

Algebra II, SoSe 2012 - Lösung Blatt 2

2.1. Vorüberlegung:

Beim Durchführen des Euklidischen Algorithmus dürfen wir Polynome vor einer Division mit Rest mit Einheiten multiplizieren.

Denn: $f, g \in K[X]$, $c \in K^*$. Dann

$$\bullet \quad c \cdot f = q \cdot g + r \quad \Rightarrow \quad f = \left(\frac{1}{c} \cdot q\right) \cdot g + \frac{1}{c} \cdot r$$

$\Rightarrow$ Rest unterscheidet sich nur um Einheit

$$\bullet \quad f = q \cdot (c \cdot g) + r \quad \Rightarrow \quad f = (q \cdot c) \cdot g + r$$

$\Rightarrow$ Rest gleich.

Also: Ist $z_0, z_1, \dots, z_n$ die Folge aus dem Euklidischen Algorithmus mit $z_n = 0$, so ergibt sich mit Multiplikation mit Einheiten eine Folge $c_0 z_0, c_1 z_1, \dots, c_n z_n$ mit c_i Einheit. $z_n = 0 \Rightarrow c_n z_n = 0$ (Folge bricht an der selben Stelle ab) und $\text{ggT}(z_0, z_1) = z_{n-1} \stackrel{\text{ggT bis auf Einheit!}}{=} c_{n-1} z_{n-1}$.

Damit zur Aufgabe:

$$(i) \quad f(X) = X^5 + 6X^3 + 3X + 4$$

$$f'(X) = 5X^4 + 18X^2 + 3.$$

$$\text{Wähle} \quad z_0 = 5 \cdot f = 5X^5 + 30X^3 + 15X + 20$$

$$z_1 = f' = 5X^4 + 18X^2 + 3.$$

$$(5X^5 + 30X^3 + 15X + 20) : (5X^4 + 18X^2 + 3) = X$$

$$\underline{5X^5 + 18X^3 + 3X}$$

$$12X^3 + 12X + 20$$

$$\Rightarrow z_2 = 3X^3 + 3X + 5 \quad \left(\cdot \frac{1}{4} \right)$$

Berechnen $3 \cdot z_1 : z_2$

$$(15X^4 + 54X^2 + 9) : (3X^3 + 3X + 5) = 5X$$

$$\underline{15X^4 + 15X^2 + 25X}$$

$$39X^2 - 25X + 9$$

$$\Rightarrow z_3 = 39X^2 - 25X + 9$$

Berechnen $13 \cdot z_2 : z_3$

$$(39X^3 + 39X + 65) : (39X^2 - 25X + 9) = X + \frac{25}{39}$$

$$\underline{39X^3 - 25X^2 + 9X}$$

$$25X^2 + 30X + 65$$

$$\underline{25X^2 - \frac{625}{39}X + \frac{75}{13}}$$

$$\frac{1795}{39}X + \frac{770}{13}$$

$$\xrightarrow{\cdot 39} 1795X + 2310$$

$$\xrightarrow{\cdot \frac{1}{5}} 359X + 462$$

$$\Rightarrow z_4 = 359X + 462$$

Untersuche $z_3 : z_4$:

$$(39X^2 - 25X + 9) : (359X + 462)$$

Rest ist nicht 0, denn sonst:

$$z_3 = q \cdot z_4 \quad \text{d.h. } z_4 \mid z_3 \quad \text{also auch mod 2}$$

$$\left(\text{in } \mathbb{Z}/2\mathbb{Z} \right) : \quad X \mid X^2 + X + 1 \quad \nmid$$

Also ist der Rest z_5 bei der Division $z_3 : z_4$ nicht 0
und $\deg z_5 < \deg z_4 = 1 \Rightarrow \deg z_5 = 0$ also $z_5 \in K^*$.

$$\stackrel{\text{insb.}}{\Rightarrow} z_6 = 0, \quad \text{d.h. } \text{ggT}(f, f') = z_5 \in K^*$$

$$\Rightarrow \text{ggT}(f, f') = 1$$

$$\stackrel{\text{VL}}{\Rightarrow} f \text{ hat keine mehrfachen Nullstellen.}$$

