Übungsblatt 8

Aufgabe 1. Seine K ein Körper, $f \in K[X]$ mit $\deg(f) > 0$ und L ein Zerfällungskörper von f. Zeigen Sie, dass

$$[L : K] \leq \deg(f)!$$

gilt.

Beweis. Sei $a \neq 0$ der Leitkoeffizient von f, so ist der Zerfällungskörper von $a^{-1}f$ auch L und somit ist o.B.d.A. f normiert. Wir beweisen die Behauptung mittels vollständiger Induktion nach $n := \deg(f)$. Sei $n = 1$, so ist bereits K der Zerfällungskörper von f und somit gilt $K = L$ und insbesondere $[L : K] = 1$. Sei nun $n > 1$. Ist f irreduzibel über K mit Nullstelle $a \in L$, so gilt $[K(\alpha) : K] = n$ und $f(X) = (X - a)g(X)$ mit $g \in K(a)[X]$ und $\deg(g) = n - 1$. Da auch L der Zerfällungskörper von g über $K(a)$ ist, gilt nach der Induktionsvoraussetzung

$$[L : K(a)] \leq \deg(g)! = (n-1)!$$

und somit

$$[L : K] = [K : K(a)] \cdot [K(a) : K] \leq n(n-1)! = n!.$$

Ist f reduzibel über K und seien $f_1, f_2 \in K[X] \setminus K$ mit $f = f_1 f_2$, $n_1 := \deg(f_1), n_2 := \deg(f_2) \geq 1$ und $n = n_1 + n_2$. Sei L_1 der Zerfällungskörper von f_1 über K. Nach der Induktionsvoraussetzung gilt

$$[L_1 : K] \leq n_1!.$$

Da L der Zerfällungskörper von f_2 über L_1 ist, gilt nach der Induktionsvoraussetzung

$$[L : L_1] \leq n_2!.$$

Wir erhalten somit

$$[L : K] = [L : L_1] \cdot [L_1 : K] \leq n_1! n_2! \leq (n_1 + n_2)!.$$

□

Aufgabe 2. Zeigen Sie, dass das Polynom

$$f(X) = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$$

irreduzibel ist.

Beweis. Zunächst zeigen wir, dass f keine Nullstellen in $\mathbb{Q}$ besitzt. Sei $\frac{a}{b} \in \mathbb{Q}$ (vollständig gekürzt) eine Nullstelle von f, so gilt nach Blatt 6 Aufgabe 2, dass $a|1$ und $b|1$ und somit $\frac{a}{b} = \pm 1$. Allerdings sind ± 1 keine Nullstellen von f, somit besitzt f keine Nullstellen in $\mathbb{Q}$. Nun reicht es zu zeigen, dass f von keinem (normierten) Polynom von Grad 2 geteilt wird. Eine einfache Polynomdivision liefert

$$(X^4 - 10X^2 + 1) = (X^2 + aX + b) \cdot (X^2 - aX - 10 - b + a^2) + \left(a(10 + 2b - a^2)X + 1 - b(-10 - b + a^2)\right).$$

Im Folgenden zeigen wir, dass es keine $a, b \in \mathbb{Q}$ gibt, sodass $X^2 + aX + b$ das Polynom f teilt. Damit es f teilt, muss nämlich gelten

$$a(10 + 2b - a^2) = 0 \text{ und } b(-10 - b + a^2) = 1.$$

Die erste Bedingung liefert uns $a = 0$ oder $10 + 2b - a^2 = 0$. Ist $a = 0$, so gilt nach der zweiten Bedingung $b = -5 \pm \sqrt{25 - 1} = -5 \pm 2\sqrt{6} \notin \mathbb{Q}$. Also gilt $10 + 2b - a^2 = 0$, was äquivalent ist zu $b(-10 - b + a^2) = b^2$. Setzt man letzteres in die zweite Bedingung ein, erhält man $1 = b(-10 - b + a^2) = b^2$, d.h. $b = \pm 1$. Somit erhalten wir durch die zweite Bedingung $a^2 \in \{12, -8\}$, d.h. $a \notin \mathbb{Q}$. Also gilt insgesamt, dass f weder von einem Polynom von Grad 1 noch 2 in $\mathbb{Q}[X]$ geteilt wird und ist somit irreduzibel. □

Aufgabe 3. Betrachten Sie die Erweiterung $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ von $\mathbb{Q}$. Bestimmen Sie den Grad $[L : \mathbb{Q}]$, sowie das Minimalpolynom des Elements

$$\alpha := \sqrt{2} + \sqrt{3} \in L.$$

Schließen Sie, dass $L = \mathbb{Q}$. Bestimmen Sie α^{-1} explizit in Termen von $\sqrt{2}$ und $\sqrt{3}$.

