

## 5. Undergrupper

Konvensjoner: (1) Normalt betegnes binæroperasjonen  $*: G \times G \rightarrow G$  på en gruppe bare med " $\cdot$ " eller " $+$ ", selv om det ikke betyr mult/add av tall.

Hvis man bruker multiplikativt notasjon, skrivs man " $ab$ " istedet for " $a \cdot b$ ".

- (2) Additiv notasjon " $+$ " er normalt forbeholdt abelske grupper.  
 (3) Id-elt betegnes med  $\begin{cases} e & \text{hvis mult. not.} \\ 0 & \text{hvis add. not.} \end{cases}$

- (4) Inverselementet til  $a \in G$  betegnes med  $\begin{cases} a^{-1} & \text{hvis mult. not.} \\ -a & \text{hvis add. not.} \end{cases}$

- (5) La  $a \in G$ . Hvis  $G$  er multiplikativ:

$$\begin{aligned} a^0 &\stackrel{\text{def}}{=} e \\ a^n &\stackrel{\text{def}}{=} \underbrace{aa \cdots a}_n \quad \left\{ \begin{array}{l} n > 1 \\ n = 1 \end{array} \right. \\ a^{-n} &\stackrel{\text{def}}{=} \underbrace{a^{-1}a^{-1} \cdots a^{-1}}_n \end{aligned}$$

Hvis  $G$  er additiv:

$$\begin{aligned} na &\stackrel{\text{def}}{=} \underbrace{a+a+\cdots+a}_n \quad (n > 1) \\ -na &\stackrel{\text{def}}{=} (-a)+(-a)+\cdots+(-a) \end{aligned}$$

Def: La  $G$  være en gruppe

- (1) Orderen til  $G$  er antall elt i  $G$ , skriv  $|G|$ . Gruppen er endelig hvis  $|G| < \infty$ .

- (2) En undermengde  $H \subseteq G$  er en undergruppe av  $G$ , dersom  
 (i)  $H$  er lukket under den binære operasjonen på  $G$   
 (ii)  $H$  er selv en gruppe med den binære operasjonen.

Skriv  $H \leq G$ , og  $H < G$  hvis  $H \neq G$ .

- (3) En undergruppe  $H < G$  kallas en ekte undergruppe. Undergruppen  $\{e\}$ , som kun består av id-eltet, kallas den trivuelle undergruppen.

Eksempler: (1) La  $G = \mathbb{Z}$  med vanlig addisjon. For  $m \in \mathbb{N}$ , la

$$H = m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\} = \{\dots -2m, -m, 0, m, 2m, \dots\}$$

Da er  $H$  en ekte undergr. av  $G$ . ( $H < G$ )

- (2) La  $G = \mathbb{C} \setminus \{0\}$  med vanlig mult. For  $m \in \mathbb{N}$ , la

$$H = U_m = \{z \in \mathbb{C} \mid z^m = 1\}$$

Da er  $H$  en ekte undergr. av  $G$ . Merk at  $|G| = \infty$ ,  $H < \infty$ .

(3) La  $G = \mathbb{C}$  med vanlig addisjon. For  $m \in \mathbb{N}$  er da  $\{m\}$  ikke en undergruppe, siden den ikke er lukket under add. F.eks er  $1, i \in \mathbb{U}_4$ , men  $1+i \notin \mathbb{U}_4$ .

(4) La  $G$  og  $H$  være følgende multipiktive grupper:

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

$$H = SL(2, \mathbb{R}) = \{ M \in M_2(\mathbb{R}) \mid \det(M) = 1 \}$$

Da er  $H < G$ .

Teorem 5.14 La  $G$  være en gruppe og  $\emptyset \neq H \subseteq G$  en undermenge. Da er  $H \leq G$  (dvs  $H$  undergr av  $G$ ) hvis og bare hvis

- (1)  $H$  er lukket under bin.op på  $G$  (dvs  $a, b \in H \Rightarrow ab \in H$ )
- (2) Id-eltet  $e \in G$  ligger i  $H$ .
- (3)  $a \in H \Rightarrow a^{-1} \in H$ .

Teorem 5.14 (superversjon). La  $G$  være en grupp  $\emptyset \neq H \subseteq G$ . Da er  $H \leq G$  hvis og bare hvis

$$(1) a, b \in H \implies ab^{-1} \in H$$

Beweis: Oppgave.

