1 **a)** Definer en avbildning $\phi : \mathbf{Z} \to K$ ved $\phi(1) = 1$. Vi får en embedding $\mathbf{Z}/ker(\phi) \subseteq K$ av ringer. Da $\mathbf{Z}$ er et PID, følger det at $ker(\phi) = (m)$ der $m \in \mathbf{Z}$. Siden K er en kropp, følger det at $m = p$ der p er et primtall. Vi får $\mathbf{Z}/(p) = \mathbf{F}_p \subseteq K$ og påstanden er bevist.

b) Siden K er endelig følger det at $[K, \mathbf{F}_p] < \infty$. La $e_1, .., e_n$ være en basis for K over $\mathbf{F}_p$. Hvert element x i K kan skrives som en lineær kombinasjon $x = a_1e_1 + ... + a_ne_n$ der $a_i \in \mathbf{F}_p$ er vilkårlig. Det følger derfor at antall elementer i K er p^n.

2 **a)** Anta $\sqrt{p} \in \mathbf{Q}$. Det følger da at $\sqrt{q} = a/b$ der $a, b \in \mathbf{Z}$ og a, b ikke har noen felles faktor. Vi får at $q = a^2/b^2$ og videre $b^2q = a^2$. Det følger at $p|a^2$ og siden p er prim følger det at $p|a$, i.e $a = pA$, der $A \in \mathbf{Z}$. Dette gir videre at $pb^2 = p^2A^2$. Vi får at $b^2 = pA^2$ som gir at $p|b^2$. Da p er et primtall følger det at $p|b$ og vi får at $b = pB$ som gir en motsigelse. Anta $\sqrt{q} \in \mathbf{Q}(\sqrt{p})$. Vi får en likning

$$\sqrt{q} = u + v\sqrt{p}$$

der $u, v \in \mathbf{Q}$. Vi kvadrerer og får

$$q = u^2 + 2uv\sqrt{p} + pv^2$$

som gir likningen

$$2uv\sqrt{p} = q - u^2 - pv^2.$$

Om $uv \neq 0$ får vi $\sqrt{p} = (q - u^2 - pv^2)/2uv \in \mathbf{Q}$ som er en motsigelse. Anta derfor at $uv = 0$. Om $u = 0$ får vi likningen $q = pv^2$ som impliserer at $p|q$ - motsigelse. Om $v = 0$ får vi likningen $q = u^2$ som er en motsigelse da q er prim. Følgelig må $\sqrt{q} \notin \mathbf{Q}(\sqrt{p})$.

b) Fra resultatet over følger det at polynomet $P(x) = T^2 - p \in \mathbf{Q}[x]$ er irredusibelt da $\pm\sqrt{p} \notin \mathbf{Q}$. Følgelig er $[\mathbf{Q}(\sqrt{p}) : \mathbf{Q}] = deg(P(x)) = 2$. La $\alpha = \sqrt{p} + \sqrt{q}$ og $\beta = \sqrt{p} - \sqrt{q}$. Det følger at polynomet

$$Q(x) = (x - \alpha)(x - \beta) = x^2 + 2\sqrt{p}x + p - q \in \mathbf{Q}(\sqrt{p})$$

er irredusibelt, da $\alpha, \beta \notin \mathbf{Q}(\sqrt{p})$. Vi får en inklusjon av kropper

$$\mathbf{Q}(\sqrt{p} \subseteq \mathbf{Q}(\sqrt{p}, \alpha) = \mathbf{Q}(\sqrt{p}, \sqrt{q})$$

og derfor er $[\mathbf{Q}(\sqrt{p}, \sqrt{q}) : \mathbf{Q}(\sqrt{p})] = deg(Q(x)) = 2$. Dette gir

$$[\mathbf{Q}(\sqrt{p}, \sqrt{q}) : \mathbf{Q}] = deg(Q(x))deg(P(x)) = 4.$$

3 **a)** La $f(x) = x^3 + x^2 + x + 1$. Vi får $g(x) = x^4 - 1 = (x-1)f(x)$. En rot for $f(x)$ i $K = \mathbf{F}_7$ er en rot for $g(x)$ forskjellig fra 1. Vi får $g(6) = 6^4 - 1 = 1295 = 7 \times 185 = 0$ i K. Det følger derfor at $x - 6$ deler $f(x)$ i $K[x]$. Vi bruker polynomdivisjon og får $f(x) = (x-6)(x^2+1) = (x+1)(x^2+1)$. Polynomet $p(x) = x^2 + 1$ er irredusibelt i $K[x]$ og faktoriseringen $f(x) = (x+1)p(x)$ er derfor en faktorisering i irredusible polynomer.

b) La $\alpha \in \overline{K}$ være en rot for $p(x)$. Det følger da at $K(\alpha)$ er rotkroppen for $f(x)$ og $[K(\alpha) : K] = deg(p(x)) = 2$. En basis for $K(\alpha)$ over K er $B = \{1, \alpha\}$. Det følger videre at antall elementer i $K(\alpha)$ er lik $7^2 = 49$.

c) Vi må beregne $a, b \in K$ slik at $(1+\alpha)(a+b\alpha) = 1$. Merk: siden $\alpha^2 + 1 = 0$ følger det at $\alpha^2 = -1 = 7 - 1 = 6$ i K: Vi multipliserer ut og får likningssystemet

$$a + b\alpha + a\alpha + b\alpha^2 = a + 6b + (a+b)\alpha = 1$$

Da $1, \alpha$ er en basis, får vi likningene $I : a + 6b = 1$ og $II : a + b = 0$ i K. Vi får fra $I : b = -a$. Innsatt i II gir dette $a - 6a = -5a = 2a = 1$ og $a = 1/2 = 4$ i K. (Merk: $2 \times 4 = 8 = 7 + 1 = 1$ i K, så $1/2 = 4$.) Vi får $b = -a = -4 = 7 - 4 = 3$ og derfor er $1/(1+\alpha) = 4 + 3\alpha$.