Beweis. Da das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ gerade $X^2 - 2$ ist, gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}(\sqrt{2})$ ist $X^2 - 3$, da $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Letzteres sieht man wie folgt ein. Angenommen $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, so existieren wegen $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ gerade $a, b \in \mathbb{Q}$ mit

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

Ist $a = 0$, so gilt $3 = 2b^2$, ein Widerspruch. Ist $b = 0$, so gilt $\sqrt{3} \in \mathbb{Q}$, ein Widerspruch. Also sind $a, b \neq 0$ und wir erhalten

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

und somit

$$\frac{3 - a^2 - 2b^2}{2ab} = \sqrt{2} \in \mathbb{Q},$$

ein Widerspruch.
Es gilt also $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3}))] = 2$ und damit

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

Das Minimalpolynom von $\alpha = \sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$ ist $f(X) = X^4 - 10X^2 + 1$, denn es gilt $f(\alpha) = 0$ und nach Aufgabe 2 ist es irreduzibel. Somit gilt

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$$

und

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

Also gilt

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

d.h. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$.
Aus $0 = f(\alpha) = \alpha^4 - 10\alpha^2 + 1$ folgt $1 = -\alpha^4 + 10\alpha^2 = \alpha(-\alpha^3 + 10\alpha)$, d.h.

$$\alpha^{-1} = -\alpha^3 + 10\alpha = -\sqrt{2} + \sqrt{3}.$$

□

Aufgabe 4. Seien p eine Primzahl, K ein Körper und $a \in K \setminus K^p$ ein Element in K, das keine p-te Potenz eines Elements in K ist. Zeigen Sie, dass

$$X^p - a \in K[X]$$

irreduzibel ist.

Beweis. Sei $V \subseteq \overline{K}$ die Nullstellenmenge von f in dem algebraischen Abschluss $\overline{K}$ von K, so gilt

$$X^p - a = \prod_{v \in V} (X - v)^{n_v}.$$

Angenommen f ist reduzibel, so existieren $g, h \in K[X] \setminus K$ mit $f = gh$, mit $V(g) \cup V(h) = V$ und $m_v, m'_v \in \mathbb{N}$, $m_v + m'_v = n_v$

$$g(X) = \prod_{v \in V(g)} (X - v)^{m_v} \text{ und } h(X) = \prod_{v \in V(h)} (X - v)^{m'_v}.$$

Mit $G \coloneqq \prod_{v\in V(g)} v^{m_v}$, $H \coloneqq \prod_{v\in V(h)} v^{m'_v}$, $v^p = a$ für alle $v \in V$ und $n \coloneqq \deg(g)$

$$G^p = \left(\prod_{v\in V(g)} v^{m_v}\right)^p = a^n \text{ und } H^p = \left(\prod_{v\in V(f)} v^{m'_v}\right)^p = a^{p-n}.$$

Da $p > n \geq 1$ und p eine Primzahl ist, gilt $\mathrm{ggT}(p,n) = 1$. Letzteres ist äquivalent zu der Existenz von $k, l \in \mathbb{Z}$ mit $kn + lp = 1$ (Lemma von Bézout).
Wir erhalten somit

$$a = a^{kn+pl} = (a^n)^k \cdot (a^n)^l \cdot (a^{p-n})^l = (G^p)^k \cdot (G^p)^l \cdot (H^p)^l = \left(G^{k+l}H^l\right)^p.$$

Da $g, h \in K[X]$ sind, gilt insbesondere

$$(-1)^n g(0) = (-1)^n \prod_{v\in V(g)} (0-v)^{m_v} = G \in K \text{ und } (-1)^{p-n} h(0) = (-1)^{p-n} \prod_{v\in V(h)} (0-v)^{m'_v} = H \in K.$$

Insgesamt erhalten wir also mit $a = \left(G^{k+l}H^l\right)^p$, dass $a \in K^p$ gilt, ein Widerspruch. $\square$