Eksempel: (1) La  $O(2, \mathbb{R}) = \{ M \in M_2(\mathbb{R}) \mid M \text{ ortogonal} \text{ (dvs } M^T = M^{-1}) \}$ . Da er  $O(2, \mathbb{R}) \leq GL(2, \mathbb{R})$ . For  $M_1, M_2 \in O(2, \mathbb{R})$  gjelder

$$(M_1 M_2)^T = M_2^T M_1^T = M_2^{-1} M_1^{-1} = (M_1 M_2)^{-1} \quad \text{medvendig}$$

$$(M_1 M_2^{-1})^T = (M_2^{-1})^T M_1^T = M_2 M_1^{-1} = (M_1 M_2^{-1})^{-1}$$

$$\Rightarrow O(2, \mathbb{R}) < GL(2, \mathbb{R}). \quad (\text{den ortogonale gruppen})$$

$$\text{La } SO(2, \mathbb{R}) = \{ M \in O(2, \mathbb{R}) \mid \det(M) = 1 \}$$

$$\xrightarrow{\text{vis!}} SO(2, \mathbb{R}) < O(2, \mathbb{R}) \quad (\text{den spesielle ortogonale gruppen})$$

(2) Mktg eksempel / Jenganger i gruppeteori. For  $n \in \mathbb{N}$ , la

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$$

og  $+_n$  addisjon modulo  $n$ . F.eks i  $\mathbb{Z}_{21}$  har vi

$$13 +_2 18 = 10 \quad \text{fordi } 31 \equiv 10 \pmod{21}$$

Da er  $(\mathbb{Z}_n, +_n)$  en abelsk gruppe (vis!).

Merk at  $|\mathbb{Z}_n| = n$ , så for alle  $n \in \mathbb{N}$  finnes det minst en gruppe av orden  $n$ . Se på  $\mathbb{Z}_9$  (med  $+_9$  som bin.op.).

$$\mathbb{Z}_9 = \{0, 1, \dots, 8\}$$

Se nå på

$$H = \{0, 3, 6\} \subseteq \mathbb{Z}_9.$$

Er  $H$  en undergruppe av  $\mathbb{Z}_9$ ? Ja! Det essensielle er at 3 og 6 er inverser av hverandre i  $\mathbb{Z}_9$ :  $6 = -3$  og  $3 = -6$ .

Vis nå:  $a, b \in H \Rightarrow a +_9 b \in H$  og  $a -_9 b \in H$

$$\Rightarrow H$$
 undergr av  $\mathbb{Z}_9$  fra T.5.14

Merk:  $H_1, H_2 \leq G$  undergrupper  $\Rightarrow H_1 \cap H_2 \leq G$  undergr (T.5.14)  
 $(SO(2, \mathbb{R}) = O(2, \mathbb{R}) \cap SL(2, \mathbb{R}))$

Sykliske undergr: La  $G$  være en (mult.)gruppe og  $a \in G$ . La  $H \leq G$  være en undergr med  $a \in H$ . Da har vi også  $a^{-1} \in H$ , og  $e = a^0 \in H$ . Siden  $H$  er lukket under mult (bin.op) er

$$a^n \in H$$

$$a^{-n} = (a^{-1})^n \in H$$

$\forall n \in \mathbb{N}$ . Derfor:

$$\langle a \rangle \stackrel{\text{def}}{=} \{a^t \mid t \in \mathbb{Z}\} \subseteq H.$$

Teorem 5.17  $\langle a \rangle$  er en undergr av  $H$ . (og døres også av  $G$ )

Def: (1)  $\langle a \rangle$  kallas den sykliske undergr av  $G$  generert av  $a$ . Merk at hvis  $H \leq G$  och  $a \in H$ , så är  $\langle a \rangle \leq H$ , dvs  $\langle a \rangle$  är den minste undergr av  $G$  som inneh.  $a$ .

(2)  $G$  är syklisk hvis  $\exists a \in G$  med  $\langle a \rangle = G$ . Da är  $a$  en generator för  $G$ .

Merk: (1) En syklisk gruppe kan ha flera generatorer

(2)  $\langle a \rangle$  kan vara endelig, dvs ofta slike att  $a^t = a^s$  för  $t \neq s$ .

Eksempler: (1) For gruppen  $\mathbb{Z}_9$  är  $\langle 3 \rangle = \langle 6 \rangle = \{0, 3, 6\}$ . mens

$$\langle 1 \rangle = \langle 2 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 8 \rangle = \mathbb{Z}_9 \text{ og } \langle 0 \rangle = \{0\}$$

(2) For  $U_4 = \{z \in \mathbb{C} \mid z^4 = 1\} = \{1, -1, i, -i\}$  (med mult.) ∵

$$\langle 1 \rangle = \{1\}$$

$$\langle -1 \rangle = \{-1\}$$

$$\langle i \rangle = U_4$$

$$\langle -i \rangle = U_4$$

(3) For  $\mathbb{Z}$  är  $\langle 20 \rangle = \{\dots, -40, -20, 0, 20, 40, \dots\} = \{20m \mid m \in \mathbb{Z}\}$