Übungsblatt 5

Aufgabe 1

~~Bemerkung~~
Erinnerung (Aufgabe 2, Tutoriumsblatt 5):

Irreduzible Polynome in $\mathbb{F}_2[X]$

$$\left.\begin{array}{ll}\text{Grad } 2: & X^2+X+1 \\ \text{Grad } 3: & X^3+X^2+1, \quad X^3+X+1\end{array}\right\} \text{keine Nullstelle in } \mathbb{F}_2$$

$$\text{Grad } 4: \quad \underbrace{X^4+X^3+1, \quad X^4+X+1, \quad X^4+X^3+X^2+X+1}_{\text{keine NS und } \neq (X^2+X+1)^2 = X^4+X^2+1}$$

(1)

$$X^4-2X^3+X+3 \mod 2 = \underset{\text{irreduzibel}}{X^4+X+1} \in \mathbb{F}_2[X]$$

$$\underset{\text{in } \mathbb{Z}[X]}{\text{irreduzibel}} \xleftarrow[\text{Satz 2.35}]{}$$

(2) $f = X^5-6X^3+2X^2-4X+5 \mod 2 = X^5+1 = (X+1)\underbrace{(X^4+X^3+X^2+X+1)}_{\substack{\text{irreduzibel}\\ \text{nach Bmk}}}$ in $\mathbb{F}_2[X]$

Angenommen, $f = P\cdot Q$ ist reduzibel in $\mathbb{Z}[X]$ ($\underset{\text{Satz von Gauß}}{\Leftrightarrow}$ $\mathbb{Q}[X]$)

Wir können annehmen P & Q normiert (da f normiert ist)

$$\begin{array}{ll}\mathbb{Z}[X] & f = P\cdot Q \\ \big\downarrow & \big\downarrow \text{ Reduktion mod 2} \\ \mathbb{F}_2[X] & \bar{f} = \bar{P}\cdot\bar{Q} = (X+1)(X^4+X^3+X^2+X+1)\end{array}$$

Grad $=1$ irreduzibel in $\mathbb{F}_2[X]$

Grad $\bar{P}$ = Grad $P \geq 1$
Grad $\bar{Q}$ = Grad $Q \geq 1$
da P & Q normiert sind

Es folgt dass Grad P = Grad $\bar{P} = 1$
(oder Grad Q = Grad $\bar{Q} = 1$)
$\Downarrow$
f hat eine NS in $\mathbb{Z}$

Aber f hat keine NS in $\mathbb{Z}$ (es ist genug zu zeigen dass $\pm 1, \pm 5$ keine NS sind) Widerspruch ↯

Aufgabe 2

a) $\alpha = \sqrt{1+\sqrt{3}} \in \mathbb{R}$

$$\alpha^2 = 1 + \sqrt{3}$$
$$\alpha^2 - 1 = \sqrt{3}$$
$$(\alpha^2 - 1)^2 = 3 \implies \alpha^4 - 2\alpha^2 + 2 = 0$$

α ist eine Nullstelle von $P(X) = X^4 - 2X^2 + 2 \in \mathbb{Z}[X]$

Nach Eisensteinkriterium $(p=2)$ ist $P(X)$ irreduzibel in $\mathbb{Z}[X]$ (auch in $\mathbb{Q}[X]$ nach Gauss Lemma)

Es folgt: $P(X)$ ist das min. Polynom von α über $\mathbb{Q}$.

Wir haben $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \text{Grad } P = 4$

b) $\beta = \sqrt{3 + 2\sqrt{2}} \in \mathbb{R}$

$$\beta^2 = 3 + 2\sqrt{2}$$
$$\beta^2 - 3 = 2\sqrt{2} \implies (\beta^2 - 3)^2 = 8 \implies \beta^4 - 6\beta^2 + 1 = 0$$

β ist eine Nullstelle von $P(X) = X^4 - 6X^2 + 1$

$P(X)$ hat keine Nullstellen in $\mathbb{Z}$.

Wenn $P(X)$ ist reduzibel in $\mathbb{Z}[X]$, dann gilt

$$P = X^4 - 6X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d), \quad a, b, c, d \in \mathbb{Z}$$

$\Downarrow$ Vergleich der Koeffizienten

$$X^3: \quad 0 = a + c \implies c = -a$$
$$X^2: \quad -6 = -a^2 + b + d \quad (*)$$
$$X: \quad 0 = ad + bc$$
$$X^0: \quad 1 = bd \implies b = d = 1 \text{ oder } b = d = -1$$

$\Downarrow (*)$

$$-6 = -a^2 - 2$$
$$\Downarrow$$
$$a^2 = 4 \implies a = \pm 2$$

Wir bekommen die Zerlegung:

$$P = X^4 - 6X^2 + 1 = (X^2 + 2X \mp 1)(X^2 - 2X - 1)$$

irreduzibel, da keine NS in $\mathbb{Z}$

Minimal Polynom von $\beta/\mathbb{Q}$ teilt $P \implies$ hat Grad 2 $\implies |\mathbb{Q}(\beta) : \mathbb{Q}| = 2$

Bemerkung 1: Man kann einfache die Zerlegung von P finden:

$$P = X^4 - 6X^2 + 1 = X^4 - 2X^2 + 1 - 4X^2 = (X^2-1)^2 - (2X)^2 =$$
$$= (X^2 + 2X - 1)(X^2 - 2X - 1)$$

Bemerkung 2: Es ist schwer zu bemerken, aber es gilt

$$\beta = \sqrt{3+2\sqrt{2}} = \sqrt{1 + 2\sqrt{2} + (\sqrt{2})^2} = \sqrt{(1+\sqrt{2})^2} = 1+\sqrt{2}$$

Dann $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2})$ und $|\mathbb{Q}(\beta) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$

Aufgabe 3

(1) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$

Grad 2, da x^2-2 ist das min. Polynom von $\sqrt{2}$ über $\mathbb{Q}$.

