UNIVERSITETET I OSLO

Det matematisk-naturvitenskapelige fakultet

Eksamen i:	MAT2200 — Grupper, ringer og kropper
Eksamensdag:	Mandag 8. juni 2026
Tid for eksamen:	15.00 – 19.00
Oppgavesettet er på 8 sider.	
Vedlegg:	Ingen
Tillatte hjelpemidler:	Ingen

Kontroller at oppgavesettet er komplett før
du begynner å besvare spørsmålene.

Eksamensoppgaven består av 12 deloppgaver som hver teller like mye. Oppgaven kan besvares på norsk eller engelsk. Husk at alle svar må begrunnes. Lykke til!

Oppgave 1

a

Oppgi alle abelske grupper av orden 12, opp til isomorfi.

Løsning: Vi kan faktorisere 12 i primpotenser på følgende måter

$$2 \times 2 \times 3 \text{ og } 4 \times 3,$$

som gir følgende to ikke-isomorfe abelske grupper av orden 12:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \text{ og } \mathbb{Z}_4 \times \mathbb{Z}_3.$$

Disse kan også beskrives annerledes (og slike beskrivelser godkjennes): Gruppen $\mathbb{Z}_4 \times \mathbb{Z}_3$ er isomorf med $\mathbb{Z}_{12}$, og gruppen $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ er isomorf med $\mathbb{Z}_2 \times \mathbb{Z}_6$.

---

b

For hver slik gruppe, oppgi om gruppen inneholder et element av orden 4.

Løsning: Vi viser at $\mathbb{Z}_4 \times \mathbb{Z}_3$ inneholder et element av orden 4 og at $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ ikke inneholder et element av orden 4.

I gruppen $\mathbb{Z}_4 \times \mathbb{Z}_3$ er $(1, 0)$ et element av orden 4, siden, for $i = 1, 2, 3$, har vi at

$$i \cdot (1, 0) = (i \cdot 1, i \cdot 0) = (i, 0) \neq (0, 0)$$

(Fortsettes på side 2.)

mens

$$4 \cdot (1,0) = (4 \cdot 1, 4 \cdot 0) = (0,0).$$

Vi viser nå at i gruppen $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ finnes ikke noe element av orden 4. Anta for motsigelse at (a,b,c) er av orden 4. Da har vi at

$$4 \cdot (a,b,c) = (4 \cdot a, 4 \cdot b, 4 \cdot c) = (0,0,0),$$

så spesielt er $4 \cdot c = 0$ i $\mathbb{Z}_3$. Men for $1, 2 \in \mathbb{Z}_3$ har vi $4 \cdot 1 = 1, 4 \cdot 2 = 2$, så dette betyr at $c = 0$. Dermed er $(a,b,c) = (a,b,0)$, og vi får

$$2 \cdot (a,b,0) = (2 \cdot a, 2 \cdot b, 0) = (0,0,0),$$

altså har $(a,b,0)$ orden høyst 2. Dette er en motsigelse.

Oppgave 2

Si at en **partisjon** av mengden $\{1,2,3,4\}$ er en mengde $\{A,B\}$, hvor A og B er disjunkte delmengder av $\{1,2,3,4\}$ med $|A| = |B| = 2$. La X være mengden av slike partisjoner, det vil si

$$X = \{\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\}.$$

For $\sigma \in S_4$ og $\{\{a,b\},\{c,d\}\} \in X$, la

$$\sigma \cdot \{\{a,b\},\{c,d\}\} = \{\{\sigma(a),\sigma(b)\},\{\sigma(c),\sigma(d)\}\}.$$

a

Vis at dette definerer en gruppevirkning av S_4 på X.

