

Algebra II, SoSe 2012 - Lösung Blatt 1

1.1. Wir zeigen vorab:

$K[X]$ enthält unendlich viele paarweise nichtassozierte (*) irreduzible Polynome.

Dazu übertragen wir Euklids Beweis über die Unendlichkeit der Menge der Primzahlen in $\mathbb{Z}$ auf unsere Situation.

↗ $K[X]$ enthält nur endlich viele paarweise nichtassozierte irreduzible Polynome

$$p_1, \dots, p_r \in K[X].$$

(beachte: Es gibt mindestens eines, z.B. $X-1$). Dann:

$$p_i \text{ irreduzibel} \Rightarrow \deg p_i \geq 1 \quad \forall i$$

Definiere

$$a := \left(\prod_{i=1}^r p_i \right) + 1 \in K[X]$$

$$\text{Da } K \text{ Körper, folgt } \deg \prod_{i=1}^r p_i = \sum_{i=1}^r \underbrace{\deg p_i}_{\geq 1} \geq r$$

und damit $\deg a \geq r \geq 1$, also $a \notin K$.

Wegen $(K[X])^* = K^*$ ist damit $a \neq 0$ und keine Einheit.

Da K Körper folgt:

$K[X]$ euklidischer Ring, insbesondere faktorieller Ring.

a kann also in irreduzible Faktoren zerlegt werden.

^{insb.}
 $\Rightarrow \exists p \in K[X]$ irreduzibel mit $p \mid a$

Indem wir p ggf. mit einer Einheit multiplizieren können wir also annehmen:

$$p = p_j \quad \text{für ein } j \in \{1, \dots, r\}.$$

$$\text{Damit folgt: } p_j = p \mid a \quad \text{und} \quad p_j \mid \left(\prod_{i=1}^r p_i \right)$$

$$\Rightarrow p_j \mid \left(a - \prod_{i=1}^r p_i \right)$$

$$\left(\text{Denn: } p_j \cdot c_1 = a, \quad p_j \cdot c_2 = \prod_{i=1}^r p_i \right)$$

$$\Rightarrow a - \prod_{i=1}^r p_i = p_j \cdot c_1 - p_j \cdot c_2 = p_j (c_1 - c_2)$$

Da $a - \prod_{i=1}^r p_i = 1$ gilt, folgt also: $p_j \mid 1$, d.h.
 p_j ist Einheit $\swarrow$
 p_j irreduzibel

Also ist (*) gezeigt. Damit folgt die Aussage sofort:

(*) ^{insb.} $\Rightarrow \exists N$ -viele paarweise nichtassozierte irreduzible Polynome
 $p_i \in K[X], i \in N$

Durch Multiplikation mit geeigneten Einheiten dürfen wir annehmen:

$$p_i \text{ normiert} \quad \forall i \in N$$

Da K algebraisch abgeschlossen ist, gilt $\deg p_i = 1 \quad \forall i \in N$

(sonst: p_i zerfällt über K in Linearfaktoren, d.h.

$$p_i = \prod_j \underbrace{(X - d_j)}_{\notin K^*} \quad \begin{array}{l} \text{↯} \\ p_i \text{ irreduzibel} \end{array} \quad \Bigg)$$

$$\Rightarrow p_i = X - c_i \quad \forall i \in \mathbb{N} \text{ und geeignete } c_i \in K.$$

$$p_i \text{ paarweise nicht assoziiert} \Rightarrow c_i \neq c_j \quad \forall i \neq j$$

$$\Rightarrow |\{c_i \mid i \in \mathbb{N}\}| = \infty \quad \text{d.h. insbesondere } |K| = \infty.$$



1.2. • Wir berechnen zunächst den Zerfällungskörper L_a von $f_a := X^2 + a \in \mathbb{Q}[X]$ für $a \in \mathbb{Q}$.

