NTNU

Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i **TMA4150 Algebra**

Faglig kontakt under eksamen: Torkil Utvik Stai

Tlf: 47638459

Eksamensdato:

Eksamenstid (fra–til):

Hjelpemiddelkode/Tillatte hjelpemidler: D: Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

Målform/språk: bokmål

Antall sider: 4

Antall sider vedlegg: 0

Kontrollert av:

Informasjon om trykking av eksamensoppgave	
Originalen er:	
1-sidig ☐	**2-sidig** ☒
sort/hvit ☒	**farger** ☐
skal ha flervalgskjema ☐	

Dato Sign

Oppgave 1

(i) $12 = 2^2 \cdot 3$, så det finnes to abelske grupper av orden 12 opp til isomorfi, nemlig

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3;$$
$$\mathbb{Z}_4 \times \mathbb{Z}_3.$$

(ii) Et element i G er et inverterbart element i $\mathbb{Z}_{21}$, altså et element i $\mathbb{Z}_{21}$ som er relativt primisk til 21. Det betyr at $G = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

Observér at $\phi((1, 0)) := 13$ og $\phi((0, 1)) := 2$ entydig utvides til en gruppehomomorfi $\phi\colon \mathbb{Z}_2 \times \mathbb{Z}_6 \to G$. Det er rett fram å verifisere at $\ker \phi = \{(0, 0)\}$, som betyr at ϕ er injektiv. ϕ er dermed også surjektiv — fordi $|G| = |\mathbb{Z}_2 \times \mathbb{Z}_6|$ — så ϕ er en isomorfi. Altså er $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

Oppgave 2 D_8 virker på mengden X av alle fargelegginger av hjørnene til en regulær åttekant med tre farger tilgjengelig, det vil si $|X| = 3^8$. Antallet distinkte åttekanter er det samme som antallet baner r i X, som ved Burnsides formel er

$$\begin{aligned}
r &= \frac{1}{|D_8|} \sum_{g \in D_8} |X_g| \\
&= \frac{1}{16} \left(|X_{\rho_0}| + 4 \cdot |X_{\rho_1}| + 2 \cdot |X_{\rho_2}| + |X_{\rho_4}| + 4 \cdot |X_{\mu_h}| + 4 \cdot |X_{\mu_m}|\right) \\
&= \frac{1}{16} \left(3^8 + 4 \cdot 3 + 2 \cdot 3^2 + 3^4 + 4 \cdot 3^5 + 4 \cdot 3^4\right) \\
&= 498.
\end{aligned}$$

Oppgave 3

a) (i) Anta at $C(G) \subset N$. La $g \in G$ og $x \in N$. Da er

$$gxg^{-1} = gxg^{-1}x^{-1}x \in N,$$

fordi $gxg^{-1}x^{-1} \in C(G) \subset N$ og $x \in N$, så N er normal i G. For å se at G/N er abelsk, la $aN, bN \in G/N$. Siden $bab^{-1}a^{-1} \in C(G) \subset N$, blir

$N = bab^{-1}a^{-1}N$, og dermed

$$\begin{aligned}(aN)(bN) &= abN \\ &= N(abN) \\ &= (bab^{-1}a^{-1}N)(abN) \\ &= bab^{-1}a^{-1}abN \\ &= baN \\ &= (bN)(aN).\end{aligned}$$

(ii) Anta at N er normal i G og at G/N er abelsk. La $a, b \in G$ være vilkårlige. Da blir $abN = (aN)(bN) = (bN)(aN) = baN$. Dette impliserer $aba^{-1}b^{-1}N = N$, altså $aba^{-1}b^{-1} \in N$. Dermed er N en undergruppe som inneholder alle generatorene til $C(G)$, så $C(G) \subset N$.

b) Anta at G' er abelsk og at $\phi\colon G \to G'$ er en gruppehomomorfi. Ved første isomorfisetning er $G/\ker\phi \cong \operatorname{im}\phi$. $\operatorname{im}\phi$ er en undergruppe av G', så $\operatorname{im}\phi$ er abelsk. Dermed er $C(G) \subset \ker\phi$ ved **a)**(ii). Ved **a)**(i) er $C(G)$ en normal undergruppe av G, så $C(G)$ blir automatisk en normal undergruppe av $\ker\phi$.

