27. mars 2026

# MAT2200 — Grupper, ringer og kropper

Obligatorisk oppgave 2 av 2

### Innleveringsfrist

Torsdag 9. april 2026, 14.30 i Canvas (canvas.uio.no).

Løsninger kan skrives på norsk eller engelsk. Ethvert forsøk på besvart oppgave vil godkjennes.

### Fullstendige retningnslinjer om obligatoriske oppgaver:

https://www.uio.no/studier/eksamen/obligatoriske-aktiviteter/mn-math-oblig.html

**Problem 1.** La $G$ og $H$ være endelige grupper, og la $\phi\colon G \to H$ være en gruppehomomorfi.

(a) Bruk Lagranges teorem og fundamentalteoremet for gruppehomomorfier til å vise at $|G|/|\ker\phi|$ deler $|H|$.

(b) Anta nå at $\gcd(|G|, |H|) = 1$. Vis at da er $\phi$ den trivielle homomorfien, det vil si $\phi(g) = e$ for alle $g \in G$.

**Problem 2.** La $R$ og $S$ være ringer med identitetselementer $1_R \in R$ og $1_S \in S$, slik at $1_S \neq 0$. La $\phi\colon R \to S$ være en ringhomomorfi slik at $\phi(1_R) = 1_S$.

(a) Vis at hvis $r \in R$ er en enhet[1], så er $\phi(r)$ en enhet i $S$.

(b) Vis at hvis $R$ er en kropp, så er $\phi$ injektiv.

(c) Vis at den motsatte implikasjonen fra punkt (a) ikke er sann, det vil si: Finn et eksempel på en ringhomomorfi $\phi\colon R \to S$ med $\phi(1_R) = 1_S \neq 0$ og en $r \in R$ slik at $\phi(r)$ er en enhet i $S$, men $r$ er ikke en enhet i $R$.

*Hint:* Du kan finne et eksempel med $R = \mathbb{Z}$.

**Problem 3.** Se på produktringen $\mathbb{Z} \times \mathbb{Z}$, og la

$$R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \equiv n \pmod 2\} \subseteq \mathbb{Z} \times \mathbb{Z}.$$

(a) Vis at $R$ er en underring av $\mathbb{Z} \times \mathbb{Z}$.

(b) Finn alle 0-divisorer i $R$.

**Problem 4.** La $F$ være en kropp. Vi sier at $a \in F$ er et kvadrat hvis det finnes en $b \in F$ slik at $a = b^2$.

(a) Vis at $a \in F$ er et kvadrat hvis og bare hvis polynomet $x^2 - a \in F[x]$ er redusibelt.

La nå $p \geq 3$ være et primtall og la $a \in \mathbb{Z}_p$ med $a \neq 0$.

(b) Vis at hvis $a$ er et kvadrat, så er $a^{\frac{p-1}{2}} = 1$.

(c) Vis at hvis $a^{\frac{p-1}{2}} = 1$, så er $a$ et kvadrat.

*Hint:* Bruk Korollar 23.6 fra boken som sier at den multiplikative gruppen $\mathbb{Z}_p^*$ er syklisk, og skriv $a$ som $g^k$ for en generator $g$ av $\mathbb{Z}_p^*$.

[1] Altså det som på engelsk kalles *unit*.