Behauptung: $\forall a \in \mathbb{Q}$ gilt

$$L_a = \{c + \alpha d \mid c, d \in \mathbb{Q}\} \subset \mathbb{C} \quad (*)$$

wobei $\alpha \in \mathbb{C}$ eine Nullstelle von f_a sei.

Dazu:

Sei $\alpha \in \mathbb{C}$ eine Nullstelle von f_a .

$\Rightarrow -\alpha$ ist weitere Nullstelle und $\{\alpha, -\alpha\}$ sind alle Nullstellen von f_a .

$$\begin{aligned} \Rightarrow L_a &= \mathbb{Q}(\alpha, -\alpha) = \mathbb{Q}(\alpha) \stackrel{\alpha \text{ algebraisch}}{=} \mathbb{Q}[\alpha] \\ &= \{f(\alpha) \mid f \in \mathbb{Q}[X]\} \end{aligned}$$

$$\begin{aligned} \stackrel{\substack{\alpha^2 \in \mathbb{Q} \\ \text{da } \alpha^2 = -a}}{\curvearrowright} &= \{f(\alpha) \mid f \in \mathbb{Q}[X], \deg f \leq 1\} \\ &= \{c + \alpha d \mid c, d \in \mathbb{Q}\} \end{aligned}$$

also ist $(*)$ nachgewiesen.

$$\left(\text{Alternativ: Die Menge ist bereits Körper, da} \right. \\ \left. \frac{1}{c + \alpha d} = \frac{c - \alpha d}{(c + \alpha d)(c - \alpha d)} = \frac{c - \alpha d}{c^2 - \alpha^2 d} = \frac{c}{c^2 + \alpha d^2} - \alpha \frac{d}{c^2 + \alpha d^2} \right)$$

$\swarrow \quad \searrow$
 $\in \mathbb{Q} \quad \in \mathbb{Q}$

- Seien $a, b \in \mathbb{Q}^*$ mit $L_a = L_b$ gegeben. Wir zeigen:

$$\exists f \in \mathbb{Q}^* \text{ mit } b = f^2 a.$$

Dazu:

Seien $\alpha, \beta \in \mathbb{C}$ die Nullstellen von f_a bzw. f_b .

$$a, b \neq 0 \Rightarrow \alpha, \beta \neq 0.$$

- Gelte $\alpha \in \mathbb{Q}$. Dann:

$$\mathbb{Q} = \mathbb{Q}(\alpha) = L_a = L_b = \mathbb{Q}(\beta) \Rightarrow \beta \in \mathbb{Q}$$

Schreibe $\beta = \frac{\beta}{\alpha} \cdot \alpha \Rightarrow f := \frac{\beta}{\alpha} \in \mathbb{Q}^*$ (beachte: $\alpha, \beta \neq 0$)

Damit:

$$b = -\beta^2 = -(f\alpha)^2 = -f^2 \alpha^2 = f^2 a, \text{ d.h.}$$

die Aussage stimmt.

- Gelte $\alpha \notin \mathbb{Q}$.

$$\Rightarrow \beta \notin \mathbb{Q} \quad (\text{sonst: } \mathbb{Q} = \mathbb{Q}(\beta) = L_b = L_a = \mathbb{Q}(\alpha) \Rightarrow \alpha \in \mathbb{Q} \text{ } \nabla)$$

Wegen $L_a = L_b$ folgt aus (*):

$$\beta \in \{c + \alpha d \mid c, d \in \mathbb{Q}\}$$

$$\Rightarrow \beta = e + \alpha f \quad \text{für gewisse } e, f \in \mathbb{Q}.$$

Es ist $f \neq 0$, da sonst $\beta = e \in \mathbb{Q}$ wäre $\nabla \beta \notin \mathbb{Q}$.

$$\text{Also: } \beta = e + \alpha f \quad \text{für gewisse } e \in \mathbb{Q}, f \in \mathbb{Q}^*$$