Oppgave 4 En gruppe G er oppløsbar hvis den har en komposisjonsrekke med abelske komposisjonsfaktorer.

(i) La G være en gruppe med $|G| = p^n$. Ved 'Sylow I' har G en undergruppe P_{n-1} av orden p^{n-1}, og P_{n-1} er normal i en undergruppe av G av orden p^n, i.e. P_{n-1} er normal i G. På samme måte har P_{n-1} en undergruppe P_{n-2} av orden p^{n-2}, og P_{n-2} er normal i en undergruppe av P_{n-1} av orden p^{n-1}, i.e. P_{n-2} er normal i P_{n-1}. Hvis vi fortsetter slik, får vi en komposisjonsrekke

$$\{e\} < P_1 < \cdots < P_{n-2} < P_{n-1} < G$$

hvor hver komposisjonsfaktor har orden p, i.e. hver komposisjonsfaktor er isomorf med den abelske gruppa $\mathbb{Z}_p$. Altså er G oppløsbar.

(ii) La $n \geq 3$, og la $\rho_k \in D_n$ for $0 \leq k \leq n-1$ være rotasjon om sentrum i den regulære n-kanten med $2k\pi/n$ radianer mot klokka. Den sykliske undergruppa av D_n generert av ρ_1 er

$$\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2, \ldots, \rho_{n-1}\} \cong \mathbb{Z}_n.$$

Siden $|D_n| = 2n$, er $(D_n : \langle \rho_1 \rangle) = 2$, så $\mathbb{Z}_n$ er en normal undergruppe av D_n. Gruppen $\mathbb{Z}_n$ er opplagt oppløsbar: Enhver endelig gruppe har en komposisjonsrekke og enhver undergruppe eller faktorgruppe av en abelsk gruppe er abelsk. Det betyr at hvis $\{0\} < G_1 < \cdots G_t < \mathbb{Z}_n$ er en komposisjonsrekke for $\mathbb{Z}_n$, så vil

$$\{0\} < G_1 < \cdots G_t < \mathbb{Z}_n < D_n$$

være en komposisjonsrekke for D_n med abelske komposisjonsfaktorer (merk at $D_n/\mathbb{Z}_n \cong \mathbb{Z}_2$).

Oppgave 5 Det er klart at $e \in Z(S_n)$. La $\rho \in S_n \setminus \{e\}$. Da må det finnes $i, j \in \{1, \ldots, n\}$ med $i \neq j$ slik at $\rho(i) = j$. Siden $n \geq 3$ finnes det en $k \in \{1, \ldots, n\}$ som er forskjellig fra både i og j. Se på transposisjonen $\tau = (i, k) \in S_n$. Da blir

$$\tau\rho(i) = \tau(j) = j \text{ og } \rho\tau(i) = \rho(k) \neq j,$$

som betyr at $\rho\tau \neq \tau\rho$, i.e. $\rho \notin Z(S_n)$. Dermed er $Z(S_n) = \{e\}$.

Oppgave 6

(i) Polynomet $p(x)$ har grad 2 og ingen røtter i $\mathbb{Z}_3$. Dermed er $p(x)$ irredusibelt over $\mathbb{Z}_3$, så $\langle p(x) \rangle$ er et maksimalt ideal i ringen $\mathbb{Z}_3[x]$. Det betyr at faktorringen F er en kropp. F har dimensjon 2 som vektorrom over $\mathbb{Z}_3$, så antallet elementer i F er $|\mathbb{Z}_3|^2 = 9$.

