NTNU

Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i **TMA4150 Algebra**

Faglig kontakt under eksamen: Johanne Haugland

Tlf: 95757487

Eksamensdato: 27. mai 2019

Eksamenstid (fra–til): 09:00-13:00

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

Annen informasjon:
Eksamenssettet består av de ti oppgavene 1a, 1b, 2a, 2b, 3, 4, 5a, 5b, 6 og 7. Hver av disse teller like mye i vurderingen. Alle svar skal begrunnes.

Målform/språk: bokmål

Antall sider: 6

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

a) Vi har primtallsfaktoriseringen $20 = 2^2 \cdot 5$. Ved fundamentalteoremet for endeliggenererte abelske grupper vet vi dermed at det finnes nøyaktig to abelske grupper av orden 20 opp til isomorfi, nemlig $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$ og $\mathbb{Z}_4 \times \mathbb{Z}_5$.

b) Først skriver vi σ som et produkt av disjunkte sykler:

$$\sigma = (1,4,8,7)(2,9,3,5,6).$$

Når en permutasjon er skrevet som et produkt av disjunkte sykler, vet vi at ordenen til permutasjonen er lik minste felles multiplum av syklenes lengder. Dermed er $\mathrm{ord}(\sigma) = \mathrm{lcm}(4,5) = 20$, så H har orden 20. Siden gruppen H er syklisk, er den nødvendigvis også abelsk. Av de to gruppene fra oppgave **a)** er det kun $\mathbb{Z}_4 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{20}$ som er syklisk, så H må være isomorf med denne.

Oppgave 2

a) Et generelt femtegradspolynom i $\mathbb{Z}_2[x]$ er på formen

$$p(x) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

der $a_i \in \mathbb{Z}_2$. Dersom polynomet $p(x)$ skal være irredusibelt, må vi ha at $p(\alpha) \neq 0$ for alle $\alpha \in \mathbb{Z}_2$, for ellers er $(x-\alpha)$ en faktor. Dermed må

$$p(0) = a_0 \neq 0,$$

i.e. vi har $a_0 = 1$. Videre må

$$p(1) = 1 + a_4 + a_3 + a_2 + a_1 + 1 \neq 0.$$

Siden vi jobber modulo 2, betyr dette at vi må ha et *odde* antall av koeffisientene a_1, a_2, a_3 og a_4 lik 1. Dette argumentet viser at følgende femtegradspolynomer i $\mathbb{Z}_2[x]$ ikke har røtter:

$$\begin{aligned}
p_1(x) &= x^5 + x^4 + 1\\
p_2(x) &= x^5 + x^3 + 1\\
p_3(x) &= x^5 + x^2 + 1\\
p_4(x) &= x^5 + x + 1\\
p_5(x) &= x^5 + x^4 + x^3 + x^2 + 1\\
p_6(x) &= x^5 + x^4 + x^3 + x + 1\\
p_7(x) &= x^5 + x^4 + x^2 + x + 1\\
p_8(x) &= x^5 + x^3 + x^2 + x + 1
\end{aligned}$$

Men er alle disse polynomene irredusible? Nei!

Hvis polynomet $p(x)$ *ikke* er irredusibelt og *ikke* har noen rot, må det være på formen

$$p(x) = f(x)g(x),$$

der $\deg(f(x)) = 2$, $\deg(g(x)) = 3$ og verken $f(x)$ eller $g(x)$ har røtter. Ved tilsvarende argumentasjon som ovenfor ser vi at $f(x) = x^2+x+1$ er det eneste andregradspolynomet i $\mathbb{Z}_2[x]$ som ikke har røtter, mens $g_1(x) = x^3+x^2+1$ og $g_2(x) = x^3+x+1$ er de eneste tredjegradspolynomene uten røtter. Utregning viser at

$$\begin{aligned} f(x)g_1(x) &= p_4(x) \\ f(x)g_2(x) &= p_1(x). \end{aligned}$$

Polynomene $p_1(x)$ og $p_4(x)$ er dermed ikke irredusible.

