Øving 2 - MA3202

Øving 2.

15.1.1. $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_7[x]$ har ingen røtter i $\mathbb{Z}_7$, og er dermed irredusibel (Prop 1.3 i kap 15)

15.1.2. $x^4 + 8 \in \mathbb{Q}[x]$ har ingen røtter i $\mathbb{Q}$ og dermed er eneste mulighet for å faktorisere polynomet gitt ved

$$x^2 + 8 = (x^2 + ax + b)(x^2 + cx + d) \quad a, b, c, d \in \mathbb{Q}$$

Lemma 1.6 i kap 15: vi kan anta $a, b, c, d \in \mathbb{Z}$.

Får da
(1) $a + c = 0$
(2) $b + ac + d = 0$
(3) $ad + bc = 0$
(4) $bd = 8$

(1) + (3) gir
$a(d-b) = 0$

I. $a = 0$
$\Rightarrow b + d = 0$
$bd = 8$ $\not\#$ $b, d \in \mathbb{Z}$

II. $d = b$
$db = 8$ $\not\#$ $bd \in \mathbb{Z}$.

15.1.4. $f(x) = x^3 + ax^2 + bx + 1 \in \mathbb{Z}[x]$

redusibel $\Leftrightarrow$ $a = b$ eller $a + b = -2$.

Redusibel $\underset{\text{Prop 1.3.}}{\Leftrightarrow}$ $f(x)$ har rot i $\mathbb{Z}[x]$

Teorem 1.7 Hvis $f(x)$ har rot α må

$\alpha \mid 1 \Rightarrow \alpha = \pm 1$.

$f(1) = 1 + a + b + 1$

$f(-1) = a - b$.

Så f har rot $\Leftrightarrow$ $a + b = -2$ eller $a = b$.

16.1.6. a), b) Irreducible ved Eisensteins kriterium

$p = 5$.

b) $x^4 - 3x^2 + 9$

$$= (x^2 + ax + b)(x^2 + cx + d)$$

$$= x^4 + (a+c)x^3 + (d+b+ac)x^2$$

$$+ (ad+bc)x + bd$$

$\Rightarrow$

$$a + c = 0$$

$$d + b + ac = -3$$

$$ad + bc = 0 \quad \Rightarrow \quad a(d-b) = 0$$

$$bd = 9 \quad \Rightarrow \quad a = 0 \ \vee \ d = b$$

$$a = 0 \Rightarrow c = 0$$

$$d + b = -3$$

$$bd = 9$$

$\divideontimes$

Derved: $d = b$

$$bd = 3 \Rightarrow b = d = 3$$

$$\Rightarrow ac = -9$$

$$\Rightarrow a = 3 \text{ og } c = -3$$

$a, b, c, d = 3, 3, -3, 3$ oppfyller lignngene, så

$$x^4 - 3x^2 + 9 = (x^2 + 3x + 3)(x^2 - 3x + 3)$$

15.2.1. $p(x) = x^2 - x - 1$ irred. over $\mathbb{Z}_3$,

siden ingen rot i $\mathbb{Z}_3$ (prop 1.3)

$K = \mathbb{Z}[x]/(p(x)) \simeq \{a + b\alpha \mid a, b \in \mathbb{Z}_3\}$

med α rot i $p(x)$, altså

$\alpha^2 = \alpha + 1$.

Polynomdivisjon: $x^2 + 2x + 2 : x - \alpha = x + (2 + \alpha)$

Dermed: den andre rota: $-(2 + \alpha) = 2\alpha + 1$ er i K.

15.2.2. $p(x) = x^3 - 2 \in \mathbb{Q}[x]$

irred. (Eisensteins krit. $p = 2$).

Røtter: $2^{1/3}$, $w 2^{1/3}$, $w^2 2^{1/3}$ der $w = e^{\frac{2\pi i}{3}}$

Da er $\mathbb{Q}(2^{\frac{1}{3}}, w) = \mathbb{Q}(2^{1/3}, w 2^{1/3}, w^2 2^{1/3})$

en slik kropp siden $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$

da $2^{1/3}$ har min. pol. $p(x)$. og

$[\mathbb{Q}(\omega, 2^{1/3}) : \mathbb{Q}(2^{1/3})] = 2$ siden

ω er rot i $x^2+x+1=0$

(dette følger av at $x^3-1 = (x-1)(x^2+x+1)$)

som er irredusibel, og dermed min.poly. til ω.