Wir berechnen:

$$\begin{aligned} -b = \beta^2 &= (e + \alpha f)^2 = e^2 + 2ef\alpha + \alpha^2 f^2 \\ &= e^2 + 2ef\alpha - af^2 \end{aligned}$$

$$\Rightarrow e\alpha \stackrel{f \neq 0}{=} \frac{af^2 - b - e^2}{2f} \in \mathbb{Q} \quad (\text{da } a, b, e, f \in \mathbb{Q})$$

$$\Rightarrow e = 0, \text{ da sonst } \alpha = \frac{af^2 - b - e^2}{2ef} \in \mathbb{Q} \quad \nRightarrow \alpha \notin \mathbb{Q}.$$

Damit haben wir gezeigt: $\beta = f \cdot \alpha$ für ein $f \in \mathbb{Q}^*$.

Wie oben im Fall $\alpha \in \mathbb{Q}$ folgt nun

$$b = -\beta^2 = -f^2 \alpha^2 = f^2 a.$$

In jedem Fall gilt also die Behauptung.

- Seien nun $a, b \in \mathbb{Q}^*$ mit $b = f^2 a$ für ein $f \in \mathbb{Q}^*$ gegeben.

Wir zeigen: $L_a = L_b$

Sei wieder $\alpha \in \mathbb{C}$ die Nullstelle von f_a , d.h. $\alpha^2 = -a$.

Dann:

$$(f\alpha)^2 = f^2 \alpha^2 = -f^2 a = -b,$$

d.h. $f\alpha$ ist Nullstelle von f_b und damit folgt aus (*):

$$L_b = \{c + f\alpha d \mid c, d \in \mathbb{Q}\}$$

$$f \in \mathbb{Q}^* \Rightarrow \{c + \alpha d \mid c, d \in \mathbb{Q}\} = L_a \quad \text{wie gewünscht.}$$

Damit haben wir:

$$\{(a,b) \in (\mathbb{Q}^*)^2 \mid L_a = L_b\} = \{(a,b) \in (\mathbb{Q}^*)^2 \mid \exists f \in \mathbb{Q}^* \text{ mit } b = f^2 a\}$$

- Die Fälle $a=0$ bzw. $b=0$.

Seien wieder $\alpha, \beta \in \mathbb{C}$ die Nullstellen von f_a bzw. f_b .

Ist $a=0$, dann: $\alpha=0$

$\Rightarrow \mathbb{Q} = \mathbb{Q}(\alpha)$ und damit:

$$L_a = L_b \stackrel{(*)}{\Leftrightarrow} \mathbb{Q}(\beta) = \mathbb{Q} \Leftrightarrow \beta \in \mathbb{Q}$$

$$\Leftrightarrow b = -c^2 \text{ für ein } c \in \mathbb{Q}$$

Analog gilt im Fall $b=0$:

$$L_a = L_b \Leftrightarrow a = -c^2 \text{ für ein } c \in \mathbb{Q}.$$

Damit ergibt sich insgesamt:

$$\{(a,b) \in \mathbb{Q}^2 \mid L_a = L_b\}$$

$$= \{(a,b) \in (\mathbb{Q}^*)^2 \mid \exists f \in \mathbb{Q}^* \text{ mit } b = f^2 a\}$$

$$\cup \{(0, -c^2) \in \mathbb{Q}^2 \mid c \in \mathbb{Q}\}$$

$$\cup \{(-c^2, 0) \in \mathbb{Q}^2 \mid c \in \mathbb{Q}\}.$$



1.3. (i) $X^2 - 3 \in \mathbb{Q}[X]$

Nullstellen in $\mathbb{C}$: $\pm\sqrt{3}$.

$\Rightarrow \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{3}, -\sqrt{3})$ ist Zerfällungskörper
(explizit wie in 1.2: $\mathbb{Q}(\sqrt{3}) = \{c + \sqrt{3}d \mid c, d \in \mathbb{Q}\}$)

$X^2 - 3$ ist irreduzibel, z.B.

