NTNU
Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i **MA3202 Galoisteori**

Faglig kontakt under eksamen: Christian Fredrik Skau

Tlf: 73 59 17 55

Eksamensdato: 6. juni 2019

Eksamenstid (fra–til): 09:00–13:00

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

Annen informasjon:
Alle deloppgaver teller likt.

Målform/språk: bokmål

Antall sider: 2

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

a) Det finnes 21 irredusible moniske polynomer av grad 2 over $\mathbb{F}_7 = \mathrm{GF}(7)$. Hvor mange irredusible moniske polynomer finnes det av grad 3 over $\mathbb{F}_7$?

b) La $\mathbb{E}$ være en endelig kropp, og la $\mathbb{F}$ og $\mathbb{K}$ være underkropper av $\mathbb{E}$ slik at $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}]$. Vis at $\mathbb{F} = \mathbb{K}$.

c) La $\mathbb{E}$ være en uendelig kropp (dvs. $|\mathbb{E}| = \infty$), og la $\mathbb{F}$ og $\mathbb{K}$ være underkropper slik at $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}] < \infty$. Er da alltid $\mathbb{F} = \mathbb{K}$? (Gi begrunnelse.)

Oppgave 2

a) La $\mathbb{F}$ og $\mathbb{K}$ være to kropper slik at $\mathbb{F} \subseteq \mathbb{K}$. Anta α er algebraisk over $\mathbb{F}$ og over $\mathbb{K}$. Vis at $[\mathbb{K}(\alpha) : \mathbb{K}] \leq [\mathbb{F}(\alpha) : \mathbb{F}]$. (Hint: Betrakt minimalpolynomet.)

b) La $\mathbb{E}$ være rotkroppen til polynomet $f(x) = x^{13} - 12 \in \mathbb{Q}[x]$. Finn ordenen til Galoisgruppen $G = G(\mathbb{E}|\mathbb{Q})$. (Gi begrunnelse.)

c) Vis at det finnes en mellomkropp $\mathbb{K}$, dvs. $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{E}$, slik at $[\mathbb{K} : \mathbb{Q}] = 39$. (Hint: Bruk Sylow-teori.)

d) Begrunn, ved å appellere til hovedsatsen i Galoisteori, at $G = G(\mathbb{E}|\mathbb{Q})$ i oppgave **b)** er en ikke-abelsk gruppe.

e) Røttene til $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ er $\alpha = \sqrt[3]{2} (\in \mathbb{R}), \omega\alpha, \omega^2\alpha$, der $\omega = e^{\frac{2\pi i}{3}}$. Vis at $\mathbb{Q}(\omega\alpha)$ ikke inneholder α.

Oppgave 3 Vis at 3 er et irredusibelt element i $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$, men at 3 ikke er et primsk element i $\mathbb{Z}[\sqrt{-5}]$.

Oppgave 4

a) La $(0 \neq) f_i(x) \in \mathbb{F}[x], i = 1, 2, ..., n, ...$ der $\mathbb{F}$ er en kropp. La $f_i(\alpha_i) = 0$, der $\alpha_i \in \overline{\mathbb{F}}$ for $i = 1, 2, ..., n, ...$ Vi at $[\mathbb{L} : \mathbb{F}] \leq \deg(f_1(x)) \cdot \deg(f_2(x)) \cdots \deg(f_n(x))$ for alle n, der $\mathbb{L} = \mathbb{F}(\alpha_1, \alpha_2, ..., \alpha_n)$. (Hint: Bruk induksjon.)

b) La karakteristikken til kroppen $\mathbb{K}$ være 0. La $\mathbb{L}$ være en algebraisk lukket kropp som inneholder $\mathbb{K}$, og anta at $1 < [\mathbb{L} : \mathbb{K}] < \infty$. Vis at $\mathbb{L}$ er en Galoisk utvidelse av $\mathbb{K}$.