(ii) Völlig analog, daher weniger ausführlich:

$$f(X) = X^4 - 5X^3 + 6X^2 + 4X - 8$$

$$f'(X) = 4X^3 - 15X^2 + 12X + 4$$

$$(4X^4 - 20X^3 + 24X^2 + 16X - 32) : (4X^3 - 15X^2 + 12X + 4) = X - \frac{5}{4}$$

$$\underline{4X^4 - 15X^3 + 12X^2 + 4X}$$

$$-5X^3 + 12X^2 + 12X - 32$$

$$\underline{-5X^3 + \frac{75}{4}X^2 - 15X - 5}$$

$$-\frac{27}{4}X^2 + 27X - 27 \quad \stackrel{-4}{\cdot \frac{1}{27}} \quad X^2 - 4X + 4$$

$$(4X^3 - 15X^2 + 12X + 4) : (X^2 - 4X + 4) = 4X + 1$$

$$\underline{4X^3 - 16X^2 + 16X}$$

$$X^2 - 4X + 4$$

$$\underline{X^2 - 4X + 4}$$

0

$$\Rightarrow \text{ggT}(f, f') = (X-2)^2 \quad (= X^2 - 4X + 4)$$

$\Rightarrow 2$ ist mehrfache Nullstelle.

$$(iii) \quad f(X) = X^5 + 5X + 5$$

Eisenstein mit $p=5 \Rightarrow f \in \mathbb{Z}[X]$ irreduzibel.

$f_{\text{prim}} \Rightarrow f \in \mathbb{Q}[X]$ irreduzibel

Da $\text{char}(\mathbb{Q}) = 0$ kann f daher nach VL keine mehrfachen Nullstellen besitzen. ■

2.2. (i) Es ist

$$K(X^p, Y^p) = \text{Quot}(K[X^p, Y^p]).$$

X^p und Y^p sind in $K[X^p, Y^p]$ offenbar Primelemente

$$\stackrel{\text{Eisenstein}}{\Rightarrow} Z^p - Y^p \in K[X^p, Y^p][Z] \text{ irreduzibel}$$

$$\stackrel{\substack{\text{primitiv,} \\ \text{Gau\ss}}}{\Rightarrow} Z^p - Y^p \in K(X^p, Y^p)[Z] \text{ irreduzibel, also} \\ \text{Minimalpolynom von } Y \text{ \u00fcber } K(X^p, Y^p).$$

Wegen $K(X^p, Y^p)(Y) = K(X^p, Y)$ folgt:

$$[K(X^p, Y) : K(X^p, Y^p)] = p \quad (\text{Grad v. } Z^p - Y^p).$$

Au\u00dferdem ist offenbar X^p Primelement in $K[X^p, Y]$, d.h.
mit der gleichen Argumentation ist

$$Z^p - X^p \in K(X^p, Y)[Z]$$

Minimalpolynom von X . Wegen $K(X^p, Y)(X) = K(X, Y) = L$ folgt

$$[K(X, Y) : K(X^p, Y)] = p$$

Also:

$$[L : E] = [K(X, Y) : K(X^p, Y)] \cdot [K(X^p, Y) : K(X^p, Y^p)]$$

$$= p \cdot p$$

$$= p^2$$

(ii) Vorüberlegung:

Charakteristik von K ist $p > 0$.

$\Rightarrow$ Charakteristik von $K[X, Y]$ ist wegen $K \subset K[X, Y]$ ebenfalls $p > 0$.

$$\stackrel{\text{Frobenius}}{\Rightarrow} (f+g)^p = f^p + g^p \quad \forall f, g \in K[X, Y] \quad (*)$$

Sei nun $f \in K[X, Y]$. $\Rightarrow f(X, Y) = \sum a_{\mu\nu} X^\mu Y^\nu$

für gewisse $a_{\mu\nu} \in K$. Dann berechnen wir:

$$\begin{aligned} f(X, Y)^p &= \left(\sum a_{\mu\nu} X^\mu Y^\nu \right)^p \stackrel{(*)}{=} \sum (a_{\mu\nu} X^\mu Y^\nu)^p \\ &= \sum a_{\mu\nu}^p (X^p)^\mu (Y^p)^\nu \end{aligned}$$

$$\Rightarrow f(X, Y)^p \in K[X^p, Y^p]. \quad (**)$$

Damit zur Aufgabe:

Es ist $L = K(X, Y) = \text{Quot}(K[X, Y])$ und

$$E = K(X^p, Y^p) = \text{Quot}(K[X^p, Y^p]).$$

Ist $\alpha \in L$ beliebig, dann gilt $\alpha = \frac{f(X, Y)}{g(X, Y)}$ für gewisse

$f, g \in K[X, Y]$.

$$\Rightarrow \alpha^p = \frac{f(X, Y)^p}{g(X, Y)^p}. \quad \text{Da nach } (**) \quad f(X, Y)^p, g(X, Y)^p \in K[X^p, Y^p]$$

gilt, folgt: $\alpha^p \in \text{Quot}(K[X^p, Y^p]) = K(X^p, Y^p) = E$.

(iii) Sei $\alpha \in L$.

$\Rightarrow \alpha$ ist Nullstelle des Polynoms $Z^p - \alpha^p \in L[Z]$.

Nach (ii) ist $\alpha^p \in E$, d.h. $Z^p - \alpha^p \in E[Z]$.

$\Rightarrow$ Das Minimalpolynom von α über E ist ein Teiler von $Z^p - \alpha^p$ und hat daher einen Grad $\leq p$.

$\nearrow \alpha \in L$ primitives Element von L/E , d.h.

$$L = E(\alpha).$$

Sei $f \in E[Z]$ das Minimalpolynom von α .

$$\stackrel{\text{so}}{\Rightarrow} \deg f \leq p$$

$$\stackrel{\text{VL}}{\Rightarrow} [L:E] = [E(\alpha):E] = \deg f \leq p.$$

Nach Teil (i) gilt aber $[L:E] = p^2$ $\nmid$

Also besitzt L/E kein primitives Element. ◻

2.3. (i) Sei $\bar{K}$ ein algebraischer Abschluss von K .

$\Rightarrow K(\alpha) \subset \bar{K}$ und natürlich $K(\alpha+1) = K(\alpha)$.

Da f normiert und irreduzibel mit $f(\alpha) = 0$ ist, ist f das Minimalpolynom von α .

$f(\alpha+1) = 0$
 $\Rightarrow \exists$ Körperhomomorphismus $\tau: K(\alpha) \rightarrow K(\alpha)$ mit
 $\tau(\alpha) = \alpha + 1$ (und $\tau|_K = \text{id}_K$, d.h. Fortsetzung von id_K).

Da $K(\alpha) \subset \bar{K}$ algebraische Erweiterung ist, existiert eine Fortsetzung $\sigma: \bar{K} \rightarrow \bar{K}$ von τ , welche ein Isomorphismus von $\bar{K}$ über K ist (beachte: $\bar{K}$ algebraisch abgeschlossen!).

Es gilt $\sigma(\alpha) = \tau(\alpha) = \alpha + 1$.

Mit σ ist $\forall n \in \mathbb{N}$ auch $\sigma^n \in \text{Aut}_K(\bar{K})$, und es ist

$$\sigma^n(\alpha) = \alpha + \underbrace{1 + \dots + 1}_{n\text{-mal}}.$$

$\Rightarrow \forall n \in \mathbb{N}$ ist $\sigma^n(\alpha) = \alpha + \underbrace{1 + \dots + 1}_n$ eine Nullstelle von f .

Da f nur endlich viele Nullstellen besitzt muss also ein $m \in \mathbb{N}$ existieren mit $\underbrace{1 + \dots + 1}_{m\text{-mal}} = 0$.

$\Rightarrow K$ hat Charakteristik > 0 .