$X^2 - 3$ primitiv $\Rightarrow$ genügt Irreduzibilität über $\mathbb{Z}$ zu zeigen.

Wähle $p = 3 \Rightarrow p \nmid 1, p \mid 3, p^2 \nmid 3$

$\xRightarrow{\text{Eisenstein}} X^2 - 3$ irreduzibel. (alternativ: direkt wegen Nullstellen)

$\Rightarrow X^2 - 3$ ist Minimalpolynom von $\sqrt{3}$ (da normiert)

$$\xRightarrow{\text{VL}} [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \deg(X^2 - 3) = 2.$$

(ii) $f = X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$

• Wähle $p = 2 \Rightarrow p \nmid 1, p \mid -2, p^2 \nmid -2$

$\xRightarrow{\text{Eisenstein}} f$ ist irreduzibel über $\mathbb{Z}$

$\xRightarrow{f \text{ primitiv}} f$ ist irreduzibel über $\mathbb{Q}$

• Bestimme Zerfällungskörper

$$\begin{aligned} X^4 - 2X^2 - 2 &= (X^2)^2 - 2 \cdot 1 \cdot X^2 + 1^2 - 1^2 - 2 \\ &= (X^2 - 1)^2 - 3 \\ &= (X^2 - 1)^2 - \sqrt{3}^2 \\ &= (X^2 - 1 + \sqrt{3})(X^2 - 1 - \sqrt{3}) \end{aligned}$$

$\Rightarrow$ Die Nullstellen von f in $\mathbb{C}$ sind

$$\pm \sqrt{1+\sqrt{3}} \quad \text{und} \quad \pm \sqrt{1-\sqrt{3}}$$

$$\Rightarrow Z := \mathbb{Q}(\sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}}) \subset \mathbb{C}$$

ist der Zerfällungskörper von f in $\mathbb{C}$.

• Bestimme den Grad $[Z:\mathbb{Q}]$

Adjungiere zunächst $\sqrt{1+\sqrt{3}}$ zu $\mathbb{Q}$. Da f normiert und irreduzibel über $\mathbb{Q}$ ist und $f(\sqrt{1+\sqrt{3}}) = 0$ gilt, ist f das Minimalpolynom von $\sqrt{1+\sqrt{3}}$ über $\mathbb{Q}$.

$$\stackrel{VL}{\Rightarrow} [\mathbb{Q}(\sqrt{1+\sqrt{3}}):\mathbb{Q}] = \deg f = 4$$

$$\text{Nun ist } \sqrt{1+\sqrt{3}} \in \mathbb{Q}(\sqrt{1+\sqrt{3}})$$

$$\stackrel{+2}{\Rightarrow} 1+\sqrt{3} \in \mathbb{Q}(\sqrt{1+\sqrt{3}})$$

$$\stackrel{\cdot(-1)}{\Rightarrow} -1-\sqrt{3} \in \mathbb{Q}(\sqrt{1+\sqrt{3}})$$

$$\stackrel{+2}{\Rightarrow} 1-\sqrt{3} \in \mathbb{Q}(\sqrt{1+\sqrt{3}})$$

$$\text{Betrachte } g := X^2 - (1-\sqrt{3}) \in \mathbb{Q}(\sqrt{1+\sqrt{3}})[X]$$

$$\text{Nullstellen von } g: \pm \sqrt{1-\sqrt{3}}.$$

$$\text{Da } 1-\sqrt{3} < 0 \text{ gilt, ist } \sqrt{1-\sqrt{3}} \notin \mathbb{R}.$$

$$\text{Andererseits ist } 1+\sqrt{3} > 0, \text{ d.h. } \sqrt{1+\sqrt{3}} \in \mathbb{R} \text{ und damit}$$

$$\mathbb{Q}(\sqrt{1+\sqrt{3}}) \subset \mathbb{R}$$

$$\Rightarrow \pm \sqrt{1-\sqrt{3}} \notin \mathbb{Q}(\sqrt{1+\sqrt{3}})$$

$\Rightarrow g \in \mathbb{Q}(\sqrt{1+\sqrt{3}})[X]$ ist irreduzibel und (da normiert)
damit das Minimalpolynom von $\sqrt{1-\sqrt{3}}$ über $\mathbb{Q}(\sqrt{1+\sqrt{3}})$.

