

# MA2201 / TMA4150

- \* Grupper (abelske, undergrupper, sykliske grupper, permutasjonsgrupper)
  - grunnleggende abstrakt algebraisk struktur
  - matematikk, matematisk fysikk, kjemi, .....
- \* Restklasser, faktorgrupper, homomorfier, gruppevirkninger, Sylowteori
- \* Ringer (= grupper med ekstra struktur)
- \* Kropper (= ringer med ekstra struktur)

## 1.-4. Grupper

Def: La  $S$  være en mengde. En binær operasjon  $*$  på  $S$  er en funksjon

$$S \times S \longrightarrow S$$
$$(a, b) \longmapsto a * b$$

Eksempler: (1)  $S = \mathbb{Z}$ ,  $*$  = addisjon

(2)  $S = \mathbb{Z}$ ,  $*$  = multiplikasjon

(3)  $S = \mathbb{R}$ ,  $a * b = \pi$  for alle  $a, b \in \mathbb{R}$

(4)  $S = C[0, 1] = \{f: [0, 1] \rightarrow \mathbb{R} \mid f \text{ kont}\}$ ,  $*$  = addisjon av funksjoner:  $(f+g)(x) = f(x) + g(x)$

(5)  $S = P_{\mathbb{R}}^4(x) = \{p(x) \mid p(x) \text{ polynom}^m / \text{koeff i } \mathbb{R}, \text{ deg } p(x) \leq 4\}$   
 $= \{a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 \mid a_i \in \mathbb{R}\}$

$*$  = addisjon av polynomer

Def: En gruppe  $(G, *)$  er en ikke-tom mengde  $G$  sammen med en binær operasjon  $*$  på  $G$  (dvs funksjon  $G \times G \rightarrow G$ ,  $(a, b) \mapsto a * b$ ) slik at

(1) Operasjonen  $*$  er assosiativ:  $g * (h * k) = (g * h) * k \quad \forall g, h, k \in G$

(2) Identitetselement finnes:  $\exists e \in G$  slik at  $e * g = g = g * e \quad \forall g \in G$ .

(3) Inverser finnes:  $\forall g \in G$  finnes en  $h \in G$  med  $g * h = e = h * g$

Grupper er abelske hvis i tillegg:

(4) Operasjonen  $*$  er kommutativ:  $g * h = h * g \quad \forall g, h \in G$ .

Eksempler: (1)  $(\mathbb{Z}, +)$  er en abelsk gruppe:

- (1) addisjon er assosiativ
- (2)  $e=0$  er id-elt:  $0+n=n+0=n \quad \forall n \in \mathbb{Z}$
- (3) inverser finnes:  $\forall n \in \mathbb{Z}$  er  $n+(-n)=(-n)+n=0$
- (4) addisjon er kommutativ

(2)  $(\mathbb{Z}, \cdot)$  er ikke en gruppe:

- (1) (2) + (4) ok (id-elt er  $e=1$ )
- (3) ikke ok: for elementet  $3 \in \mathbb{Z}$  finnes ingen  $n \in \mathbb{Z}$  med  $3 \cdot n = 1$ .

(3)  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$  er abelske grupper med

$$(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +) \quad \text{undergrupper}$$

(4)  $(\mathbb{Q} \setminus \{0\}, \cdot)$ ,  $(\mathbb{R} \setminus \{0\}, \cdot)$ ,  $(\mathbb{C} \setminus \{0\}, \cdot)$  er abelske grupper

med 1 som id-elt:

- (1) multiplikasjon er assosiativ
- (2)  $e=1$  id-elt
- (3) Inverser finnes:  $a \in \mathbb{Q} \setminus \{0\} \Rightarrow \exists b \in \mathbb{Q} \setminus \{0\}$  med  $ab=ba=1$   
 $a \in \mathbb{R} \setminus \{0\} \Rightarrow \exists b \in \mathbb{R} \setminus \{0\}$  med  $ab=ba=1$   
 $a \in \mathbb{C} \setminus \{0\} \Rightarrow \exists b \in \mathbb{C} \setminus \{0\}$  med  $ab=ba=1$
- (4) multiplikasjon er kommutativ

(5) La  $G = M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$  med

$*$  = addisjon av matriser (vi skriver +)

Da er  $(M_2(\mathbb{R}), +)$  en abelsk gruppe med  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$  som id-elt.

(6) La  $G = GL(2, \mathbb{R}) = \{ M \in M_2(\mathbb{R}) \mid M \text{ er invertibel} \}$ .

Da er  $(GL(2, \mathbb{R}), +)$  ikke en gruppe, for operasjonen + (matriseaddisjon) er ikke en binær op på  $GL(2, \mathbb{R})$ :

$$\begin{array}{ccc} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} & + & \begin{pmatrix} -2 & 0 \\ 0 & 0 \end{pmatrix} & = & \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \\ \uparrow & & \uparrow & & \uparrow \\ GL(2, \mathbb{R}) & & GL(2, \mathbb{R}) & & GL(2, \mathbb{R}) \end{array}$$

Mer la istedet  $*$  = matrisemultiplikasjon (skriv  $\cdot$ ). Da er

$(GL(2, \mathbb{R}), \cdot)$  en gruppe som ikke er abelsk:

Matrisemultiplikasjon er en binær op på  $GL(2, \mathbb{R})$  siden

$$M_1, M_2 \in GL(2, \mathbb{R}) \Rightarrow M_1 \cdot M_2 \in GL(2, \mathbb{R})$$

Id-elt:  $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Ikke abelsk:  $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$

(7)  $(C[0,1], +)$  er en abelsk gruppe med id-elt funksjonen  $f: [0,1] \rightarrow \mathbb{R}$  gitt ved  $f(x) = 0 \forall x \in [0,1]$ .

(8)  $(P_{\mathbb{R}}^4(x), +)$  er en abelsk gruppe med id-elt polynom  $p(x) = 0$ .

(9)  $SL(2, \mathbb{R}) = \{ M \in M_2(\mathbb{R}) \mid \det(M) = 1 \} \subset GL(2, \mathbb{R})$ .

Siden  $\det(M_1 M_2) = \det(M_1) \cdot \det(M_2)$  er matrixmultiplikasjon en binær operasjon på  $SL(2, \mathbb{R})$ . Videre gjelder

$$M \in SL(2, \mathbb{R}) \Rightarrow M^{-1} \in SL(2, \mathbb{R})$$

$\Rightarrow (SL(2, \mathbb{R}), \cdot)$  er en gruppe (ikke abelsk, vis!). Har

$$(SL(2, \mathbb{R}), \cdot) \subset (GL(2, \mathbb{R}), \cdot) \quad \text{undergruppe}$$

(10) Vektorrom er spesielt abelske grupper

(11)  $(\mathbb{Z}, +, \cdot)$  er en ring

(12)  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  er kropp