Eksamen 2016

Galois-teori

2016)

Oppg 1. $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

a) E - rotkroppen ? røtter $\sqrt[4]{2}$, $\sqrt[4]{2}\, i$, $-\sqrt[4]{2}$, $-\sqrt[4]{2}\, i$

$$\left(w^4 = 1 \quad w = e^{\frac{2\pi i}{4}} = i \right)$$

$E = \mathbb{Q}(2^{1/4}, i)$. i rot i x^2+1 irredusibel i $\mathbb{Q}$.

x^4-2 er min. polynom til $2^{1/4}$.

$$\mathbb{Q} \subseteq \mathbb{Q}(2^{1/4}) \subseteq \mathbb{Q}(2^{1/4}, i) \qquad [\mathbb{Q}(2^{1/4}) : \mathbb{Q}] = 2.$$

x^2+1 irred. over $\mathbb{Q}(2^{1/4})$, siden $i \notin \mathbb{Q}(2^{1/4})$

$$\Rightarrow [\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}(2^{1/4})] = 2$$

$$\Rightarrow [E : \mathbb{Q}] = 2 \cdot 4$$

b) Hvis $G(E/\mathbb{Q})$ - abelsk, så er alle undergrupper normale

$\Rightarrow$ alle kropper K s.a. $\mathbb{Q} \subseteq K \subseteq E$ er normale (ved FTGT).

Men $\mathbb{Q}(2^{1/4})$ er ikke en normal utvidelse av $\mathbb{Q}$, siden $2^{1/4}$ er rot i $f(x) = x^4-2$, men $w 2^{1/4}$ er ikke i $\mathbb{Q}(2^{1/4})$.

Oppg 2.

a) Finn enhetene i $\mathbb{Z}[\sqrt{-p}]$

Anta $u \cdot v = 1$. $\quad N(u \cdot v) = N(1) = 1$

$u = a + b\sqrt{-p}$

$v = c + d\sqrt{-p}$

$$\Updownarrow$$

$$(a^2 + pb^2)(c^2 + pd^2) = 1 \qquad a, b, c, d \in \mathbb{Z}.$$

$$\Downarrow$$

$$|a| = |c| = 1, \quad |b| = |d| = 0.$$

$$\Downarrow$$

Enhetene er ± 1.

Anta $1 \pm \sqrt{-p} = (a + b\sqrt{-p})(c + d\sqrt{-p})$

$$\Downarrow$$

$$1 + p = (a^2 + b^2 p)(c^2 + d^2 p)$$

$$\Downarrow$$

enten $a^2 = b^2 = 1 = c^2$ og $d = 0$ $\vee$ $a^2 = c^2 = d^2 = 1$ og $b = 0$.

$\Rightarrow 1 \pm \sqrt{-p}$ irredusibel.

Anta $2 = (1 + \sqrt{-p})(a + b\sqrt{-p})$

$$4 = (1 + p)(a^2 + b^2 p)$$

$\Rightarrow \quad p = 3 \quad a^2 = 1, \; b^2 = 0. \quad \Rightarrow \quad 1 + \sqrt{-p}$ ikke divisor i 2.

b) For p odde (altså $p \neq 2$)

er $\mathbb{Z}[\sqrt{-p}]$ ikke UFD

siden

$$(1+\sqrt{-p})(1-\sqrt{-p}) = 1+p = 2 \cdot \frac{1+p}{2}.$$

trenger p odde

Altså

$$\underbrace{(1+\sqrt{-p})(1-\sqrt{-p})}_{\text{irred.}} = 2 \cdot \frac{1+p}{2}$$

Hvis UFD, må $(1+\sqrt{-p})$ eller $(1-\sqrt{-p})$ være faktor i 2 ↯ (a)

(NB! $\mathbb{Z}[\sqrt{-2}]$ er UFD, øving 1).

3. Antall ulike F-automorfier $E \to E$ ($E \supseteq F$ endelig).

$E = F(\alpha)$.