?

Min. Polynom von $\sqrt{3}$ über $\mathbb{Q}[\sqrt{2}]$ teilt x^2-3

$\Rightarrow$ Grad = 1 oder 2

Angenommen, $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 1$

Dann $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2},\sqrt{3}) \Leftrightarrow \sqrt{3} \in \mathbb{Q}(\sqrt{2})$.

$\mathbb{Q}$-Basis $1, \sqrt{2}$.

Es folgt: $\sqrt{3} = a \cdot 1 + b \cdot \sqrt{2}$ mit $a, b \in \mathbb{Q}$

$$\Downarrow$$

$$\underset{\in\mathbb{Q}}{3} = \underset{\in\mathbb{Q}}{a^2} + \underset{\in\mathbb{Q}}{\underbrace{2ab}}\sqrt{2} + \underset{\in\mathbb{Q}}{\underbrace{2b^2}} \quad \text{in } \mathbb{Q}(\sqrt{2})$$

$$\Downarrow$$

$2ab = 0$ (sonst $\sqrt{2} \in \mathbb{Q}$)

$a = 0 \Rightarrow 3 = 2b^2$ nicht möglich in $\mathbb{Q}$ $\left(\sqrt{\tfrac{3}{2}} \notin \mathbb{Q}\right)$

$b = 0 \Rightarrow 3 = a^2$ —— " ——

$\lightning$ mit $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 1$

Es folgt:

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

$\Downarrow$ Grad formel

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

Aufgabe 3

(2) $1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}$ ist eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{2},\sqrt{3})$. ~~über $\mathbb{Q}$~~.

Sei $\alpha = \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$. Angenommen, $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subsetneq \mathbb{Q}(\sqrt{2},\sqrt{3})$

$$\overbrace{\mathbb{Q} \underset{2}{\subset} \mathbb{Q}(\underbrace{\sqrt{2}+\sqrt{3}}_{\notin \mathbb{Q}}) \underset{2}{\subsetneq} \mathbb{Q}(\sqrt{2},\sqrt{3})}^{4 \text{ nach } 1)}$$

Wenn $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ dann $1, \alpha$ ist eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\alpha)$.

$\alpha^2 \in \mathbb{Q}(\alpha) \Rightarrow \alpha^2 = a \cdot 1 + b \cdot \alpha$ in $\mathbb{Q}(\alpha)$ mit $a, b \in \mathbb{Q}$

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

$$5 + 2\sqrt{6} = a + b\sqrt{2} + b\sqrt{3}$$

$$\underline{\underline{(5-a)}} \cdot 1 - \underline{\underline{b}}\sqrt{2} - \underline{\underline{b}}\sqrt{3} + \underline{\underline{2}}\sqrt{2}\sqrt{3} = 0 \quad ⚡$$

da $1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}$ $\mathbb{Q}$-linear unabhängig sind

(3)

$$\alpha = \sqrt{2}+\sqrt{3}$$
$$\alpha^2 = 5 + 2\sqrt{6}$$
$$\alpha^2 - 5 = 2\sqrt{6}$$
$$(\alpha^2-5)^2 = 24$$
$$\alpha^4 - 10\alpha^2 + 1 = 0$$
$$\Downarrow$$

α ist eine NS von $X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$

- Min Polynom f von α teilt $X^4 - 10X^2 + 1$
- $\operatorname{Grad} f = [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] \overset{(1)}{=} 4$

Es folgt: $f = X^4 - 10X^2 + 1$.

Aufgabe 4

$f = x^{p-1} + x^{p-2} + \dots + x + 1$ primitive $\Rightarrow$ (irr in $\mathbb{Z}[X] \Leftrightarrow$ irr in $\mathbb{Q}[X]$)

$f(x)$ ist irreduzibel in $\mathbb{Z}[X]$ $\Leftrightarrow$ $\tilde{f}(x) := f(x+1)$ irred. in $\mathbb{Z}[X]$.

$$f = \frac{x^p - 1}{x - 1}$$

$$\tilde{f} = f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x} =$$

$$= \frac{\sum_{k=0}^{p} \binom{p}{k} x^k - 1}{x} \underset{\binom{p}{0} x^0 = 1}{=\!=\!=} \sum_{k=1}^{p} \binom{p}{k} x^{k-1}$$

Wir wollen Eisensteinkriterium (Satz 2.34) für Primzahl p

~~Lead~~ Hauptkoeff von x^{p-1}: $\binom{p}{p} x^{p-1} = x^{p-1}$ $\Rightarrow$ $\tilde{f}$ ist normiert

für $1 \leq k \leq p-1$ $\quad p \mid \binom{p}{k} = \dfrac{p!}{\underbrace{k!(p-k)!}_{\text{teilerfremd mit } p}}$

$k = 1$ $\quad \binom{p}{1} x^{1-1} = \dfrac{p!}{1!(p-1)!} = p$ ← nicht durch p^2 teilbar

Es folgt nach Eisensteinkriterium: $\tilde{f}$ ist irr in $\mathbb{Z}[X]$

$\Downarrow$

auch f ist irreduzibel