Oppgave 5 Det syklotomiske polynomet $\Phi_8(x) \in \mathbb{Z}[x]$ er et irredusibelt polynom over $\mathbb{Q}$, der røttene til $\Phi_8(x)$ er de primitive enhetsrøttene av orden 8. (Dette skal du ikke bevise.) La $\mathbb{E}$ være rotkroppen til $\Phi_8(x)$ over $\mathbb{Q}$. Bestem Galoisgruppen $G = G(\mathbb{E}|\mathbb{Q})$.

1

MA 3202 : Galoisteori

Løsningsforslag for eksamen 6 juni 2019

Oppgave 1 a) Det er ialt $7^3 = \underline{343}$ moniske polynomer av grad 3 over $\mathbb{F}_7$.
(Observér at dersom et polynom av grad 3 har to røtter som ligger i $\mathbb{F}_7$, så vil også den tredje roten ligge i $\mathbb{F}_7$.)

Antall redusible moniske polynomer av grad 3 med tre distinkte røtter i $\mathbb{F}_7$ er $\binom{7}{3} = \underline{35}$.
Antall redusible moniske polynomer av grad 3 med nøyaktig to sammenfallende røtter i $\mathbb{F}_7$ er $7 \cdot 6 = \underline{42}$.
Antall redusible moniske polynomer av grad 3 med nøyaktig en rot i $\mathbb{F}_7$ er 7 ganger antall irredusible moniske polynomer av grad 2, altså $7 \cdot 21 = \underline{147}$. Antall redusible moniske polynomer av grad 3 med tre identiske røtter i $\mathbb{F}_7$ er $\underline{7}$.
Antall irredusible moniske polynomer av grad 3 over $\mathbb{F}_7$ er altså:

$$343 - (35 + 42 + 147 + 7) = \underline{\underline{112}}$$

b) La $E = GF(p^n)$. Da er $F = GF(p^m)$, $K = GF(p^k)$ der $m \mid n$ og $k \mid n$. Dessuten er $[E:F] = \frac{n}{m}$, $[E:K] = \frac{n}{k}$. Siden $[E:F] = [E:K]$, så må $m = k$, og altså er $F = K$.

c) La $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $F = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}(\sqrt{3})$. Da er $F \neq K$, men $[E:F] = [E:K] = 2$. Svaret på spørsmålet er altså nei.

Oppgave 2

a) La $p(x) \in F(x)$ $(\subseteq K[x])$ og $q(x) \in K[x]$ være minimalpolynomene til α over F og K, henholdsvis. Da vil $q(x) \mid p(x)$ i $K[x]$, og altså $\text{grad}(q(x)) \leq \text{grad}(p(x))$. Siden $[K(\alpha):K] = \text{grad}(q(x))$, $[F(\alpha):F] = \text{grad}(p(x))$, så vil $[K(\alpha):K] \leq [F(\alpha):F]$.

b) $f(x)$ er irredusibel over $\mathbb{Q}$ ifølge Eisenstein's kriterium (bruk primtallet $p = 3$). La $\alpha = \sqrt[13]{12} \in \mathbb{R}$ være den reelle roten til $f(x)$. Da er $[\mathbb{Q}(\alpha):\mathbb{Q}] = \text{grad}(f(x)) = 13$. Røttene til $f(x)$ er $\alpha, \omega\alpha, \omega^2\alpha, \cdots, \omega^{12}\alpha$, der ω er en primitiv 13'ende enhetsrot (for eksempel, $\omega = e^{2\pi i/13}$). Minimalpolynomet til ω over $\mathbb{Q}$ er

$$x^{12} + x^{11} + \cdots + x + 1 \quad \left(= \frac{x^{13}-1}{x-1}\right).$$

Da er $[\mathbb{Q}(\omega):\mathbb{Q}] = 12$. Siden

$$[E:\mathbb{Q}] = [\mathbb{Q}(\alpha)(\omega):\mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha):\mathbb{Q}]$$

$$= [\mathbb{Q}(\omega)(\alpha):\mathbb{Q}(\omega)] \cdot [\mathbb{Q}(\omega):\mathbb{Q}]$$

så må $13 \mid [E:\mathbb{Q}]$ og $12 \mid [E:\mathbb{Q}]$, og altså $12 \cdot 13 \mid [E:\mathbb{Q}]$. Ifølge a) så er

$$[\mathbb{Q}(\alpha)(\omega):\mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\omega):\mathbb{Q}] \; (= 12).$$

