Übungsblatt 9

Aufgabe 1. Berechnen Sie die Grade der Zerfällungskörper über $\mathbb{Q}$ der folgenden Polynome in $\mathbb{Q}[X]$:

(1) $X^4 - 2$,

(2) $X^4 + 2$,

(3) $X^4 + X^2 + 1$,

(4) $X^6 - 4$.

Bitte begründen Sie Ihre Angaben.

Sei o.E. $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, d.h. wir betten die Zerfällungskörper der obigen Polynome in $\mathbb{C}$ ein.

(1) Es gilt

$$X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2}) = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2})$$

und damit ist der Zerfällungskörper $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$. Im euklidischen Ring $\mathbb{Z}[i]$ (siehe Blatt 5 Aufgabe 1) ist $p = 1 + i$, wegen $N(1+i) = 2$ prim in $\mathbb{Z}$, ein Primelement. Das Eisenstein Kriterium liefert die Irreduzibilität von $X^4 - 2$ in $\mathbb{Z}[i][X]$ und somit auch die Irreduzibilität in $Q(\mathbb{Z}[i])[X] = \mathbb{Q}(i)[X]$. Somit ist das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(i)$ gerade $X^4 - 2$ und wir erhalten

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 4 \cdot 2 = 8.$$

(2) Es gilt

$$X^4 + 2 = (X^2 - i\sqrt{2})(X^2 + i\sqrt{2}) = (X - \sqrt{i\sqrt{2}})(X + \sqrt{i\sqrt{2}})(X - i\sqrt{i\sqrt{2}})(X + i\sqrt{i\sqrt{2}}).$$

Mit

$$\sqrt{i} = \exp\left(\frac{\pi}{2}i\right)^{\frac{1}{2}} = \exp\left(\frac{\pi}{4}i\right) = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2}(1+i)$$

gilt

$$\sqrt{i\sqrt{2}} = \sqrt{i}\sqrt[4]{2} = \frac{\sqrt{2}}{2}(1+i)\sqrt[4]{2} = 2^{-\frac{1}{4}}(1+i).$$

Somit erhalten wir

$$X^4 + 2 = \left(X - 2^{-\frac{1}{4}}(1+i)\right)\left(X + 2^{-\frac{1}{4}}(1+i)\right)\left(X - 2^{-\frac{1}{4}}(i-1)\right)\left(X + 2^{-\frac{1}{4}}(i-1)\right).$$

Der Zerfällungskörper ist $\mathbb{Q}\left(2^{-\frac{1}{4}}(1+i), 2^{-\frac{1}{4}}(1-i)\right) = \mathbb{Q}(\sqrt[4]{2}, i)$ und es gilt wie in (1)

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8.$$

(3) Mit der Substitution $z = X^2$ erhalten wir

$$X^4 + X^2 + 1 = z^2 + z + 1.$$

Die Nullstellen von $z^2 + z + 1$ sind die primitiven dritten Einheitswurzeln

$$\zeta_3 := -\frac{1}{2} + \frac{\sqrt{3}}{2}i = \exp\left(\frac{2\pi}{3}i\right) \text{ und } \bar{\zeta_3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i = \exp\left(\frac{2\cdot 2\pi}{3}i\right) = \zeta_3^2.$$

Die Nullstellen von $X^4 + X^2 + 1$ lauten schließlich

$$\pm\sqrt{\zeta_3} = \pm\exp\left(\frac{2\pi}{6}i\right) \text{ und } \pm\sqrt{\bar{\zeta}_3} = \pm\exp\left(\frac{2\pi}{3}i\right) = \pm\zeta_3.$$

Somit gilt mit der primitiven sechsten Einheitswurzel $\zeta_6 := \sqrt{\zeta_3} = \exp\left(\frac{2\pi}{6}i\right)$

$$X^4 + X^2 + 1 = (X - \zeta_6)(X + \zeta_6)(X - \zeta_3)(X + \zeta_3).$$

Der Zerfällungskörper ist $\mathbb{Q}(\zeta_3, \zeta_6) = \mathbb{Q}(\zeta_6)$. Das Minimalpolynom von ζ_6 über $\mathbb{Q}$ ist $X^2 - X + 1$. Somit gilt

$$[\mathbb{Q}(\zeta_6) : \mathbb{Q}] = 2.$$

(4) Es gilt

$$\begin{aligned} X^6 - 4 &= (X^3 - 2)(X^3 + 2) \\ &= (X - \sqrt[3]{2})(X - \zeta_3\sqrt[3]{2})(X - \zeta_3^2\sqrt[3]{2})\left(X - (-\sqrt[3]{2})\right)\left(X - (-\zeta_3\sqrt[3]{2})\right)\left(X - (-\zeta_3^2\sqrt[3]{2})\right), \end{aligned}$$