Konklusjon: De irredusible femtegradspolynomene i $\mathbb{Z}_2[x]$ er $p_2(x), p_3(x), p_5(x), p_6(x), p_7(x)$ og $p_8(x)$ fra listen ovenfor.

b) La $f(x)$ være et av de irredusible femtegradspolynomene i som vi fant i oppgave **a)**. La $(f(x))$ være idealet generert av $f(x)$ i $\mathbb{Z}_2[x]$. Fra teorien som er gjennomgått i kurset, vet vi at $(f(x))$ er et maksimalt ideal og at faktorringen

$$\mathbb{Z}_2[x]/(f(x))$$

er en kropp med

$$2^{\deg(f(x))} = 2^5 = 32$$

elementer.

Oppgave 3

(i) Vi viser de fire punktene nedenfor. Samlet beviser dette at $(G, *)$ er en gruppe.

(0) **Binæroperasjon**: Vi må vise at for $a, b \in G$, så vil også $a * b \in G$. Anta

$$a * b = a + b + ab = -1.$$

Siden

$$a + b + ab + 1 = (a+1)(b+1),$$

innebærer antakelsen at enten a eller b er lik -1. Dermed er operasjonen $*$ en binæroperasjon på mengden G.

(1) **Assosiativitet**: La $a, b, c \in G$. Vi har

$$\begin{aligned}(a * b) * c &= (a + b + ab) * c \\ &= a + b + ab + c + (a + b + ab)c \\ &= a + b + c + bc + a(b + c + bc) \\ &= a * (b + c + bc) = a * (b * c),\end{aligned}$$

så binæroperasjonen er assosiativ.

(2) **Identitetselement**: 0 er identitetselement, siden

$$a * 0 = a + 0 + a \cdot 0 = a = 0 + a + 0 \cdot a = 0 * a$$

for alle $a \in G$.

(3) **Inverser**: La $a \in G$. Vi har

$$a * \frac{-a}{a+1} = a - \frac{a}{a+1} - \frac{a^2}{a+1} = \frac{a(a+1) - a - a^2}{a+1} = 0,$$

og tilsvarende motsatt vei. Observer at nevneren ikke er 0, siden $a \in G$. Det gjenstår å vise at

$$\frac{-a}{a+1} \in G.$$

Anta det motsatte, altså at

$$\frac{-a}{a+1} = -1.$$

Dette impliserer at $1 = 0$, som er en motsigelse. Vi kan dermed konkludere at ethvert element $a \in G$ har en invers $a^{-1} = \frac{-a}{a+1}$ som ligger i G.

(ii) For enhver $x \in \mathbb{R}$ har vi

$$-1 * x = -1 + x - x = -1.$$

Siden $1 \neq 0$, betyr dette at elementet -1 ikke har noen invers, så $(\mathbb{R}, *)$ er ikke en gruppe.

Oppgave 4

Se på avbildningen

$$\phi\colon G \times G \longrightarrow G$$

definert ved $\phi((g,h)) = gh^{-1}$. Vi ser at

$$\phi((g_1,h_1)(g_2,h_2)) = \phi((g_1g_2, h_1h_2)) = g_1g_2(h_1h_2)^{-1} = g_1g_2h_2^{-1}h_1^{-1}.$$

På den annen side har vi

$$\phi((g_1,h_1))\phi((g_2,h_2)) = g_1h_1^{-1}g_2h_2^{-1}.$$

Ettersom G er abelsk, er disse like, så ϕ er en gruppehomomorfi.

La e være identitetselementet i G. Kjernen til ϕ er

$$\begin{aligned}\operatorname{Ker}(\phi) &= \{(g,h) \in G \times G \mid \phi((g,h)) = e\}\\ &= \{(g,h) \in G \times G \mid gh^{-1} = e\}\\ &= \{(g,h) \in G \times G \mid g = h\} = \Delta G.\end{aligned}$$

Vi vet fra resultater gjennomgått i kurset at kjernen til en gruppehomomorfi er en normal undergruppe, og kan dermed konkludere at ΔG er en normal undergruppe av $G \times G$. Siden $\phi((g,e)) = g$, er ϕ surjektiv. Ved fundamentalteoremet for gruppehomomorfier får vi at faktorgruppen $(G \times G)/\Delta G$ er isomorf med G.