Løsning: Vi skriver σx for $\sigma \cdot x$, og vi må vise at avbildningen

$$(\sigma, x) \mapsto \sigma x \quad \sigma \in S_4, x \in X$$

tilfredsstiller de to aksiomene for en gruppevirkning, altså

$$ex = x \qquad \forall x \in X$$

og

$$\sigma_1(\sigma_2 x) = (\sigma_1\sigma_2)x \qquad \forall \sigma_1, \sigma_2 \in S_4, x \in X$$

For $x = \{\{a,b\},\{c,d\}\}$, har vi

$$ex = e\{\{a,b\},\{c,d\}\} = \{\{e(a),e(b)\},\{e(c),e(d)\}\} = \{\{a,b\},\{c,d\}\} = x.$$

For $\sigma_1, \sigma_2 \in S_4$ har vi

$$\begin{aligned}
\sigma_1(\sigma_2 x) &= \sigma_1\{\{\sigma_2(a),\sigma_2(b)\},\{\sigma_2(c),\sigma_2(d)\}\} \\
&= \{\{\sigma_1(\sigma_2(a)),\sigma_1(\sigma_2(b))\},\{\sigma_1(\sigma_2(c)),\sigma_1(\sigma_2(d))\}\} \\
&= \{\{(\sigma_1\sigma_2)(a),(\sigma_1\sigma_2)(b)\},\{(\sigma_1\sigma_2)(c),(\sigma_1\sigma_2)(d)\}\} \\
&= (\sigma_1\sigma_2)\{\{a,b\},\{c,d\}\} = (\sigma_1\sigma_2)x
\end{aligned}$$

(Fortsettes på side 3.)

For $\sigma \in S_4$, la

$$X_\sigma = \{x \in X \mid \sigma x = x\},$$

og la

$$H = \{\sigma \in S_4 \mid X_\sigma = X\},$$

det vil si at H er mengden av de $\sigma \in S_4$ som fikserer hele X.

b

Vi oppgir (og du kan bruke) at H har nøyaktig fire elementer. Finn disse.

Løsning: Vi påstår at H består av

$$e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3).$$

Siden vi har fått oppgitt at H inneholder 4 elementer, holder det å sjekke at disse 4 elementene ligger i H, altså at de tilfredsstiller $X_\sigma = X$. For alle $x \in X$ har vi som en konsekvens av aksiomene for en gruppevirkning at $ex = x$, så dermed er $X_e = X$.

Vi viser nå at for $\sigma = (1,2)(3,4)$, gjelder $X_\sigma = X$:

$$\sigma\{\{1,2\},\{3,4\}\} = \{\{2,1\},\{3,4\}\} = \{\{1,2\},\{3,4\}\}$$
$$\sigma\{\{1,3\},\{2,4\}\} = \{\{2,4\},\{1,3\}\} = \{\{1,3\},\{2,4\}\}$$
$$\sigma\{\{1,4\},\{2,3\}\} = \{\{2,3\},\{1,4\}\} = \{\{1,4\},\{2,3\}\}$$

Tilsvarende utregninger viser at $(1,3)(2,4)$ og $(1,4)(2,3)$ ligger i H.

---

c

Vis at H er en normal undergruppe av S_4.

Løsning: Vi viser først at H er en undergruppe av S_4. Vi har $e \in H$. Hvis $\sigma \in H$, har vi for alle $x \in X$ at

$$\sigma x = x,$$

som impliserer at

$$\sigma^{-1}x = \sigma^{-1}(\sigma x) = (\sigma^{-1}\sigma)x = ex = x.$$

Dermed ligger $\sigma^{-1} \in H$. Hvis $\sigma_1, \sigma_2 \in H$ og $x \in X$, har vi at

$$(\sigma_1\sigma_2)x = \sigma_1(\sigma_2 x) = \sigma_1 x = x,$$

som betyr at $\sigma_1\sigma_2 \in H$. Dermed har vi vist at H er en undergruppe, og det gjenstår å vise at H er normal.

Hvis $\tau \in S_4, \sigma \in H$ og $x \in X$, har vi at

$$(\tau\sigma\tau^{-1})x = \tau(\sigma(\tau^{-1}x)) = \tau(\tau^{-1}x) = (\tau\tau^{-1})x = ex = x.$$

Dermed ligger $\tau\sigma\tau^{-1} \in H$; dette viser at H er normal.

Alternative løsninger:

(Fortsettes på side 4.)