4 **a)** La $p(x) = x^3 - 3$ og $q(x) = x^2 + x + 1$. La α være en rot for $p(x)$ og ω en rot for $q(x)$. Det følger at $\omega^2 = -\omega - 1$ og $\omega^3 = \omega(-\omega - 1) = -\omega^2 - \omega = 1$. Følgelig er $\omega^3 = 1$ og $\omega \neq 1$. Videre er $(\omega^2)^3 = (\omega^3)^2 = 1^2 = 1$. Videre er $\omega \neq \omega^2$: Anta at $\omega = \omega^2$. Det følger da at $\omega(\omega - 1) = 0$, men siden $\omega \neq 0$ følger det at $\omega = 1$ - motsigelse. Derfor må $\omega \neq \omega^2$. Vi får: $(\omega\alpha)^3 = \omega^3\alpha^3 = \alpha^3 = 3$. Vi får også at $(\omega^2\alpha)^3 = (\omega^2)^3\alpha^3 = \alpha^3 = 3$, så $\alpha, \omega\alpha, \omega^2\alpha$ er tre distinkte røtter for likningen $x^3 - 3 = 0$. En eksplisitt beregning viser at $\omega = 1/2(-1 + i\sqrt{3})$ og $\omega^2 = 1/2(-1 - i\sqrt{3})$. Videre er $\alpha \in \mathbf{R}$ en reell kubikk rot av 3. La $E = \mathbf{Q}(\alpha, \omega)$ være rotkroppen til $p(x)$. Det følger at $[E : \mathbf{Q}] = 6$, og siden $\mathbf{Q} \subseteq E$ er Galois (den er normal og separabel) har vi fra Galois teoriens hovedsats at $|G(E/\mathbf{Q})| = 6 = [E : \mathbf{Q}]$. La $\sigma \in G = G(E/\mathbf{Q})$. En basis for E over $\mathbf{Q}$ er gitt av elementene

$$1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2.$$

Videre er $p(\alpha) = 0$ og siden $p(x) \in \mathbf{Q}[x]$ følger det at $\sigma(\alpha)$ også er en rot for $p(x)$. Videre er $q(\omega) = 0$ og $q(x) \in \mathbf{Q}[x]$. Følgelig er $\sigma(\omega)$ igjen en rot for $q(x)$. Det følger at $\sigma(\alpha)$ må være et av elementene $\alpha, \omega\alpha, \omega\alpha^2$ og $\sigma(\omega)$ må være et av elementene ω, ω^2. Vi får da at σ er entydig bestemt av virkningen på α og ω. Gruppen G består derfor av følgende seks elementer: $\sigma_1 = e$ - identiteten, samt følgende seks automorfier (som alle fikserer $\mathbf{Q}$):

$$\sigma_2(\alpha) = \omega\alpha \quad (1)$$
$$\sigma_2(\omega) = \omega \quad (2)$$

$$\sigma_3(\alpha) = \omega^2\alpha \quad (3)$$
$$\sigma_3(\omega) = \omega \quad (4)$$

$$\sigma_4(\alpha) = \alpha \quad (5)$$
$$\sigma_4(\omega) = \omega^2 \quad (6)$$

$$\sigma_5(\alpha) = \omega\alpha \tag{7}$$
$$\sigma_5(\omega) = \omega^2 \tag{8}$$

$$\sigma_6(\alpha) = \omega^2\alpha \tag{9}$$
$$\sigma_6(\omega) = \omega^2 \tag{10}$$

Om vi legger tallene $\alpha, \omega\alpha, \omega^2\alpha$ inn i det komplekse tallplanet $\mathbf{C}$ og lar γ være operasjonen som roterer 120 grader moturs samt τ er operasjonen som reflekterer om x-aksen, så får vi at gruppen av symmetrier av triangelet T definert av tallene $\alpha, \omega\alpha, \omega^2\alpha$ er generert av elementene $e, \gamma, \gamma^2, \tau, \tau\gamma, \tau\gamma^2$. Videre sjekker vi at følgende holder: $\sigma_1 = e, \sigma_2 = \gamma, \sigma_3 = \gamma^2, \sigma_4 = \tau, \sigma_5 = \tau\gamma^2$ samt $\sigma_6 = \tau\gamma$. Følgelig er $G(E/\mathbf{Q})$ lik gruppen av symmetrier av et likesidet triangel.

b) La β være en reell rot av $p(x)$. Da er $\beta = \alpha$ i notasjonen over, og vi ser at de eneste automorfiene i $G(E/\mathbf{Q})$ som fikserer β er $\sigma_1 = e$ og $\sigma_4 = \tau$. Da $\tau^2 = e$ følger det at $H_L = \{e, \tau\}$ er isomorf med $\mathbf{Z}/2\mathbf{Z}$. Siden utvidelsen $\mathbf{Q} \subseteq \mathbf{Q}(\beta)$ ikke er normal, følger det fra Galois teoriens hovedsats at gruppen H_L ikke er normal i $G(E/\mathbf{Q})$.

5 **a)** La $\alpha \in \overline{K}$ være en rot for polynomet $q(T) = T^p - x$. Vi har da at $\alpha^p = x$. Det følger at

$$(T - \alpha)^p = T^p + (-1)^p\alpha^p = T^p - \alpha^p = T^p - x = q(T)$$

i ringen $K(\alpha)[x]$. Derfor er $d = p$.

b) Siden $q(T)$ har en unik rot α med multiplisitet p følger det at $K(\alpha)$ er rotkroppen til $q(T)$.