Senere vil vi derfor sige at $\mathrm{GL}_2(\mathbb{F}_2)$ er isomorf med S_3.