NTNU

Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i **TMA4150 Algebra**

Faglig kontakt under eksamen: Torkil Utvik Stai

Tlf: 47638459

Eksamensdato: 29. mai 2018

Eksamenstid (fra–til): 15:00–19:00

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

Målform/språk: bokmål

Antall sider: 5

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

Merk! Studenter finner sensur i Studentweb. Har du spørsmål om din sensur må du kontakte instituttet ditt. Eksamenskontoret vil ikke kunne svare på slike spørsmål.

Oppgave 1 $24 = 2^3 \cdot 3$, så det finnes tre abelske grupper av orden 24 opp til isomorfi, nemlig

$$\begin{aligned}&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3;\\&\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3;\\&\mathbb{Z}_8 \times \mathbb{Z}_3.\end{aligned}$$

Skriv $G = \mathbb{Z}_{12} \times \mathbb{Z}_8 / \langle(3,4)\rangle$, og observér at $\langle(3,4)\rangle = \{(0,0),(3,4),(6,0),(9,4)\}$. Det er klart at elementet $(0,1) + \langle(3,4)\rangle \in G$ har orden 8. Siden $\mathbb{Z}_8 \times \mathbb{Z}_3$ er den eneste abelske gruppen av orden 24 som inneholder et element av orden 8, konkluderer vi med at $G \cong \mathbb{Z}_8 \times \mathbb{Z}_3$.

Oppgave 2

(i) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 8 & 6 & 3 & 1 & 5 & 7 \end{pmatrix} = (1,4,6)(3,8,7,5)$.

(ii) Ordenen til σ er lik minste felles multiplum av ordenen til $(1,4,6)$ og ordenen til $(3,8,7,5)$, altså $|\langle\sigma\rangle| = 3 \cdot 4 = 12$.

(iii) Vi kan skrive σ som et produkt av et odde antall transposisjoner, for eksempel

$$\sigma = (1,4,6)(3,8,7,5) = (1,6)(1,4)(3,5)(3,7)(3,8).$$

Dermed er σ en odde permutasjon, så σ tilhører ikke A_8.

Oppgave 3

a) D_5 består av de følgende permutasjonene.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \qquad \rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$
$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \qquad \rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$$
$$\rho_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$
$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$
$$\mu_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} \qquad \mu_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$$

D_5 er ikke normal i S_5: D_5 inneholder sykelen $(1,2,3,4,5)$, men ikke dens konjugerte $(1,2)(1,2,3,4,5)(1,2)^{-1} = (1,2)(1,2,3,4,5)(1,2) = (2,1,3,4,5)$.

b) D_5 virker på mengden X av alle fargelegginger av hjørnene til en regulær femkant med fire farger tilgjengelig, det vil si $|X| = 4^5$. Antallet distinkte femkanter er det samme som antallet baner r i X, som ved Burnsides formel er

$$\begin{aligned} r &= \frac{1}{|D_5|} \sum_{g \in D_5} |X_g| \\ &= \frac{1}{10} \left(|X_{\rho_0}| + 4 \cdot |X_{\rho_1}| + 5 \cdot |X_{\mu_1}|\right) \\ &= \frac{1}{10} \left(4^5 + 4 \cdot 4 + 5 \cdot 4^3\right) \\ &= 136. \end{aligned}$$

Oppgave 4

a) En gruppe G er simpel dersom den er ikke-triviell og undergruppene $\{e\}$ og G er de eneste normale undergruppene av G.

(i) La G være en gruppe av orden $28 = 2^2 \cdot 7$. La n være antallet Sylow 7-undergrupper av G. Da må $n \mid 28$ og $n \equiv 1 (\mathsf{mod}\ 7)$ ved 'Sylow III'. $n = 1$ er den eneste løsningen, så G har nøyaktig én Sylow 7-undergruppe P. For hver $g \in G$ er $|gPg^{-1}| = 7$, i.e. gPg^{-1} er en Sylow 7-undergruppe. Dette impliserer $gPg^{-1} = P$ for hver $g \in G$, som betyr at P er normal i G. Dermed er G ikke simpel.

(ii) La G være en gruppe av orden $2^{p-1}(2^p - 1)$ hvor p og $2^p - 1$ er primtall. La n være antallet Sylow $(2^p - 1)$-undergrupper av G. Ved 'Sylow III' må $n \mid 2^{p-1}(2^p - 1)$ og $n \equiv 1 (\mathsf{mod}\ 2^p - 1)$. Den eneste løsningen er $n = 1$, så vi kan konkludere med at G ikke er simpel ved å argumentere som i oppgave (i).

b) En komposisjonsrekke for en gruppe G er en kjede

$$\{e\} = N_0 < N_1 < N_2 < \cdots < N_{t-1} < N_t = G$$

av undergrupper av G slik at hver N_i er normal i N_{i+1}, og hver faktorgruppe N_{i+1}/N_i er simpel.