$$\Rightarrow [\mathbb{Q}(\sqrt{1+\sqrt{3}})(\sqrt{1-\sqrt{3}}) : \mathbb{Q}(\sqrt{1+\sqrt{3}})] = \deg g = 2.$$

Wegen $Z = \mathbb{Q}(\sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}}) = \mathbb{Q}(\sqrt{1+\sqrt{3}})(\sqrt{1-\sqrt{3}})$

folgt schließlich:

$$[Z : \mathbb{Q}] = \underbrace{[Z : \mathbb{Q}(\sqrt{1+\sqrt{3}})]}_{=2} \cdot \underbrace{[\mathbb{Q}(\sqrt{1+\sqrt{3}}) : \mathbb{Q}]}_{=4} = 8.$$

(iii) $f = X^4 + 1 \in \mathbb{Q}[X]$.

• Ist $\alpha \in \mathbb{C}$ Nullstelle, d.h. $\alpha^4 = -1$, dann

$$(-\alpha)^4 = \alpha^4 = -1, \quad \left(\frac{1}{\alpha}\right)^4 = \frac{1}{\alpha^4} = \frac{1}{-1} = -1$$

$$\left(-\frac{1}{\alpha}\right)^4 = \left(\frac{1}{\alpha}\right)^4 = -1$$

d.h. die Nullstellen sind $\{\alpha, -\alpha, \frac{1}{\alpha}, -\frac{1}{\alpha}\}$.

Es ist

$$\left(e^{\frac{\pi i}{4}}\right)^4 + 1 = e^{\pi i} + 1 = -1 + 1 = 0$$

d.h. $e^{\frac{\pi i}{4}} \in \mathbb{C}$ ist Nullstelle von f .

$\Rightarrow$ Der Zerfällungskörper von f ist

$$Z = \mathbb{Q}(e^{\frac{\pi i}{4}}) \subset \mathbb{C}$$

• Berechne den Grad. Zeigen: f ist irreduzibel.

f primitiv $\xRightarrow{\text{Gauß}}$ genügt zu zeigen, dass f über $\mathbb{Z}$ irreduzibel ist.

Da $\text{ggT}(1,4)=1$, kann sich in $\mathbb{Z}$ kein Primelement aus $\mathbb{Z}$ abspalten. Da f in $\mathbb{Z}$ keine Nullstelle besitzt, spaltet sich kein Linearfaktor ab. Einzige Möglichkeit wäre

$$\begin{aligned} X^4 + 1 &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a+c)X^3 + (ac+b+d)X^2 + (ad+bc)X + bd \end{aligned}$$

$$\Rightarrow b \cdot d = 1 \Rightarrow b = d = 1 \text{ oder } b = d = -1$$

$$a + c = 0 \Rightarrow a = -c$$

Also:

$$0 = ac + b + d = -c^2 + b + d$$

$$\Rightarrow \underbrace{b+d}_{=2 \text{ oder } -2} = c^2 \Rightarrow c \notin \mathbb{Z} \quad \text{⚡}$$

Also ist $f \in \mathbb{Q}[X]$ irreduzibel, d.h. Minimalpolynom von $e^{\frac{\pi i}{4}}$.
 $\Rightarrow [Z : \mathbb{Q}] = \deg f = 4$.

(iv) $f = X^5 - 1 \in \mathbb{Q}[X]$.

- Zunächst: Ist $\alpha \in \mathbb{C}$ Nullstelle von f , d.h. $\alpha^5 = 1$, dann $(\alpha^k)^5 = (\alpha^5)^k = 1^k = 1$, d.h. α^k Nullstelle von f .