(ii) Nach Voraussetzung ist $X^p - X - (\alpha^p - \alpha) \in K[X]$ und
 Offenbar ist α eine Nullstelle. Es ist:

$$\begin{aligned}
 & (\alpha - c)^p - (\alpha - c) - (\alpha^p - \alpha) \\
 & \stackrel{\text{Frobenius, } \chi(K)=p}{=} \alpha^p - \alpha - (\alpha^p - \alpha) - c^p + c \\
 & = c - c^p \quad (*)
 \end{aligned}$$

Da $\chi(K)=p$ gilt, sind $0, 1, 2, \dots, p-1 \in K$ p verschiedene
 Elemente (hier ist $j = \underbrace{1 + \dots + 1}_{j\text{-mal}}$). Da

$$\begin{aligned}
 j - j^p &= \underbrace{(1 + \dots + 1)}_j - \underbrace{(1 + \dots + 1)^p}_j \\
 & \stackrel{\text{Frobenius}}{=} \underbrace{(1 + \dots + 1)}_j - \underbrace{(1^p + \dots + 1^p)}_j = 0
 \end{aligned}$$

gilt, sind nach (*)

$$\alpha, \alpha + 1, \dots, \alpha + p - 1$$

p verschiedene Nullstellen von $X^p - X - (\alpha^p - \alpha)$ und damit
 alle Nullstellen.

Da f das Minimalpolynom von α ist, folgt

$$f \mid X^p - X - (\alpha^p - \alpha).$$

Da aber f nach Teil (i) ebenfalls die Nullstellen

$$\alpha, \alpha+1, \dots, \alpha+p-1$$

besitzt, muss $f(X) = X^p - X - (\alpha^p - \alpha)$ gelten.

(iii) Da f nach (ii) genau die p verschiedenen Nullstellen $\alpha, \alpha+1, \dots, \alpha+p-1$ besitzt, ist f separabel und damit (wegen $f(\alpha) = 0$) auch die Erweiterung $K(\alpha)/K$.

Da mit $\alpha \in K(\alpha)$ auch $\alpha+1, \dots, \alpha+p-1 \in K(\alpha)$ gilt, ist $K(\alpha)$ der Zerfällungskörper von f über K .

$\Rightarrow K(\alpha)/K$ ist auch eine normale Erweiterung.



2.4. • Bestimme E: Betrachte die Polynome

$$f_1(X) = X^2 - 3 \quad \text{und} \quad f_2(X) = X^3 - 3.$$

Mit Eisenstein ($p=3$) und Gauß folgt:

$$f_1, f_2 \in \mathbb{Q}[X] \quad \text{irreduzibel}$$

$\Rightarrow \sqrt{3}$ hat den Grad 2 über $\mathbb{Q}$ (f_1 ist Minimalpolynom)
und $\sqrt[3]{3}$ hat den Grad 3 über $\mathbb{Q}$ (f_2 ist Minimalpolynom)

Insbesondere folgt: $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{3})$ und $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt{3})$ (*)

(denn angenommen $\sqrt{3} \in \mathbb{Q}(\sqrt[3]{3}) \Rightarrow \mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt[3]{3})$.

Wegen $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ prim folgt $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt[3]{3})$,

denn $\mathbb{Q} = \mathbb{Q}(\sqrt{3})$ ist absurd, $\Rightarrow \mathbb{Q} \subset \mathbb{Q}(\sqrt{3})$

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

Die andere Aussage folgt völlig analog.)

Zerfallungskörper von f_1 ist $\mathbb{Q}(\sqrt{3})$.

Zerfallungskörper von f_2 :

$$\text{Sei } \zeta = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \quad \Rightarrow \quad \zeta^3 = 1 \quad \text{und auch}$$

$$(\zeta^2)^3 = (\zeta^3)^2 = 1 \quad \text{mit} \quad \zeta^2 \neq \zeta$$

$\Rightarrow f_2$ besitzt die Nullstellen $\sqrt[3]{3}, \zeta\sqrt[3]{3}, \zeta^2\sqrt[3]{3}$.

$\Rightarrow$ Zerfallungskörper von f_2 über $\mathbb{Q}$ ist

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

$\Rightarrow E := \mathbb{Q}(\sqrt[3]{3}, \sqrt{3}, \zeta)$ ist als Zerfällungskörper von $\{f_1, f_2\}$ normal über $\mathbb{Q}$ und offenbar ist

$$F = \mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) \subset E.$$

E ist der minimale normale Erweiterungskörper von $\mathbb{Q}(\sqrt[3]{3}, \sqrt{3})$ denn ist M ein anderer, dann liegen wegen $\sqrt[3]{3} \in M$ alle Nullstellen von f_2 in M und damit insbesondere auch