wobei $\zeta_3 := \exp\left(\frac{2\pi}{3}i\right)$ eine dritte primitive Einheitswurzel ist. Das Polynom zerfällt also über $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Das Minimalpolynom von ζ_3 über $\mathbb{Q}(\sqrt[3]{2})$ ist $X^2 + X + 1$, denn $\zeta_3 \notin \mathbb{R} \supseteq \mathbb{Q}(\sqrt[3]{2})$. Somit gilt

$$[\mathbb{Q}(\zeta_3, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_3, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Bemerkung. *Für die Berechnung von Nullstellen reeller Polynome ist die folgende Überlegung hilfreich. Sei $f \in \mathbb{R}[X]$ und $v \in \mathbb{C}$ mit $f(v) = 0$, so ist auch das komplex konjugierte Element $\bar{v}$ eine Nullstelle von f. Das heißt, dass komplexe Nullstellen immer paarweise auftreten, sofern f ein reelles Polynom ist.*

Im Beweis der Aufgaben 2 und 3 wird das folgende Lemma verwendet.

Lemma (Freshman's dream)**.** *Sei R ein Integritätsring der Charakterstik p, wobei p eine Primzahl ist. So gilt für alle $a, b \in R$ und $r \in \mathbb{N}_0$*

$$(a + b)^{p^r} = a^{p^r} + b^{p^r}.$$

Beweis. Die Aussage lässt sich einfach mittel vollständiger Induktion auf den Fall $r = 1$ reduzieren. Es reicht zu zeigen, dass $p \mid \binom{p}{v}$ für $v = 1, 2, \ldots, p-1$ gilt. Betrachte hierfür $\binom{p}{v} = \frac{p!}{(p-v)!\cdot v!}$. Im Zähler tritt der Primfaktor p auf, wobei er wegen $p - v, v < p$ für $1 \le v \le p-1$ im Nenner nicht auftritt. Wir erhalten also $p \mid \binom{p}{v}$ für $1 \le v \le p-1$ und somit wegen $\operatorname{char}(R) = p$

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p.$$

□

Aufgabe 2. Seien $L|K$ eine Körpererweiterung in Charakterstik $p > 0$ und $a \in L$ ein über K algebraisches Element. Zeigen Sie: $a \in L$ ist genau dann seperabel über K, wenn $K(a) = K(a^p)$ gilt.

Beweis. Da $\operatorname{char}(K) = p > 0$ ist, gilt nach dem obigen Lemma $f(X) = (X-a)^p = X^p - a^p \in K(a^p)[X]$ und somit $f(a) = a^p - a^p = 0$. Das Minimalpolynom $m^{K(a^p)}$ von a über $K(a^p)$ ist ein Teiler von f und somit gilt $m^{K(a^p)}(X) = (X-a)^m$ für $1 \le m \le p$. Offensichtlich teilt $m^{K(a^p)}$ das Minimalpolynom m^K von a über K in $K(a^p)[X]$. Die Separabilität von a über K ist nach Definition gleichbedeutent dazu, dass in der Linearfaktorzerlegung von m^K in $\overline{K}[X]$ der Faktor $X - a$ nur einmal vorkommt, d.h. a ist eine einfache Nullstelle von m^k. Da $m^{K(a^p)}$ ein Teiler von m^K ist, ist letzteres äquivalent zu $m = 1$ und dies ist äquivalent zu $[K(a^p) : K(a)] = \deg(m^{K(a^p)}) = m = 1$. □

Aufgabe 3. Seien K ein Körper positiver Charakteristik p, $a \in K$ und

$$f = X^p - X - a \in K[X].$$

Sei ferner L ein Erweiterungskörper von K, der eine Nullstelle von f enthält. Zeigen Sie, dass f über L vollständig in Linearfaktoren zerfällt. Schließen Sie, dass f über K separabel ist.

Beweis. Da $\mathrm{char}(K) = p > 0$ gilt, ist $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ der Primkörper von K. Betrachte für eine Nullstelle z von f in einer Erweiterung L von K

$$z, z+1, z+2, \ldots, z+p-1,$$

wobei $0, 1, 2, \ldots, p-1 \in \mathbb{F}_p$. Die obigen Elemente sind Nullstellen von f, denn für $z+v$ mit $v \in \mathbb{F}_p$ gilt nach 'Fermats Kleinem Satz' und dem obigen Lemma

$$f(z+v) = (z+v)^p - (z+v) + a = z^p + v^p - z - v + a = z^p + v - z - v + a = z^p - z + a = f(z) = 0.$$

Da die Nullstellen paarweise verschieden sind und $\deg(f) = p$ ist, gilt

$$f(X) = \prod_{v \in M} (X - v) = \prod_{v \in \mathbb{F}_p} (X - (z+v))$$

und somit ist f separabel. □