Altså er $[E:\mathbb{Q}] = 12 \cdot 13 = 156$. Ifølge hovedsatsen i Galoisteorien er $|G(E|\mathbb{Q})| = [E:\mathbb{Q}] = \underline{156}$

c) Siden $|G| = 156 = 2^2 \cdot 3 \cdot 13$ og altså $2^2 \mid |G|$, så følger det av Sylow-teori at G har en undergruppe H av orden $2^2 = 4$. Ifølge hovedsatsen i Galoisteorien så finnes det en mellomkropp K $(\mathbb{Q} \subseteq K \subseteq E)$ slik at $|G(E|K)| = |H| = 4$. Siden $|G(E|K)| = [E:K]$, $|G| = |G(E|\mathbb{Q})| = [E:\mathbb{Q}]$ og $[E:\mathbb{Q}] = [E:K]\cdot[K:\mathbb{Q}]$, så følger det at

$$[K:\mathbb{Q}] = \frac{|G|}{|H|} = \frac{156}{4} = \underline{39}$$

d) Dersom $G = G(E|\mathbb{Q})$ er abelsk, så vil enhver mellomkropp L $(\mathbb{Q} \subseteq L \subseteq E)$ være en Galoisk (og dermed normal) utvidelse av $\mathbb{Q}$, ifølge hovedsatsen i Galoisteorien. Men mellomkroppen $L = \mathbb{Q}(\sqrt[13]{12})$ er ikke noen normal utvidelse av $\mathbb{Q}$, siden ikke alle røttene til det irredusible polynomet $f(x) = x^{13} - 12 \in \mathbb{Q}[x]$ ligger i L. Altså er G en ikke-abelsk gruppe.

e) Rotkroppen L til $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ er $\mathbb{Q}(\alpha, \omega)$. Siden $f(x)$ er irredusibel (ifølge Eisenstein), og $\omega\alpha$ er en rot, så vil $[\mathbb{Q}(\omega\alpha) : \mathbb{Q}] = \text{grad}(f(x)) = 3$.

Dersom $\alpha \in \mathbb{Q}(\omega\alpha)$, så vil $\omega \in \mathbb{Q}(\omega\alpha)$, og altså $L = \mathbb{Q}(\omega\alpha)$.

Dette strider mot at $[L : \mathbb{Q}] = 2 \cdot 3 = 6$

Oppgave 3 Enhetene i $\mathbb{Z}[\sqrt{-5}]$ er ± 1. Anta $3 = \alpha\beta$, der $\alpha = a + b\sqrt{-5}$, $\beta = c + d\sqrt{-5}$; $a, b, c, d \in \mathbb{Z}$. Ved å ta normen N, får man:

$$N(3) = 3^2 = N(\alpha)N(\beta) = (a^2 + 5b^2)(c^2 + 5d^2).$$

Dette medfører at enten må $N(\alpha) = a^2 + 5b^2 = 3^2$ (og da må $N(\beta) = 1$), eller så må $N(\beta) = c^2 + 5b^2 = 3^2$ (og da må $N(\alpha) = 1$).

Altså er enten α en enhet, eller så er β en enhet. Følgelig er 3 irredusibel.

3 er en divisor i $9 = (2+\sqrt{-5})(2-\sqrt{-5})$, men 3 er ingen divisor i $2 \pm \sqrt{-5}$ siden det ikke finnes $\gamma = e + f\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ slik at $2 \pm \sqrt{-5} = 3\gamma$. Dette ser man ved å ta normen på begge sider:

$$N(2 \pm \sqrt{-5}) = 2^2 + 5 = 9 = N(3)N(\gamma) = 9 \cdot N(\gamma).$$

Da er $N(\gamma) = 1$, og altså $\gamma = \pm 1$.