- $\alpha := e^{\frac{2\pi i}{5}} \in \mathbb{C} \Rightarrow f(\alpha) = \alpha^5 - 1 = e^{2\pi i} - 1 = 1 - 1 = 0$

Da weiter $\alpha^0, \alpha^1, \dots, \alpha^4$ jeweils verschieden und damit alle Nullstellen von f sind, folgt:

$$Z = \mathbb{Q}\left(e^{\frac{2\pi i}{5}}\right)$$

ist Zerfällungskörper von f .

- f ist nicht irreduzibel:

$$X^5 - 1 = (X - 1) \underbrace{(X^4 + X^3 + X^2 + X + 1)}_{=: g}$$

Wir behaupten, dass g das Minimalpolynom von $e^{\frac{2\pi i}{5}}$ über $\mathbb{Q}$ ist. Damit folgt dann: $[Z : \mathbb{Q}] = \deg g = 4$.

Da g normiert und $g(e^{\frac{2\pi i}{5}}) = 0$ ist, genügt es also zu zeigen: $g \in \mathbb{Q}[X]$ irreduzibel.

Zu diesem Zweck zeigen wir, dass $g(X+1)$ irreduzibel ist. Wäre dann g reduzibel,

$$g = g_1 \cdot g_2 \quad \deg g_1, \deg g_2 \geq 1$$

so wegen $g(X+1) = g_1(X+1) \cdot g_2(X+1)$ auch $g(X+1)$.

Zum Berechnen von $g(X+1)$ arbeiten wir in $\mathbb{Q}(X)$:

$$g(X) = \frac{X^5 - 1}{X - 1} \Rightarrow g(X+1) = \frac{(X+1)^5 - 1}{X}$$

$$\begin{aligned} \text{Es ist } (X+1)^5 - 1 &= \left(\sum_{k=0}^5 \binom{5}{k} X^k \right) - 1 \\ &= \sum_{k=1}^5 \binom{5}{k} X^k \end{aligned}$$

also:

$$g(X+1) = \sum_{k=1}^5 \binom{5}{k} X^{k-1} = X^4 + 5X^3 + 10X^2 + 10X + 5$$

Da $g(X+1)$ primitiv ist, genügt es, Irreduzibilität über $\mathbb{Z}$ zu zeigen. Wähle $p=5$, dann:

$$p \nmid 1, \quad p \mid 5, \quad p \mid 10, \quad p^2 \nmid 5$$

Eisenstein

$\Rightarrow g(X+1)$ irreduzibel

s.o.

$\Rightarrow g$ irreduzibel.



1.4. • Zeigen zunächst:

$f = X^4 + 6X^2 + 1 \in \mathbb{Q}[X]$ ist irreduzibel.

f primitiv $\xRightarrow{\text{Gauß}}$ genügt Irreduzibilität in $\mathbb{Z}[X]$ zu zeigen.

Da $\text{ggT}(1, 6, 1) = 1$ ist, können sich keine Primelemente aus $\mathbb{Z}$ abspalten.

$\Rightarrow$ Es sind höchstens Zerlegungen des Typs

„Grad 1, Grad 3“ oder „Grad 2, Grad 2“
möglich. ($\mathbb{Z}$ ist Integritätsring).

$$\begin{aligned}\text{Es ist } X^4 + 6X^2 + 1 &= (X^2)^2 + 2 \cdot 3X^2 + 9 - 9 + 1 \\ &= (X^2 + 3)^2 - 8 \\ &= (X^2 + 3)^2 - \sqrt{8}^2 \\ &= (X^2 + \underbrace{3 - \sqrt{8}}_{\notin \mathbb{Z}})(X^2 + \underbrace{3 + \sqrt{8}}_{\notin \mathbb{Z}})\end{aligned}$$

$\Rightarrow f$ besitzt in $\mathbb{Z}$ keine Nullstellen, d.h. in $\mathbb{Z}$ kann kein Linearfaktor abgespalten werden.

