Norges teknisk–naturvitenskapelige universitet
Institutt for matematikk

**Løsningsforslag — Øving 2**

## Oppgaver fra boka

$\boxed{5.23}$ For å finne gruppen generert av $A = \left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$, starter vi med å gange matrisen med seg selv for å se om vi finner et mønster:

$$A^2 = \begin{bmatrix}1 & 2\\0 & 1\end{bmatrix} \qquad A^3 = \begin{bmatrix}1 & 3\\0 & 1\end{bmatrix}.$$

Ved induksjon kan vi vise at for positive heltall $n$ er

$$A^n = \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}.$$

Ved å invertere $A^n$ finner vi at for positive heltall $n$ er

$$A^{-n} = \begin{bmatrix}1 & -n\\0 & 1\end{bmatrix}.$$

Følgelig har vi at

$$G = \left\langle \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix} \right\rangle = \left\{ \begin{bmatrix}1 & n\\0 & 1\end{bmatrix} \middle| n \in \mathbb{Z} \right\}$$

$\boxed{5.42}$ Vi antar at $\phi : G \to G'$ er en isomorfi av grupper, og at gruppen $G$ er syklisk. La $g$ være en generator for $G$.

La $x' \in G'$. Da har vi at:

$$\begin{aligned} x' &= \phi(x) && x \in G, \text{ fordi } \phi \text{ er en isomorfi} \\ &= \phi(g^n) && n \in \mathbb{Z} \\ &= \phi(g)^n && \text{fordi } \phi \text{ er en isomorfi} \end{aligned}$$

Følgelig er $G'$ generert av $\phi(g)$ og dermed syklisk.

$\boxed{5.53}$ For å sjekke om en relasjon er en ekvivalensrelasjon, må vi sjekke at den er refleksiv, symmetrisk og transitiv:

refleksiv: For $a \in G$ er $aa^{-1} = e \in H$, dermed er $a \sim a$.

symmetrisk: Om $a \sim b$ vet vi at $ab^{-1} \in H$. Men da er $ba^{-1} = (ab^{-1})^{-1} \in H$, og $b \sim a$.

transitiv: Om $a \sim b$, $b \sim c$ vet vi at $ab^{-1} \in H$ og $bc^{-1} \in H$. Da er $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$.

$\boxed{6.14}$ Vi ønsker å finne alle automorfiene på $\mathbb{Z}_8$. Når vi ser på oppgave 5.42 ser vi hvis $\phi : G \to G'$ er en isomorfi, og $g \in G$ er en generator, så må også $\phi(g)$ være en generator. Videre ser vi i oppgave 6.44 at en isomorfi fra en syklisk gruppe er bestemt av hva den gjør med én generator for gruppen.

Generatorene i $\mathbb{Z}_8$ er $\{1, 3, 5, 7\}$. Om vi tar utgangspunkt i 1, ser vi at det kun er fire mulige elementer 1 kan vi bli sendt til. Dermed er det fire automorfier på $\mathbb{Z}_8$.

$\boxed{6.44}$ Anta at $G$ er en syklisk gruppe generert av $g \in G$. Vi skal vise at en isomorfi fra $G$ til $G'$ er unikt bestemt av hva den gjør med generatoren $g$. Med andre ord: Dersom to isomorfier $\phi$ og $\psi$ er slik at $\phi(g) = \psi(g)$, så er $\phi = \psi$. De to isomorfiene $\phi$ og $\psi$ er like dersom $\phi(x) = \psi(x)$ for alle $x \in G$. Vi bruker at enhver $x \in G$ kan skrives som $x = g^n$ for en $n \in \mathbb{Z}$, og antar at $\phi(g) = \psi(g)$. Vi har da at:

$$\phi(x) = \phi(g^n) = \phi(g)^n = \psi(g)^n = \psi(g^n) = \psi(x).$$

**Eksamen vår 2013**

$\boxed{2}$ Vi antar at $G$ er en gruppe med identitetselement $e$, og at $n \geq 2$ er et heltall. Videre definerer vi:

$$H_n = \{x \in G | x^n = e\}$$

**a)** Anta at G er abelsk. Vi viser at $H_n$ er en undergruppe av $G$ ved å bruke teorem 5.14 i boka.

Lukket under binæroperasjon: Dersom $x, y \in H^n$ så har vi at

$$(xy)^n = x^n y^n = ee = e,$$

så $xy \in H^n$.