Da må $\pm 3 = 2 \pm \sqrt{-5}$, hvilket er umulig. Altså er ikke 3 noe primisk element.

Oppgave 4 a) $[F(\alpha_1):F] = \text{grad}(p_1(x))$, der $p_1(x) \in F[x]$ er minimalpolynomet til α_1. Siden $p_1(x) \mid f_1(x)$, så er $\text{grad}(p_1(x)) \leq \text{grad}(f_1(x))$, og altså er påstanden riktig for $n = 1$.

Anta at påstanden er riktig for n, altså

$$[F(\alpha_1, \dots, \alpha_n):F] \leq \text{grad}(f_1(x)) \cdots \text{grad}(f_n(x)).$$

Vi har at $[F(\alpha_1,\dots,\alpha_n,\alpha_{n+1}):F(\alpha_1,\dots,\alpha_n)] = \text{grad}(p_{n+1}(x))$, der $p_{n+1}(x) \in F(\alpha_1,\dots,\alpha_n)[x]$ er minimalpolynomet til α_{n+1} over $F(\alpha_1,\dots,\alpha_n)$. Siden $f_{n+1}(\alpha_{n+1})=0$ og $f_{n+1}(x) \in F[x] \subseteq F(\alpha_1,\dots,\alpha_n)[x]$ så vil $p_{n+1}(x) \mid f_{n+1}(x)$ i $F(\alpha_1,\dots,\alpha_n)[x]$, og altså $\text{grad}(p_{n+1}(x)) \leq \text{grad}(f_{n+1}(x))$. Vi får:

$$[F(\alpha_1,\dots,\alpha_n,\alpha_{n+1}):F] = [F(\alpha_1,\dots,\alpha_n,\alpha_{n+1}):F(\alpha_1,\dots,\alpha_n)] \cdot [F(\alpha_1,\dots,\alpha_n):F] \leq \text{grad}(p_{n+1}(x)) \cdot \text{grad}(f_1(x)) \cdots \text{grad}(f_n(x))$$

$$\leq \text{grad}(f_1(x)) \cdots \text{grad}(f_n(x)) \cdot \text{grad}(f_{n+1}(x)).$$

Altså er påstanden sann for $n+1$, og dermed er påstanden sann for alle n ifølge induksjon.

b) L er en endelig og separabel utvidelse av K. (Separabilitet følger av at karakteristikken til K er 0.) Dessuten er L en normal utvidelse av K: Anta nemlig at $p(x) \in K[x]$ er irredusibel over K. Siden $p(x) \in L[x]$ så vil alle røttene til $p(x)$ ligge i L siden L er algebraisk lukket. Altså er L en Galoisk utvidelse av K.

Oppgave 5 De primitive enhetsrøttene av orden 8 er $\omega = \omega_1 = e^{2\pi i/8}$, $\omega_2 = \omega^3$, $\omega_3 = \omega^5$, $\omega_4 = \omega^7$.

Altså er $|G| = |G(E|\mathbb{Q})| = [E:\mathbb{Q}] = 4$.

En gruppe G av orden 4 er enten syklisk eller lik Klein's Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$. La $\sigma \in G$; σ er entydig bestemt av $\sigma(\omega)$. Vi får følgende muligheter:

i) $\sigma(\omega) = \omega$. Da er $\sigma = id$.

ii) $\sigma(\omega) = \omega^3$. Da er $\sigma^2(\omega) = \omega^9 = \omega$, og altså $\sigma^2 = id$.

iii) $\sigma(\omega) = \omega^5$. Da er $\sigma^2(\omega) = \omega^{25} = \omega$, og altså $\sigma^2 = id$.

iv) $\sigma(\omega) = \omega^7$. Da er $\sigma^2(\omega^7) = \omega^{49} = \omega$. Altså er $\sigma^2 = id$.

Konklusjon: G er Klein's Vierergruppe.