$$\zeta = \frac{1}{3} \cdot \underbrace{\zeta\sqrt[3]{3}}_{\in M} \cdot \underbrace{(\sqrt[3]{3})^2}_{\in M} \in M,$$

d.h. $E \subset M$. Es ist nun

$$E = \mathbb{Q}(\sqrt[3]{3}, \sqrt{3}, -\frac{1}{2} + i\frac{\sqrt{3}}{2})$$

$$= \mathbb{Q}(\sqrt[3]{3}, \sqrt{3}, i\sqrt{3})$$

$$= \mathbb{Q}(\sqrt[3]{3}, \sqrt{3}, i) \quad (\text{Kann wegen (*) nicht weiter vereinfacht werden})$$

- Berechne primitives Element von $E/\mathbb{Q}$ mit Tschirnhausen-Algorithmus:

Zunächst: Primitives Element für $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$.

Betrachte:

$$\sqrt{3} - \gamma_1 i = \sqrt{3} + \gamma_1 i \Rightarrow \gamma_1 = 0$$

$$-\sqrt{3} - \gamma_2 i = \sqrt{3} + \gamma_2 i \Rightarrow \gamma_2 = -\sqrt{3} \cdot i$$

Tschirnhausen $\Rightarrow \sqrt[3]{3} + yi$ für $y \notin \{y_1, y_2\}$ und $y \in \mathbb{Q}$
ist primitives Element.

Wähle $y=1 \Rightarrow \mathbb{Q}(\sqrt[3]{3}, i) = \mathbb{Q}(\sqrt[3]{3} + i)$

Bestimmen nun primitives Element von

$$\mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{3}, i) = \mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{3} + i)$$

Bestimmen „auszuschließende Elemente“:

$$\sqrt[3]{3} + x_1(\sqrt[3]{3} - i) = \sqrt[3]{3} + x_1(\sqrt[3]{3} + i)$$

$$\sqrt[3]{3} + x_2(-\sqrt[3]{3} - i) = \sqrt[3]{3} + x_2(\sqrt[3]{3} + i)$$

$$\sqrt[3]{3} + x_3(-\sqrt[3]{3} + i) = \sqrt[3]{3} + x_3(\sqrt[3]{3} + i)$$

$$\zeta \sqrt[3]{3} + x_4(\sqrt[3]{3} - i) = \sqrt[3]{3} + x_4(\sqrt[3]{3} + i)$$

$$\zeta \sqrt[3]{3} + x_5(-\sqrt[3]{3} - i) = \sqrt[3]{3} + x_5(\sqrt[3]{3} + i)$$

$$\zeta \sqrt[3]{3} + x_6(-\sqrt[3]{3} + i) = \sqrt[3]{3} + x_6(\sqrt[3]{3} + i)$$

$$\zeta^2 \sqrt[3]{3} + x_7(\sqrt[3]{3} - i) = \sqrt[3]{3} + x_7(\sqrt[3]{3} + i)$$

$$\zeta^2 \sqrt[3]{3} + x_8(-\sqrt[3]{3} - i) = \sqrt[3]{3} + x_8(\sqrt[3]{3} + i)$$

$$\zeta^2 \sqrt[3]{3} + x_9(-\sqrt[3]{3} + i) = \sqrt[3]{3} + x_9(\sqrt[3]{3} + i)$$

(beachte: Minimalpolynom von $\sqrt[3]{3} + i$ über $\mathbb{Q}$ ist $X^4 - 4X^2 + 16$
denn wir wissen, dass der Grad von $\sqrt[3]{3} + i$ über $\mathbb{Q}$ 4 ist.

$$\Rightarrow \sqrt[3]{3} - i = \overline{(\sqrt[3]{3} + i)} \text{ weitere Nullstelle}$$

und da Polynom gerade auch $-\sqrt[3]{3} - i$ und $-\sqrt[3]{3} + i = \overline{(-\sqrt[3]{3} - i)}$.

Wähle $x=1$, dann ist $x \notin \{x_1, \dots, x_g\}$.

$$\Rightarrow \sqrt[3]{3} + 1(\sqrt{3} + i) = \sqrt[3]{3} + \sqrt{3} + i$$

ist ein primitives Element von $\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}, i) / \mathbb{Q}$.