Inneholder identitetselementet: $e^n = e$, så $e \in H^n$.

Inneholder inverser: Dersom $x \in H^n$, og $x'$ er inversen til $x$, så har vi at

$$(x')^n = (x')^n e = (x')^n x^n = (x'x)^n = e.$$

Dermed er $x' \in H^n$.

**b)** Her er det nok å finne et moteksempel. Siden vi vet at $H_n$ alltid er en undergruppe for abelske grupper, bør vi lete etter en ikke-abelsk gruppe $G$. Vi kan da velge $GL_2(\mathbb{R}$, gruppen av reelle, inverterbare matriser under multiplikasjon. Etter litt mere leting finner vi at

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

er elementer i $H_2$, men siden

$$(AB^2) = \left( \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \right)^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

kan $AB$ ikke være inneholdt i $H_2$. $H_2$ er ikke lukket under binæroperasjoner, og dermed ikke en undergruppe.

## Ekstraoppgaver

$\boxed{1}$ **a)** Anta først at $m \in \mathbb{Z}_n$ er en generator; da vet vi at $m$ har orden $n$, og at $m, 2m, \ldots, (n-1)m \nmid n$. Anta nå at $gcd(n,m) = x$: vi har at $\frac{n}{x}$ er et heltall og at $1 \leq \frac{n}{x} < n$. Anta videre at $x \neq 1$. Da er et av elementene $m, 2m, \ldots, (n-1)m$ lik $\frac{n}{x}m = \frac{n}{x}x\frac{m}{x} = n\frac{m}{x}$, der også $\frac{m}{x}$ er et heltall. Dermed får vi at $\frac{n}{x}m|n$, som gir en selvmotsigelse. Det følger at $x = 1$.

Anta nå at $m \in \mathbb{Z}_n$ er slik at $\gcd(m,n) = 1$. Vi har da at $am = bn$ for positive heltall $a, b$ hvis og bare hvis $a|n$; følgelig har $m$ minst orden $n$, og genererer dermed $\mathbb{Z}_n$.

**b)**

| Undergruppe | Generatorer | Elementer |
|---|---|---|
| $\mathbb{Z}_{p^3}$ | $np + m$, hvor $n, m \in \mathbb{Z}, 1 \leq m \leq p-1$ | $0, 1, \ldots, p^3 - 1$ |
| $\langle p \rangle$ | $np$, hvor $n \in \mathbb{Z}, \gcd(n,p) = 1$ | $0, p, 2p, \ldots, p^3 - p$ |
| $\langle p^2 \rangle$ | $np^2$, hvor $n \in \mathbb{Z}, \gcd(n,p) = 1$ | $0, p^2, 2p^2, \ldots, p^3 - p^2$ |
| $0$ | $0$ | $0$ |

**c)**

| Undergruppe | Generatorer | Elementer |
|---|---|---|
| $\mathbb{Z}_{pq}$ | Alle elementer som ikke er på formen $np$ eller $nq$ for $n \in \mathbb{Z}$ | $0, 1 \ldots, pq - 1$ |
| $\langle p \rangle$ | Alle elementer på formen $np$ hvor $n \in \mathbb{Z}, \gcd(n,q) = 1$ | $0, p, \ldots, (q-1)p$ |
| $\langle p \rangle$ | Alle elementer på formen $nq$ hvor $n \in \mathbb{Z}, \gcd(n,p) = 1$ | $0, q, \ldots, (p-1)q$ |
| $\{0\}$ | $0$ | $0$ |