$E \simeq F[x]/(p(x))$ $\quad p(x)$ min. poly. til $\alpha \in E$

I. En automorfi $\sigma : E \to E$ sender røtter til $p(x)$ til røtter av $p(x)$

(rot lemma)

II. En F-autom. $\sigma : E \to E$ er bestemt av $\sigma(\alpha)$

$\Rightarrow$ Det fins max. $\deg p(x) = [E : F]$ automorfier.

5. $[E : F]$ s.a. $2 \nmid [E:F]$ $\quad$ La $\alpha \in E$

$3 \nmid [E:F]$.

$F \subseteq F(\alpha^4) \subseteq F(\alpha^2) \subseteq F(\alpha) \subseteq E$ $\quad \Rightarrow [F(\alpha) : F(\alpha^2)] \mid [E:F]$

$F \subseteq F(\alpha^3) \subseteq F(\alpha) \subseteq E \quad \Rightarrow$ $\quad [F(\alpha^2) : F(\alpha^4)] \mid [E:F]$

$[F(\alpha) : F(\alpha^3)] \mid [E:F]$

$x^2 - \alpha^2 \in F[\alpha^2]$ har rot α.

så $[F(\alpha) : F(\alpha^2)] \leq 2$.

Også α^2 rot i $x^2 - \alpha^4 \in F(\alpha^4)$

så $[F(\alpha^2) : F(\alpha^4)] \leq 2$.

Og α rot i $x^3 - \alpha^3 \in F(\alpha^3)$

$[F(\alpha) : F(\alpha^3)] \leq 3$.

Men siden $2, 3 \nmid [B:F]$ ~~må~~ vi ha at

$$[F(\alpha^2) : F(\alpha^4)] = 1 = [F(\alpha) : F(\alpha^2)] = [F(\alpha) : F(\alpha^3)].$$

$$\Rightarrow F(\alpha) = F(\alpha^2) = F(\alpha^4) = F(\alpha^3)$$

Oppg. 6.

a) Teorem 18.1.1

b) (Spesialtilfelle av) Teorem 18.1.4

Oppg. 4

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{q}) \qquad p, q \text{ primtall.}$$

a) E er rotkroppen til $f(x) = (x^2 - p)(x^2 - q)$

og er dermed en normal utvidelse

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\sqrt{p})(\sqrt{q})$$

min.pol. $x^2 - p$ $\quad$ $x^2 - q$

Må vise at $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$.

Anta $\sqrt{q} = a + b\sqrt{p}$

$$\Downarrow$$

$$q = a^2 + 2ab\sqrt{p} + b^2 p$$

$$\Downarrow$$

enten $(ab \neq 0)$ $\sqrt{p} = \frac{q - a^2 - b^2 p}{2ab} \in \mathbb{Q}$ $\lightning$

eller $(a = 0)$ $q = b^2 p$ $\lightning$ $\quad$ q primtall.

eller $(b = 0)$ $q = a^2$ $\lightning$ $\quad$ — " —

Dermed $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{p})] \cdot [\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2 \cdot 2 = 4.$

En endelig, normal utvidelse av $\mathbb{Q}$ er en Galois-utvidelse, siden char $\mathbb{Q} = 0 \Rightarrow E \setminus F$ separabel.

La $\sigma \in G(B/\mathbb{Q})$:

Rotlemma $\Rightarrow$ $\sigma(\sqrt{p}) = \pm\sqrt{p}$

$\sigma(\sqrt{q}) = \pm\sqrt{q}$

$\Rightarrow \sigma^2 = id.$ (siden $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$ basis for $B \setminus \mathbb{Q}$)

$\Rightarrow G(B/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

b) GTFT $\Rightarrow$ det finnes tre mellomkropper (siden $\mathbb{Z}_2 \times \mathbb{Z}_2$ har tre ikke-trivielle ekte undergrupper).

Dette må da være

$\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{q})$ og $\mathbb{Q}(\sqrt{pq})$.

(sjekk gjerne at dette er E_{H_i} for de tre undergruppene H_i av $\mathbb{Z}_2 \times \mathbb{Z}_2$)