Altså er $[\mathbb{Q}(\omega, 2^{1/3}) : \mathbb{Q}] = [\mathbb{Q}(\omega, 2^{1/3}) : \mathbb{Q}(2^{1/3})] \cdot [\mathbb{Q}(2^{1/3}) : \mathbb{Q}]$

$= 2 \cdot 3 = \underline{6}$

15.2.4. $x^2+4 = (x+2i)(x-2i)$

Så $\mathbb{Q}(2i) = \mathbb{Q}(i)$ inneholder alle røttere

153.2.

$\sqrt{2}, \sqrt{3}$ alg. over $\mathbb{Q}$

min. polynom $x^2-2 = f(x)$

$x^2-3 = g(x)$.

$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$

$[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$

$\mathbb{Q}(\sqrt{2},\sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$

$\sqrt{3} = a+b\sqrt{2}$

$3 = a^2 + 2\sqrt{2}ab + 2b^2$

$\Downarrow$

i) hvis $ab \neq 0 \Rightarrow \sqrt{2} \in \mathbb{Q}$ ↯

ii) $a=0$ $\quad 3 = 2b^2 \Rightarrow \sqrt{\frac{3}{2}} \in \mathbb{Q}$ ↯

iii) $b=0$ $\quad 3 = a^2 \Rightarrow \sqrt{3} \in \mathbb{Q}$ ↯.

$\Rightarrow x^2-3$ irreducibel over $\mathbb{Q}(\sqrt{2})$

$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$.

$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 2 \cdot 2 = 4$.

Påstand: $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\supseteq$ ok.

Nok å vise $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$$(\sqrt{2}+\sqrt{3})^3 = \sqrt{2}^3 + 3\cdot 2\sqrt{3} + 3\cdot 3\sqrt{2} + \sqrt{3}^3$$

$$= 2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3}$$

$$= 11\sqrt{2} + 9\sqrt{3} = 9(\sqrt{2}+\sqrt{3}) + 2\sqrt{2}$$

$$\sqrt{2} = \frac{(\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})}{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

$\sqrt{3} = (\sqrt{2}+\sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

Generelt : $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p}+\sqrt{q})$

Hint: se på $(\sqrt{p}+\sqrt{q})^3$

Vis at $\sqrt{p} = \dfrac{(\sqrt{p}+\sqrt{q})^3 - (p+3q)(\sqrt{p}+\sqrt{q})}{2p-2q}$

15.3.8.

$x^n - a \in F[x]$ irredusibel, $b \in K \supseteq F$ rot.

La $m|n$ $n = mq$.

$$\Downarrow$$

$$F \subseteq F(b^m) \subseteq F(b)$$

$$\Uparrow$$

$$b^m \in F(b)$$

$x^n - a$ irred. $\Rightarrow$ $[F(b):F] = n$

(og dermed min. pol til b).

Vi har $[F(b):F(b^m)]\,[F(b^m):F] = n$ $(*)$ ved teorem 2.1.

b^m er rot i $x^q - a \in F[x]$ $\Rightarrow$ $[F(b^m):F] \leq q$.

(da er min. pol. til b^m en divisor i $x^q - a$)

b er rot i $x^m - b^m \in F(b^m)[x]$ så dermed er $[F(b):F(b^m)] \leq m$.

Kombinert med $(*)$ gir dette at $[F(b):F(b^m)] = m$ og $[F(b^m):F] = q$

15.3.10

Hint: se på $\mathbb{Q}(w^2) \subseteq \mathbb{Q}(w)$

der w er transendent over $\mathbb{Q}$, e.g. $w = \pi$.

Husk: $\mathbb{Q}(x) = \left\{ f(x)/g(x) \;\middle|\; f, g \in \mathbb{Q}[x] \;\; g \neq 0 \right\}$

Sjekk at $w \notin \mathbb{Q}(w^2)$ og at

$$\mathbb{Q}(w) \to \mathbb{Q}(w^2)$$

$$p(w)/q(w) \longrightarrow p(w^2)/q(w^2)$$ er ikke-null ring homomorfi (og dermed innbedding).