

Note om endelige legemer

Leif K. Jørgensen

1 Legemer af primtalsorden

Vi har i Lauritzen afsnit 2.1.1 set følgende:

Proposition 1 *Lad n være et positivt helt tal. Vi kan da definere en komposition $+$ på*

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$$

ved $[a] + [b] = [a + b]$.

Desuden er $(\mathbb{Z}/n\mathbb{Z}, +)$ en abelsk gruppe.

Vi har også i Lauritzen afsnit 2.3.2 set følgende:

Proposition 2 *Lad n være et positivt helt tal. Vi kan da definere en associativ og kommutativ komposition $\cdot$ på*

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$$

ved $[a] \cdot [b] = [a \cdot b]$.

Desuden er $((\mathbb{Z}/n\mathbb{Z})^, \cdot)$ en abelsk gruppe hvor $(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \mid \gcd(a, n) = 1\}$.*

Lemma 3 *Lad p være et primtal. Så er*

$$(\mathbb{Z}/p\mathbb{Z})^* = \{[1], \dots, [p-1]\} = (\mathbb{Z}/p\mathbb{Z}) \setminus \{[0]\}.$$

Følgende lemma giver en sammenhæng mellem $+$ og $\cdot$.

Lemma 4 *Den distributive lov gælder i $\mathbb{Z}/n\mathbb{Z}$:*

$$[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c],$$

for alle $a, b, c \in \mathbb{Z}$.

Bevis $[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a(b + c)] = [ab + ac] = [ab] + [ac] = [a] \cdot [b] + [a] \cdot [c]$.

Sætning 5 *Lad p være et primtal. Så er $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ et legeme.*

Dette legeme betegnes også $\mathbb{F}_p$.

Bevis Ifølge “Note om legemer” skal vi vise at 9 betingelser er opfyldt. Proposition 1 siger at følgende er opfyldt:

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

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

Proposition 2 og Lemma 3 giver betingelserne 5.–8.:

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

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

Lemma 4 giver den sidste betingelse:

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

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

□

2 Hvordan foretager man beregninger i $\mathbb{F}_p$?

- Addition: $[a] + [b] = [a + b]$. Normalt erstattes $a + b$ med divisionsresten af $a + b$ ved division med p .
- Multiplikation: $[a][b] = [ab]$. Normalt erstattes ab med divisionsresten af ab ved division med p .
- Additiv invers/subtraktion: $-[a] = [-a]$. Hvis $a \in \{1, 2, \dots, p-1\}$ så er $p - a \in \{1, 2, \dots, p-1\}$ og $-[a] = [p - a]$.
 $[a] - [b] = [a - b]$. Normalt erstattes $a - b$ med divisionsresten af $a - b$ ved division med p .
- Multiplikativ invers/division: For at beregne $[a]^{-1}$ hvor $[a] \neq [0]$ (dvs.: p går ikke op i a) skal vi bruge Euklids udvidede algoritme til at bestemme heltal λ og μ så

$$\gcd(a, p) = 1 = \lambda a + \mu p.$$

Så er $[a]^{-1} = [\lambda]$. Normalt erstattes λ med divisionsresten af λ ved division med p .

Hvis vi skal udregne $\frac{[b]}{[a]}$ beregnes først $[a]^{-1}$ og derefter kan vi multiplicere: $[b] \cdot [a]^{-1}$.

Eksempel 6 *Vi vil udregne*

$$\frac{[2] - [7]}{[2] + [7]}$$

i $\mathbb{F}_{79}$.

Først udregner vi $[2] - [7] = [-5] = [79 - 5] = [74]$. Vi kan dog med fordel regne videre med $[-5]$ da 5 er et lille tal. Desuden er $[2] + [7] = [9]$.

For at udregne $\frac{[-5]}{[9]}$ skal vi bestemme den multiplikative inverse til $[9]$. Ved hjælp af Euklids udvidede algoritme finder vi

$$\gcd(9, 79) = 1 = (-35) \cdot 9 + 4 \cdot 79,$$

altså $[9]^{-1} = [-35] = [79 - 35] = [44]$. Igen er det fordel at regne med $[-35]$. Vi får nu

$$\frac{[2] - [7]}{[2] + [7]} = [-5] \cdot [9]^{-1} = [-5] \cdot [-35] = [(-5) \cdot (-35)] = [175] = [2 \cdot 79 + 17] = [17].$$

3 Matrixgrupper

I “Note om legemer” indførte vi matricer over et vilkårligt legeme og multiplikation af sådanne matricer. Vi arbejder nu videre med dette emne og konstruerer nye grupper.

Definition 7 *Lad F være et legeme og lad n være et positivt helt tal. Mængden alle invertible matricer i $M_n(F)$ betegnes da $GL_n(F)$ og kaldes den generelle lineære gruppe af $n \times n$ matricer over F .*

Proposition 8 *$GL_n(F)$ er en gruppe med matrixmultiplikation som komposition.*

Bevis Lad $A, B \in GL_n(F)$. Så er AB invertibel med invers $(AB)^{-1} = B^{-1}A^{-1}$. AB ligger altså i $GL_n(F)$, som dermed er lukket under multiplikation. Vi skal blot vise at de tre betingelser i definitionen af en gruppe er opfyldt. Vi har allerede vist at multiplikationen er associativ. Det neutrale element er I som ligger i $GL_n(F)$, da den er sin egen inverse. Enhver matrix $A \in GL_n(F)$ har en invers ifølge definitionen af $GL_n(F)$ og den inverse ligger også i $GL_n(F)$, da A^{-1} er invertibel med invers A . $\square$

Hvis F er et endeligt legeme kan man beregne denne gruppes orden.

Proposition 9 *Lad $\mathbb{F}_q$ være et endeligt legeme med q elementer. Så har gruppen $GL_n(\mathbb{F}_q)$ orden $(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1})$.*

Eksempel 10 *Lad F være et legeme og lad n være et positivt helt tal. Lad D betegne følgende delmængde af $GL_n(F)$:*

$$D = \{aI \mid a \in F \setminus \{0\}\}.$$

Så er D en normal undergruppe af $GL_n(F)$ og D er isomorf med $(F \setminus \{0\}, \cdot)$.

Eksempel 11 *Lad F være et legeme og lad G betegne følgende delmængde af $GL_2(F)$:*

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in F \right\}.$$

Så er G en undergruppe af $GL_2(F)$ og G er isomorf med $(F, +)$.