(ii) Anta at $(ax+b)+\langle p(x) \rangle \in F$ er forskjellig fra null, i.e. at $a \neq 0$ eller at $b \neq 0$ i $\mathbb{Z}_3$. I ringen $\mathbb{Z}_3$ er $1^2 = 1 = 2^2$, så antagelsen gir at $a^2 + b^2 \neq 0$ i $\mathbb{Z}_3$. Siden $x^2 + \langle p(x) \rangle = -1 + \langle p(x) \rangle$, finner vi at

$$((ax + b) + \langle p(x) \rangle)^{-1} = \left(\frac{1}{a^2 + b^2}(-ax + b)\right) + \langle p(x) \rangle.$$

(iii) Vi har $|F^*| = 8$. La $\alpha = x + \langle p(x) \rangle \in F^*$. Da er

$$\begin{aligned}
\alpha^2 &= x^2 + \langle p(x) \rangle = 2 + \langle p(x) \rangle \neq 1 + \langle p(x) \rangle, \\
\alpha^3 &= 2x + \langle p(x) \rangle, \\
\alpha^4 &= 2x^2 + \langle p(x) \rangle = 1 + \langle p(x) \rangle,
\end{aligned}$$

i.e. α har orden 4 og er ikke en generator.

Oppgave 7

a) Ethvert ikke-null element i $\mathbb{Z}_5 \times \mathbb{Z}_5$ kan brukes som første radvektor i en matrise i G. Det finnes 5^2-1 slike vektorer. For hvert valg av første radvektor u, får vi en matrise i G hvis og bare hvis vi velger et element i $\mathbb{Z}_5 \times \mathbb{Z}_5$ som er lineært uavhengig av u, som andre radvektor. I.e. for hver u kan andre radvektor velges fritt blant elementene i $\mathbb{Z}_5 \times \mathbb{Z}_5$ som ikke er et multiplum av u. Det finnes $5^2 - 5$ slike vektorer. Det betyr at $|G| = (5^2 - 1)(5^2 - 5) = 24 \cdot 20 = 480$.

b) Vi har $g = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in G$.

(i) Siden $|G| = 480 = 2^5 \cdot 3 \cdot 5$, vil Sylow 5-undergruppene av G være undergruppene av orden 5. Siden $g^i = \left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right)$ vil g generere undergruppen

$$\langle g \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \right\},$$

i.e. en Sylow 5-undergruppe av G.

(ii) Dette følger fra ligningen

$$\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}^{-1}.$$

c) La $h \in G$ ha orden 5. Da er $h \in P$ for en Sylow 5-undergruppe P av G. Ved 'Sylow II' er P konjugert med Sylow 5-undergruppen $\langle g \rangle$, som spesielt betyr at $h = x\left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right)x^{-1}$ for en $x \in G$ og $i \in \{1, 2, 3, 4\}$. Dermed vet vi at h er konjugert med g, siden vi vet fra oppgave **b)** at $\left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right)$ er konjugert med g.

Til slutt skal vi finne antallet elementer i G av orden 5. Det er nå klart at antallet elementer i G av orden 5 er det samme som antallet elementer i banen til elementet g under konjugasjon. For å finne dette antallet, regner vi ut isotropiundergruppen G_g til g under konjugasjon. Observér at

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 - \frac{ac}{ad-bc} & \frac{a^2}{ad-bc} \\ \frac{-c^2}{ad-bc} & 1 + \frac{ac}{ad-bc} \end{pmatrix},$$

og at denne matrisen er lik g hvis og bare hvis $c = 0$ og $a = d \neq 0$. Med andre ord,

$$G_g = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \{1, 2, 3, 4\}, b \in \{0, 1, 2, 3, 4\} \right\},$$

så $|G_g| = 4 \cdot 5 = 20$. Dermed finner vi at antallet elementer i G av orden 5 er

$$|Gg| = (G : G_g) = \frac{|G|}{|G_g|} = \frac{480}{20} = 24.$$