13. april 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 ϕ den trivielle homomorfien, det vil si $\phi(g) = e$ for alle $g \in G$.

Løsninger:

(a) Ved fundamentalteoremet for gruppehomomorfier har vi at

$$G/\ker\phi \simeq \phi(G).$$

Siden $\phi(G)$ er en undergruppe av H, sier Lagranges teorem at $|\phi(G)|$ deler $|H|$. Det følger at

$$|G|/|\ker\phi| = |G/\ker\phi| = |\phi(G)|$$

deler $|H|$.

(b) La $k = |G|/|\ker\phi| = |\phi(G)|$. Da deler k både $|G|$ og $|H|$, så vi må ha $k = 1$. Dermed er $|\ker\phi| = |G|$, så vi må ha at $\ker\phi = G$. Dette betyr at $\phi(g) = e$ 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 ϕ 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 $R = \mathbb{Z}$.

Løsninger:

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

(a) Siden r er en enhet, så finnes det et element $r^{-1} \in R$ slik at $rr^{-1} = r^{-1}r = 1$. Da har vi

$$\phi(r^{-1})\phi(r) = \phi(r^{-1}r) = \phi(1) = 1$$

og

$$\phi(r)\phi(r^{-1}) = \phi(rr^{-1}) = \phi(1) = 1,$$

så $\phi(r^{-1})$ er en multiplikativ invers til $\phi(r)$. Dermed er $\phi(r)$ en enhet.

(b) Vi viser først at 0 ikke er en enhet i S. La $s \in S$. Siden $0 \neq 1$ i S, har vi at

$$0s = 0 \neq 1,$$

og dermed er s ikke en multiplikativ invers til 0. Siden dette gjelder for alle $s \in S$, har 0 ingen multiplikativ invers, så 0 er ikke en enhet.

La nå $0 \neq r \in R$. Siden R er en kropp, er r en enhet, og dermed er $\phi(r) \in S$ en enhet ved forrige deloppgave. Dermed er også $\phi(r) \neq 0$.

Det følger at $\ker \phi = \{0\}$, som betyr at ϕ er injektiv.

(c) La $\phi\colon \mathbb{Z} \to \mathbb{Q}$ være homomorfien gitt ved $\phi(n) = n/1$. Da er 2 ikke en enhet i $\mathbb{Z}$, men $\phi(2) = 2/1$ er en enhet i $\mathbb{Q}$.

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.

Løsninger:

(a) Vi viser først at R er en undergruppe av $\mathbb{Z} \times \mathbb{Z}$ med addisjon.

R inneholder den additive identiteten: Siden $0 \equiv 0 \pmod 2$, har vi $(0, 0) \in R$.

R inneholder additive inverser: For $(m, n) \in R$, har vi $m \equiv n \pmod 2$, og det følger at $-m \equiv -n \pmod 2$, slik at $-(m, n) = (-m, -n) \in R$.

R er lukket under addisjon: La $(m_1, n_1), (m_2, n_2) \in R$. Siden $m_1 \equiv n_1 \pmod 2$ og $m_2 \equiv n_2 \pmod 2$, har vi at

$$m_1 + m_2 \equiv n_1 + n_2 \pmod 2,$$

og dermed er

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2) \in R.$$

Vi viser nå at R er lukket under multiplikasjon. La $(m_1, n_1), (m_2, n_2) \in R$. Siden $m_1 \equiv n_1 \pmod 2$ og $m_2 \equiv n_2 \pmod 2$, har vi at $m_1 m_2 \equiv n_1 n_2 \pmod 2$, og dermed er

$$(m_1, n_1)(m_2, n_2) = (m_1 m_2, n_1 n_2) \in R.$$

Dermed er R en underring av $\mathbb{Z} \times \mathbb{Z}$.

(b) La $(m, n) \in R$ være et element. Vi ser på fire tilfeller:

a) $m \neq 0, n \neq 0$: Hvis $0 \neq (m', n') \in R$, har vi enten $m' \neq 0$ eller $n' \neq 0$, og det følger at $mm' \neq 0$ eller $nn' \neq 0$. Dermed er $(m, n)(m', n') = (mm', nn') \neq 0$, så (m, n) er ikke en 0-divisor.

b) $m = 0, n \neq 0$: Vi har da $(m, n) \neq 0$ og $(2, 0)(m, n) = (2m, 0n) = (0, 0) = 0$, så (m, n) er en 0-divisor.

c) $m \neq 0, n = 0$: Vi har da $(m, n) \neq 0$ og $(0, 2)(m, n) = (0m, 2n) = (0, 0) = 0$, så (m, n) er en 0-divisor.

d) $m = 0, n = 0$: Elementet $(0, 0) = 0 \in R$ er ikke en 0-divisor per bokas (ikke helt universelt brukte) definisjon.

Mengden av 0-divisorer i R blir dermed

$$\{(m, 0) \mid m \equiv 0 \pmod 2\} \cup \{(0, n) \mid n \equiv 0 \pmod 2\} \setminus \{(0, 0)\}.$$

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 $\mathbb{Z}_p^*$.

Løsninger:

(a) Anta først at a er et kvadrat, og la $b \in F$ være slik at $b^2 = a$. Da har vi at

$$(x - b)(x + b) = x^2 - b^2 = x^2 - a,$$

så $x^2 - a$ er redusibelt.

Anta nå at $f(x) = x^2 - a$ er redusibelt. Siden graden til polynomet er 2, vet vi at det da må ha en rot i F, det vil si at det finnes en $b \in F$ slik at $f(b) = 0$. Dette betyr at $b^2 - a = 0$, som vil si at $a = b^2$, så a er et kvadrat.

(b) La $a = b^2$. Siden $a \neq 0$, har vi at $b \neq 0$. Da har vi at

$$a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{2\left(\frac{p-1}{2}\right)} = b^{p-1} = 1,$$

ved Fermats lille teorem.

(c) La g være en generator av $\mathbb{Z}_p^*$, og skriv a som g^k. Siden $a^{\frac{p-1}{2}} = 1$, har vi at

$$1 = (g^k)^{\frac{p-1}{2}} = g^{\frac{k(p-1)}{2}}.$$

Siden gruppen $\mathbb{Z}_p^*$ har orden $p - 1$, har vi at $g^n = 1$ hvis og bare hvis $p - 1$ deler n. Ved ligningen over vil dermed $p - 1$ dele $\frac{k(p-1)}{2}$, og altså er $k/2$ et heltall. Dermed er $a = \left(g^{k/2}\right)^2$, så a er et kvadrat.