Oppgave 5

a) Anta at først at $|G|$ er en potens av p. La $g \in G$. Fra Lagranges teorem vet vi at $\operatorname{ord}(g)$ deler $|G|$. Dermed må også $\operatorname{ord}(g)$ være en potens av p, hvilket betyr at G en p-gruppe.

Den andre retningen viser vi kontrapositivt: Anta at $|G|$ *ikke* er en potens av p. Da finnes et primtall $q \neq p$ slik at q deler $|G|$. Ved Cauchys teorem inneholder G dermed et element av orden q. Siden dette elementet umulig kan ha en orden som er en potens av p, er G ikke en p-gruppe.

Alternativ: Om ønskelig kan man bruke første sylowteorem i stedet for Cauchys teorem. Siden q deler $|G|$, gir første sylowteorem at G har en undergruppe H av orden q. La $h \in H$ der h ikke er identitetselementet. Siden $\operatorname{ord}(h)$ må dele q (igjen ved Lagranges teorem), kan $\operatorname{ord}(h)$ umulig være en potens av p. Dermed er G ikke en p-gruppe.

b) (i) En undergruppe H av G er en sylow-p-undergruppe dersom H er en maksimal p-undergruppe av G.

(ii) La n_3 være antall sylow-3-undergrupper av en gruppe av orden 42. Ved tredje sylowteorem vet vi at

(a) n_3 deler 42;

(b) $n_3 \equiv 1 \pmod 3$.

Punkt (a) gir at $n_3 \in \{1, 2, 3, 6, 7, 14, 21, 42\}$. De eneste elementene i denne mengden som tilfredsstiller punkt (b) er 1 og 7. En gruppe av orden 42 kan altså ha enten 1 eller 7 sylow-3-undergrupper.

Oppgave 6 La X være mengden av alle mulige fargelegginger av en rose (her anses rotasjoner og speilinger som *ulike*). La G være gruppen bestående av alle symmetrier på en rose. Gruppen G virker naturlig på mengden X, og vi ønsker å finne antall baner under denne gruppevirkningen. Ved Burnsides formel vet vi at

$$\text{antall baner} = \frac{1}{|G|} \sum_{g \in G} |X_g|,$$

der $X_g = \{x \in X \mid gx = x\}$.

Gruppen G inneholder 5 rotasjoner, si $\rho_0, \rho_1, \rho_2, \rho_3$ og ρ_4, og 5 speilinger, si $\mu_1, \mu_2, \mu_3, \mu_4$ og μ_5. Dermed er $|G| = 10$.

Kombinatoriske beregninger gir at

- $|X_{\rho_0}| = |X| = 3^{10}$;
- $|X_{\rho_1}| = |X_{\rho_2}| = |X_{\rho_3}| = |X_{\rho_4}| = 3^2$;
- $|X_{\mu_i}| = 3^6$ for $i \in \{1, 2, 3, 4, 5\}$.

Ved å putte dette inn i formelen ovenfor, får vi

$$\text{antall baner} = \frac{1}{10}(3^{10} + 4 \cdot 3^2 + 5 \cdot 3^6) = 6273.$$

Konklusjon: Dersom hvert medlem skal få ei unik rose, kan lokalhistorielaget ha maksimalt 6273 medlemmer.

Oppgave 7 Siden $|G| \geq 2$, kan vi velge $g \in G$ slik at g ikke er identitetselementet e. Ettersom G er abelsk, vil enhver undergruppe av G være normal. Siden G er simpel, og dermed ikke har noen andre normale undergrupper enn $\{e\}$ og G, må undergruppen generert av g være lik G. Dette betyr at G er en syklisk gruppe.

Fra resultater gjennomgått i kurset vet vi at enhver syklisk gruppe er isomorf med enten $\mathbb{Z}$ eller $\mathbb{Z}_n$. Gruppen $\mathbb{Z}$ er ikke simpel, så vi må ha $G \simeq \mathbb{Z}_n$.

Dersom n ikke er et primtall, vil $\mathbb{Z}_n$ ha en ekte ikke-triviell undergruppe. Siden denne vil være normal, kan vi konkludere at n må være et primtall.