- Det at H er en undergruppe kan sjekkes direkte ved beskrivelsen av elementene vi har fra oppgave b og multiplikasjon i S_4.
- Normalitet av H kan vises ved å bruke at vi kjenner elementene, på følgende måte: For $(i,j)(k,l) \in H$ og $\tau \in S_4$, har vi at

$$\tau(i,j)(k,l)\tau^{-1} = (\tau(i),\tau(j))(\tau(k),\tau(l)) \in H$$

- Hele oppgave c kan også løses slik: Vi har en korrespondanse mellom gruppevirkninger av S_4 på X og homomorfier $S_4 \to S_X$. Oppgavens gruppevirkning svarer til homomorfien $\phi\colon S_4 \to S_X$ hvor $\phi(\sigma) \in S_X$ er slik at

$$\phi(\sigma)(x) = \sigma x \qquad x \in X$$

  Betingelsen $\sigma \in H$ er ekvivalent med $\sigma x = x$ for alle x, som er ekvivalent med $\phi(\sigma) = e \in S_X$. Dermed er $H = \ker\phi$, og altså en normal undergruppe.

Oppgave 3

a

Finn alle $x \in \mathbb{Z}_7$ slik at $x^{86} = 1$.

Løsning: Vi ser først at $x = 0$ ikke er en løsning av ligningen, så vi antar heretter at $x \neq 0$.

Siden $86 = 84 + 2 = 6 \times 14 + 2$, har vi i $\mathbb{Z}_7$

$$x^{86} = (x^6)^{14}x^2 = 1^{14}x^2 = x^2,$$

hvor vi bruker Fermats teorem, som sier at $x^6 = 1$ i $\mathbb{Z}_7$ siden 7 er prim og $x \neq 0$. Dermed blir ligningen ekvivalent med $x^2 = 1$. Denne kan vi løse ved å regne ut x^2 for alle $x \in \mathbb{Z}_7$, vi har

$$1^2 = 1, 2^2 = 4, 3^2 = 2, 4^2 = 2, 5^2 = 4, 6^2 = 1.$$

Løsningene blir altså $x = 1$ og $x = 6$.

---

b

La p være et primtall, la $k \in \{1,\ldots,p-2\}$, la $q \in \mathbb{N}$, og la $n = q(p-1)+k$. La $a \in \mathbb{Z}_p$. Vis at ligningen $x^n = a$ har maksimalt k løsninger for $x \in \mathbb{Z}_p$.

Løsning: Hvis $a = 0$, har vi siden $\mathbb{Z}_p$ er en kropp at $x^n = 0$ impliserer $x = 0$, så da finnes bare en løsning, altså er antall løsninger mindre enn eller lik k.

Vi antar heretter at $a \neq 0$. Da må vi ha $x \neq 0$, og som i punkt a finner vi at

$$x^n = x^{q(p-1)+k} = (x^{p-1})^q x^k = 1^q x^k = x^k,$$

(Fortsettes på side 5.)

så ligningen $x^n = a$ er ekvivalent med $x^k = a$. Løsninger av denne ligningen er det samme som røtter av polynomet $x^k - a$, og siden $\mathbb{Z}_p$ er en kropp, finnes det maksimalt k røtter av et polynom av grad k.

Oppgave 4

La S være en mengde, og la A_S være ringen av alle funksjoner $f\colon S \to \mathbb{R}$, med punktvis addisjon og multiplikasjon definert som vanlig for funksjoner.

a

Vis at A_S er et integritetsområde hvis og bare hvis S inneholder nøyaktig ett element.

Løsning: Hvis $S = \emptyset$, finnes nøyaktig én funksjon $f\colon \emptyset \to \mathbb{R}$, dermed er A_S 0-ringen, som ikke er et integritetsområde.

Hvis S har ett element, si $S = \{x\}$, har vi at $f\colon S \to \mathbb{R}$ er entydig bestemt av $f(x)$. Dette gir en isomorfi $A_S \simeq \mathbb{R}$, og siden $\mathbb{R}$ er et integritetsområde, så er A_S det også.

Hvis S har mer enn ett element, kan vi se på $x_1, x_2 \in S$ med $x_1 \neq x_2$. La $f_1, f_2\colon S \to \mathbb{R}$ være gitt ved

$$f_i(x) = \begin{cases} 1 \text{ hvis } x = x_i \\ 0 \text{ hvis } x \neq x_i. \end{cases}$$

Da er $f_1 \neq 0 \neq f_2$, og $(f_1 f_2)(x) = 0$ for alle $x \in S$, som vil si at $f_1 f_2 = 0$. Dermed er f_1, f_2 nulldivisorer i A_S, så A_S er ikke et integritetsområde.