$\mathbb{Z}_7 \times \mathbb{Z}_7$ er ikke syklisk, og $|\mathbb{Z}_7 \times \mathbb{Z}_7| = 7 \cdot 7$. Dermed vil ethvert ikke-null element i $\mathbb{Z}_7 \times \mathbb{Z}_7$ generere en undergruppe av orden 7. Vi vet også at i en gruppe av orden 7 vil ethvert ikke-null element være en generator, siden 7 er et primtall. Det betyr at det finnes $\frac{|\mathbb{Z}_7 \times \mathbb{Z}_7| - 1}{7-1} = \frac{48}{6} = 8$ undergrupper av $\mathbb{Z}_7 \times \mathbb{Z}_7$ som har orden 7. En fullstendig liste av komposisjonsrekker for gruppen $\mathbb{Z}_7 \times \mathbb{Z}_7$ er dermed som følger.

$$\{(0,0)\} < \langle (0,1) \rangle < \mathbb{Z}_7 \times \mathbb{Z}_7$$
$$\{(0,0)\} < \langle (1,0) \rangle < \mathbb{Z}_7 \times \mathbb{Z}_7$$
$$\{(0,0)\} < \langle (1,1) \rangle < \mathbb{Z}_7 \times \mathbb{Z}_7$$
$$\{(0,0)\} < \langle (1,2) \rangle < \mathbb{Z}_7 \times \mathbb{Z}_7$$
$$\{(0,0)\} < \langle (1,3) \rangle < \mathbb{Z}_7 \times \mathbb{Z}_7$$
$$\{(0,0)\} < \langle (1,4) \rangle < \mathbb{Z}_7 \times \mathbb{Z}_7$$
$$\{(0,0)\} < \langle (1,5) \rangle < \mathbb{Z}_7 \times \mathbb{Z}_7$$
$$\{(0,0)\} < \langle (1,6) \rangle < \mathbb{Z}_7 \times \mathbb{Z}_7$$

Oppgave 5 Siden H er normal i G, blir H automatisk normal i K. Dermed kan vi se på faktorgruppa K/H, og tredje isomorfisetning gir

$$G/K \cong (G/H)\Big/(K/H).$$

Det er klart at enhver faktorgruppe av en abelsk gruppe er abelsk. Dermed må G/K være abelsk, siden G/H er antatt å være abelsk.

Oppgave 6

(i) Polynomet $p(x)$ har grad 3 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 3 som vektorrom over $\mathbb{Z}_3$, så antallet elementer i F er $|\mathbb{Z}_3|^3 = 27$.

(ii) Hvis I er et ideal i en kommutativ ring R med $1_R \neq 0$, så har vi det følgende.

- I er et primideal $\iff$ faktorringen R/I er et integritetsområde.
- I er et maksimalt ideal $\iff$ faktorringen R/I er en kropp.

Siden enhver kropp er et integritetsområde, følger det at ethvert maksimalt ideal i R er et primideal. Spesielt følger det at det maksimale idealet $\langle p(x) \rangle$ i ringen $\mathbb{Z}_3[x]$ er et primideal.

Siden ringen $\mathbb{Z}_3[x]/\{0\} \cong \mathbb{Z}_3[x]$ er et integritetsområde, er idealet $\{0\}$ et primideal. Men $\mathbb{Z}_3[x]$ er ikke en kropp, så idealet $\{0\}$ er ikke et maksimalt ideal.

Oppgave 7

a) Ethvert element i S_n kan skrives som et produkt av (disjunkte) sykler, og enhver sykel kan skrives som et produkt av transposisjoner. Det betyr at transposisjonene genererer hele S_n.

(i) Oppgaven spør om S_6, men la oss vise at S_n alltid er generert av de $n-1$ transposisjonene

$$(1,2),(2,3),\ldots,(n-1,n).$$

Siden mengden av alle transposisjoner genererer S_n, er det tilstrekkelig å vise at enhver transposisjon i S_n ligger i undergruppen $L < S_n$ generert av mengden $\{(1,2),(2,3),\ldots,(n-1,n)\}$.
Velg en vilkårlig $(i,j) \in S_n$. Siden $(i,j) = (j,i)$ kan vi uten tap av generalitet anta at $i < j$. Hvis $j - i = 1$, så har vi $(i,j) = (i,i+1) \in L$. Anta nå at $j - i = k > 1$ og at $(i',j') \in L$ hver gang $j' - i' < k$. Da følger det at $(i,j) \in L$, siden

$$(i,j) = (i,i+1)(i+1,j)(i,i+1).$$

(ii) Igjen spør oppgaven om S_6, men vi viser at S_n alltid er generert av $(1,2)$ og $\rho = (1,2,\ldots,n)$. Ved punkt (i) er det tilstrekkelig å vise at enhver transposisjon på formen $(i,i+1)$ ligger i undergruppa generert av $(1,2)$ og ρ. Dette følger fra observasjonen

$$\rho^i(1,2)\rho^{-i} = (i+1,i+2).$$

b) Vi kan uten tap av generalitet anta at $(1,2) \in H$. I oppgaveteksten får vi vite at det er tilstrekkelig å vise at H inneholder en sykel på formen $(1,2,i_3,\ldots,i_p)$.

Siden p er en divisor i ordenen til H, gir Cauchys teorem at H inneholder et element γ av orden p. En slik γ må være en sykel av lengde p, siden p er et primtall. At p er et primtall betyr også at for hver $1 \leq i \leq p-1$ har γ^i orden lik p, i.e. γ^i er en sykel av lengde p. Siden $\gamma^i \in H$ for hver i, er det tilstrekkelig å vise at det eksisterer en i som er slik at $\gamma^i(1) = 2$. For å vise dette, se på mengden

$$K = \{\gamma(1), \gamma^2(1), \ldots, \gamma^{p-1}(1)\}.$$

Det er klart at $1 \notin K$. Hvis $\gamma^a(1) = \gamma^b(1)$ med $a < b$, så vil $\gamma^{b-a}(1) = 1 \in K$, som er en selvmotsigelse. Dermed må antallet elementer i K være $p-1$, som betyr at $2 \in K$, i.e. det finnes en i som er slik at $\gamma^i(1) = 2$.