MAT230 — Grupper og symmetri

Obligatorisk innlevering 1

Christian Stigen
UiS, 22. februar, 2016

Oppgave 1a

Vi ser umiddelbart at identitetselementet $e = 1$ som tilfredstiller $xe = x = ex$ (bevis under) og skriver ut multiplikasjonstabellen, for å gjøre resten enklere.

	e	4	7	13
e	e	4	7	13
4	4	e	13	7
7	7	13	4	e
13	13	7	e	4

G er en gruppe under multiplikasjon modulo 15 fordi

- vi har et unikt identitetselement $e = 1 \in G$ som tilfredstiller $xe = x = ex$, fordi $x \cdot 1 \mod n = 1 \cdot x \mod n = x \mod n$,
- multiplikasjonen modulo 15 er *lukket*, altså vil $a \cdot_{15} b \in G$ for alle $a, b \in G$ (det ser vi av tabellen),
- hvert element har en *invers* x^{-1} slik at $x^{-1}x = e = xx^{-1}$ fordi $1 \cdot 1 = e$, $4 \cdot 4 = e$, $7 \cdot 13 = e = 13 \cdot 7$ (vi gir ingen generell operasjon for dette; siden gruppen vår er så liten er det nok å gå gjennom alle mulighetene),
- multiplikasjon modulo 15 er *assosiativ*, altså $(xy)z = x(yz)$ eller $(x \cdot_n y) \cdot_n z = x \cdot_n (y \cdot_n z)$ (se merknad under).

Assosivitet for multiplikasjon modulo n kan bevises på flere måter. Den *minst* tilfredstillende jeg fant*, men som også er enklest, er å bruke $[\![a]\!]_n \equiv a$

*Se `https://proofwiki.org/wiki/Modulo_Multiplication_is_Associative`

$\mod n$. Gitt $x, y, z < n$ har vi

$$[\![a]\!]_n \cdot_n [\![b]\!]_n \equiv [\![ab]\!]_n$$

$$\begin{aligned}
([\![x]\!]_n \cdot_n [\![y]\!]_n) \cdot_n [\![z]\!]_n &= [\![xy]\!]_n \cdot_n [\![z]\!]_n \\
&= [\![(xy)z]\!]_n && \text{per definisjon} \\
&= [\![x(yz)]\!]_n && \text{assosivitet for heltallsmultiplikasjon} \\
&= [\![x]\!]_n \cdot_n [\![yz]\!]_n \\
&= [\![x]\!]_n \cdot_n ([\![y]\!]_n \cdot_n [\![z]\!]_n)
\end{aligned}$$

Oppgaven ber vel ikke eksplisitt om å føre et slikt bevis, så derfor er jeg såpass unøyaktig og stjeler et bevis fra før. Det som står i boken for addisjon (Armstrong, s. 13) kunne også blitt brukt, men jeg synes den over er enklere.

Oppgave 1b

- $1^1 = e$ og har dermed orden 1.
- $4^2 = e$ og har dermed orden 2.
- $7^4 = e$ og har dermed orden 4.
- $13^4 = e$ og har dermed orden 4.

Oppgave 1c

En undergruppe er et subsett av G som også er en gruppe under multiplikasjon modulo 15. Det eneste identitetselementet som er aktuelt er 1, dermed må dette være med i en undergruppe. Gruppen må være *lukket*, og dermed finner jeg at de eneste undergruppene er $\{1\}$ og $\{1, 4\}$.

Sistnevnte har en triviell multiplikasjonstabell,

	e	4
e	e	4
4	4	e

Oppgave 2a

Vi vet at $sr = r^{-1}s$, dermed vil $(r^3s)r = (r^3)sr = (r^3)r^{-1}s = r^2s$, og vi får

$$\begin{aligned}
(r^3s)\mathbf{r} &= (r^3)sr = (r^3)r^{-1}s = r^2s \\
(r^2s)\mathbf{r} &= (r^2)r^{-1}s = rs \\
(rs)\mathbf{r} &= rr^{-1}s = es = s \\
s\mathbf{s} &= s^2 = e && \text{fordi } s \text{ har orden 2}
\end{aligned}$$

Med andre ord er r^3s sin egen invers: $(r^3s)(r^3s) = e$.

Oppgave 2b

$$\begin{aligned}
(r^2s)(r^3s) &= (r^2s)r(r^2s) = (r^2sr)(r^2s) \\
&= (r^2r^{-1}s)(r^2s) && \text{fordi } sr = r^{-1}s \\
&= (rs)(r^2s) = (rs)r(rs) = (rsr)(rs) \\
&= (rr^{-1}s)(rs) = (es)(rs) = s(rs) \\
&= sr(s) = r^{-1}ss \\
&= r^{-1}e && \text{fordi } s \text{ har orden 2, } s^2 = e \\
&= r^{-1} = er^{-1} \\
&= r^4r^{-1} && \text{fordi } r \text{ har orden 4, } r^4 = e \\
&= r^3
\end{aligned}$$

Oppgave 2c

Vi vet at $r^4 = e$ og dermed må $r^{4k} = e$ for $k \in \mathbb{Z}$. Da $12 = 3 \cdot 4$ må $(r^3)^4 = r^4 = e$. Altså har r^3 orden 4.

For r^2s prøver vi oss fram

$$\begin{aligned}
(r^2s)^2 &= (r^2s)(r^2s) = (r^2sr)(rs) = (r^2r^{-1}s)(rs) \\
&= (rs)(rs) = (rsr)s = (rr^{-1}s)s = (es)s \\
&= ss = s^2 = e
\end{aligned}$$

Med andre ord har (r^2s) orden 2.

Oppgave 3a

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 3 & 5 & 1 & 7 & 6 & 2 \end{bmatrix} = (145)(28)(67)$$

Oppgave 3b

Vi snakker fremdeles om S_8,

$$\begin{aligned}(148)(2478) &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 3 & 8 & 5 & 6 & 7 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 7 & 5 & 6 & 8 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 3 & 7 & 5 & 6 & 1 & 2 \end{bmatrix} = (147)(28)\end{aligned}$$

Oppgave 3c

$$(14)(257) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 3 & 1 & 7 & 6 & 2 & 8 \end{bmatrix}$$

Oppgave 3d

Ikke utført.