 f über $\mathbb{Z}$ reduzibel

$$\begin{aligned}\xRightarrow{\text{Vorüber-}} \quad X^4 + 6X^2 + 1 &= (X^2 + aX + b)(X^2 + cX + d) \quad a, b, c, d \in \mathbb{Z} \\ \text{legungen} \quad &= X^4 + (a+c)X^3 + (ac+b+d)X^2 + (ad+bc)X + bd\end{aligned}$$

"Grad 0": $b \cdot d = 1 \Rightarrow b = d = 1 \text{ oder } b = d = -1$

"Grad 3": $a + c = 0 \Rightarrow a = -c$

"Grad 2": $\underbrace{ac}_{=-c^2} + b + d = 6$

$$\Rightarrow \underbrace{b+d}_{\in \{-2, 2\}} = 6 + c^2 \geq 6 \quad \text{⚡}$$

Also ist $f \in \mathbb{Q}[X]$ irreduzibel.

- Sei nun α eine Nullstelle von f in einem Erweiterungskörper von $\mathbb{Q}$. $\xRightarrow{\alpha \notin \mathbb{Z}} \alpha \neq 0 \text{ und } \alpha \neq 1$.

Es ist

$$f(-\alpha) = (-\alpha)^4 + 6(-\alpha)^2 + 1 = \alpha^4 + 6\alpha^2 + 1 = f(\alpha) = 0$$

$$\Rightarrow -\alpha \text{ ist Nullstelle und } -\alpha \neq \alpha$$

Außerdem:

$$\begin{aligned} \alpha^4 \cdot f\left(\frac{1}{\alpha}\right) &= \alpha^4 \left(\frac{1}{\alpha^4} + 6 \cdot \frac{1}{\alpha^2} + 1 \right) = 1 + 6\alpha^2 + \alpha^4 \\ &= f(\alpha) = 0 \end{aligned}$$

$$\xRightarrow{\alpha \neq 0} f\left(\frac{1}{\alpha}\right) = 0 \quad \text{d.h. wg. } \alpha \neq 1 \text{ ist } \frac{1}{\alpha} \text{ weitere Nullstelle.}$$

$$\xRightarrow{\text{wie oben}} -\frac{1}{\alpha} \text{ ist ebenfalls Nullstelle}$$

$$\Rightarrow \left\{ \alpha, -\alpha, \frac{1}{\alpha}, -\frac{1}{\alpha} \right\} \text{ sind alle Nullstellen von } f.$$

- Die Aussage ergibt sich mit dem Verfahren von Kronecker.
Ausführlich:

f irreduzibel $\Rightarrow (f)$ maximales Ideal

$\Rightarrow \mathbb{Q}[X]/(f)$ ist ein Körper

Haben Körperhomomorphismus (stets injektiv also Einbettung)
als Komposition

$$\mathbb{Q} \hookrightarrow \mathbb{Q}[X] \xrightarrow{\pi} \mathbb{Q}[X]/(f)$$

d.h. wir können $\mathbb{Q}[X]/(f)$ als Erweiterungskörper von $\mathbb{Q}$
auffassen. Setze $\alpha := \pi(X) = X + (f)$.

$$\Rightarrow \mathbb{Q}[X]/(f) = \mathbb{Q}(\alpha) \quad (\text{Adjunktion in } \mathbb{Q}[X]/(f) !)$$

Außerdem ist α eine Nullstelle von f , denn

$$\begin{aligned} f(\alpha) &= f(\pi(X)) = \pi(X)^4 + 6\pi(X)^2 + 1 \\ &= \pi(X^4 + 6X^2 + 1) \\ &= \pi(f) = f + (f) = 0 \end{aligned}$$

$$\text{Wegen } \mathbb{Q}(\alpha, -\alpha, \frac{1}{2}, -\frac{1}{2}) = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/(f)$$

ist also $\mathbb{Q}[X]/(f)$ Zerfällungskörper von f .