---

b

La $T \subseteq S$, og la

$$I_T = \{f \in A_S \mid f(t) = 0 \text{ for alle } t \in T\}.$$

Vis at I_T er et ideal i A_S og at $A_S/I_T \simeq A_T$.

Løsning: Vi ser på avbildningen $\phi\colon A_S \to A_T$ gitt ved begrensning av domene, det vil si at for $f \in A_S$ og $x \in T$ lar vi

$$\phi(f)(x) = f(x).$$

Vi har nå for $f, g \in A_S$ at $\phi(f) + \phi(g) = \phi(f+g)$ og $\phi(f)\phi(g) = \phi(fg)$, så ϕ er en ringhomomorfi. Vi har at

$$f \in \ker\phi \Leftrightarrow f(t) = 0 \ \forall t \in T \Leftrightarrow f \in I_T,$$

som vil si at $I_T = \ker\phi$. Dermed er I_T et ideal.

(Fortsettes på side 6.)

For $f \in A_T$, kan vi la $g \in A_S$ være definert ved

$$g(x) = \begin{cases} f(x) \text{ hvis } x \in T \\ 0 \text{ hvis } x \notin T, \end{cases}$$

Da har vi $\phi(g) = f$, og siden dette gjelder for alle f, er ϕ surjektiv.

Nå gir fundamentalteoremet for ringhomomorfier at

$$A_S/I_T = A_S/\ker\phi \simeq \phi(A_S) = A_T.$$

Oppgave 5

La $\omega = e^{\frac{2\pi i}{7}} \in \mathbb{C}$, og la $E = \mathbb{Q}(\omega)$. Polynomet

$$\Phi_7(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

er irredusibelt over $\mathbb{Q}$, og dette kan brukes uten bevis.

a

Vis at E er rotkroppen til $\Phi_7(x)$ over $\mathbb{Q}$.

Løsning: Røttene til $x^7 - 1$ i $\mathbb{C}$ er sjuenderøtter av 1, altså $e^{\frac{2\pi ik}{7}} = \omega^k$ for $k = 0, \ldots, 6$. Dermed har vi faktoriseringen

$$x^7 - 1 = \prod_{k=0}^{6}(x - \omega^k),$$

som gir faktoriseringen

$$\Phi_7(x) = \prod_{k=1}^{6}(x - \omega^k).$$

Altså er røttene til $\Phi_7(x)$ gitt ved $\omega, \omega^2, \ldots, \omega^6$, og rotkroppen til $\Phi_7(x)$ over $\mathbb{Q}$ er

$$F := \mathbb{Q}(\omega, \omega^2, \ldots, \omega^6).$$

Siden $\omega \in F$, har vi $E \subseteq F$, og siden $\omega^i \in E$ for $i = 1, \ldots, 6$ har vi $F \subseteq E$. Dermed er $E = F$, som var det vi ville vise.

---

b

Vis at det finnes en automorfi $\sigma \in G(E/\mathbb{Q})$ med $\sigma(\omega) = \omega^3$, og at σ har orden 6. Vis at $G(E/\mathbb{Q}) \simeq \mathbb{Z}_6$.

(Fortsettes på side 7.)

Løsning: I forrige oppgave viste vi at både ω og ω^3 er røtter av $\Phi_7(x)$, og siden $\Phi_7(x)$ er irredusibelt over $\mathbb{Q}$, så er ω og ω^3 konjugerte over $\mathbb{Q}$. Dermed finnes en unik homomorfi av kropper

$$\sigma\colon E = \mathbb{Q}(\omega) \to \mathbb{Q}(\omega^3)$$

som fikserer $\mathbb{Q}$ og som er slik at $\sigma(\omega) = \omega^3$.

Siden $\omega^3 \in E$, så er $\mathbb{Q}(\omega^3) \subseteq E$. Dermed har σ bilde i E, og siden σ er injektiv og E er endelig-dimensjonal som vektorrom over $\mathbb{Q}$, så må σ være surjektiv.[1]

Vi vet at $\omega^7 = 1$, og får at

$$\begin{aligned}
\sigma^2(\omega) &= \sigma(\omega^3) = \omega^9 = \omega^2 \\
\sigma^3(\omega) &= \sigma(\omega^2) = \omega^6 \\
\sigma^4(\omega) &= \sigma(\omega^6) = \omega^{18} = \omega^4 \\
\sigma^5(\omega) &= \sigma(\omega^4) = \omega^{12} = \omega^5 \\
\sigma^6(\omega) &= \sigma(\omega^5) = \omega^{15} = \omega.
\end{aligned}$$

Siden $\sigma^i(\omega) \neq \omega$ for $i = 1, \ldots, 5$, har vi $\sigma^i \neq \mathrm{id}_E$ for $i = 1, \ldots, 5$. Siden $\sigma^6(\omega) = \omega$, har vi $\sigma^6 = \mathrm{id}_E$. Altså har σ orden 6.

Kroppsutvidelsen $\mathbb{Q} \leq E$ er separabel og en rotkropp, og dermed har vi

$$|G(E/\mathbb{Q})| = \{E : \mathbb{Q}\} = [E : \mathbb{Q}] = \deg \Phi_7(x) = 6.$$

Dermed er $G(E/\mathbb{Q}) = \langle\sigma\rangle \simeq \mathbb{Z}_6$.

---

c

La $K = \mathbb{Q}(\omega + \omega^6)$. Vis at

- $K \leq E$,
- $[K : \mathbb{Q}] = 3$,

og at K er den eneste kroppen med disse to egenskapene.

Løsning: Siden $\omega + \omega^6 \in E$, har vi at $K \leq E$. Enhver kropp $F \leq E$ har karakteristikk 0, og må dermed inneholde $\mathbb{Q}$. Kropper F som ligger mellom $\mathbb{Q}$ og E er i bijeksjon med undergrupper av $G(E/\mathbb{Q})$. Denne bijeksjonen sender F til $G(E/F)$ og er slik at $[F : \mathbb{Q}]$ er lik indeks av gruppen $G(E/F)$ i $G(E/\mathbb{Q})$.

Siden $\langle\sigma^3\rangle \leq G(E/\mathbb{Q}) = \langle\sigma\rangle$ er den unike undergruppen av indeks 3, har vi at det finnes en unik underkropp $E_{\langle\sigma^3\rangle}$ av E av grad 3 over $\mathbb{Q}$.

Det gjenstår å vise at $K = E_{\langle\sigma^3\rangle}$, eller ekvivalent at $G(E/K) = \langle\sigma^3\rangle$. Vi har $\omega^6 = \omega^{-1}$, og dermed at

$$\sigma^3(\omega + \omega^6) = \sigma^3(\omega + \omega^{-1}) = \omega^6 + \omega^{-6} = \omega + \omega^{-1} = \omega + \omega^6.$$

[1] *Alternativt:* Siden E er en rotkropp, og σ er en homomorfi fra E inn i den algebraiske tillukningen $\overline{\mathbb{Q}}$, så må σ være en automorfi.

(Fortsettes på side 8.)

Dermed vil $\sigma^3 \in G(E/\mathbb{Q})$ fiksere K, så $\sigma^3 \in G(E/K)$. Siden σ^3 har orden 2, vil 2 dele $|G(E/K)|$, altså er $G(E/K)$ enten lik $\langle\sigma^3\rangle$ eller $G(E/\mathbb{Q})$. Men

$$\sigma(\omega+\omega^6) = \sigma(\omega+\omega^{-1}) = \omega^3+\omega^{-3} = \omega^3+\omega^4 \neq \omega+\omega^6$$

siden

$$\omega^6-\omega^4-\omega^3+\omega = \omega(\omega^5-\omega^3-\omega^2+1),$$

og $1,\omega,\ldots,\omega^5$ er lineært uavhengige over $\mathbb{Q}$. Dermed har vi $G(E/K) = \langle\sigma^3\rangle$, så $[K:\mathbb{Q}] = 3$.

SLUTT

Ordliste

- kropp — field
- rotkropp — splitting field
- integritetsområde — integral domain
- gruppevirkning — group action