Universität Konstanz
Fachbereich Mathematik und Statistik
Wintersemester 2014/2015

Christoph Hanselka
Markus Schweighofer

Einführung in die Algebra, Übungsblatt 12, Lösungsvorschlag

Aufgabe 2. Sei K ein Körper und $a \in K(X) \setminus K$. Zeige

(a) Durch $\varphi(X) = a$ und $\varphi|_K = \mathrm{id}_K$ wird eine Körpereinbettung $\varphi\colon K(X) \to K(X)$ gegeben.

(b) Bestimme den Körpergrad $[K(X) : \varphi(K(X))]$.

Lösungsvorschlag. (a) Nach 2.3.14(b) ist jeder Körperhomomorphismus (also Ringhomomorphismus zwischen Körpern) automatisch injektiv und damit eine Körpereinbettung. Die Behauptung besagt also, dass es genau einen Ringhomomorphismus $\varphi\colon K(X) \to K(X)$ mit $\varphi|_K = \mathrm{id}_K$ und $\varphi(X) = a$ gibt. Nun gibt es nach 2.2.8 genau einen Ringhomomorphismus $\psi\colon K[X] \to K(X)$ mit $\psi|_K = \mathrm{id}_K$ und $\psi(X) = a$. Die Behauptung ist offensichtlich dazu äquivalent, dass dieses ψ genau eine Fortsetzung zu einem Ringhomomorphismus $\varphi\colon K(X) \to K(X)$ erlaubt. Wegen $K(X) = S^{-1}K[X]$ für die multiplikative Menge $S := K[X] \setminus \{0\}$, ist dies nach 2.3.7 dazu äquivalent, dass $\psi(S) \subseteq K(X)^\times$. Wegen $K(X)^\times = K(X) \setminus \{0\}$, ist dies äquivalent zur Injektivität von ψ. Dass ψ injektiv ist, heißt aber gerade, dass a nicht algebraisch über K ist.

Angenommen a wäre algebraisch über K, so wäre die ganze Körpererweiterung $K(a)|K$ nach §4.1 algebraisch und wegen der Transitivität der Algebraizität 4.1.17 auch X algebraisch über K, denn wir zeigen gleich, dass X algebraisch über $K(a)$ ist. Widerspruch!

Wir zeigen nun, dass X algebraisch über $K(a)$ ist. Schreibe $a = \frac{g}{h}$ mit $g, h \in K[X] \setminus \{0\}$. Schreibe weiter $g = \sum_{i=0}^d g_i X^i$ und $h = \sum_{i=0}^d h_i X^i$ mit $g_i, h_i \in K$ und $d := \max\{\deg g, \deg h\} > 0$. Wir setzen

$$f := g(Y) - h(Y)a \in K(a)[Y].$$

Dann ist $\deg f = d$: Es ist $g_d \neq 0$ oder $h_d \neq 0$ und der Koeffizient $g_d - ah_d$ von Y^d in f verschwindet wegen $a \notin K$ nicht. Insbesondere ist f nicht das Nullpolynom. Nun ist $f(X) = g - ha = 0$, also X algebraisch über $K(a)$.

(b) Wir zeigen, dass das eben definierte Polynom f sogar das Minimalpolynom von X über $K(a) = \varphi(K(X))$ ist, wenn wir g und h sogar teilerfremd wählen (was durch vollständiges Kürzen des Bruchs immer möglich ist, da $K[X]$ faktoriell ist). Damit erhalten wir dann $[K(X) : \varphi(K(X))] = \deg f = \max\{\deg g, \deg h\}$ mit 4.1.10. Da a nicht algebraisch über K ist, ist es algebraisch unabhängig über K. Wir können a also als Unbestimmte behandeln, das heißt $K[a]$ ist ein Polynomring und $K(a)$ ein

Körper von rationalen Funktionen über K. Betrachte nun wieder den Polynomring $K(a)[Y]$ über $K(a)$ in einer Unbestimmten Y und seinen Unterring $K[a, Y]$, welcher ein Polynomring in den zwei Unbestimmten a und Y ist (vergleiche 2.2.11).

Als Polynom in a über dem Körper $K(Y)$ ist f vom Grad 1, also irreduzibel. Außerdem ist f primitiv in $K[Y][a]$, da seine Koeffizienten $g(Y)$ und $h(Y)$ in $K[Y]$ teilerfremd sind. Nach dem Lemma von Gauß 2.5.9(c) ist f also auch irreduzibel in $K[Y][a]$. Also ist f ein irreduzibles Element in $K[Y][a] = K[Y, a] = K[a, Y] = K[a][Y]$. Da f als Polynom in Y über $K[a]$ den Grad $d > 0$ hat wie oben gesehen, ist f auch irreduzibel in $K(a)[Y]$ nach 2.5.9.(b), was nach 4.1.9 zu zeigen war.

Beachte, dass wir auch benutzt haben, dass Primelemente $\neq 0$ in faktoriellen Ringen dasselbe sind wie irreduzible Elemente (siehe 2.4.1) und dass Polynomringe über Körpern (hier in ein oder zwei Variablen) faktoriell sind (Satz von Gauß, 2.5.10).

Aufgabe 3.

(a) Sei $L|K$ eine Körpererweiterung mit $\operatorname{char} K \neq 2$. Zeige

$$[L : K] \leq 2 \iff \exists a \in K : L = K(\sqrt{a}).$$

Hinweis: Mache eine „quadratische Ergänzung".

(b) Sei $M \subseteq \mathbb{C}$ mit $\{0, 1\} \subseteq M$, $K := \mathbb{Q}(M \cup M^*)$ wie auf dem letzten Blatt und $a \in \mathbb{C}$. Zeige $a \in \,\bar{\curlywedge}\, M$ genau dann, wenn es $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\mathbb{C}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ gibt mit $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

Hinweis: Zeige, um leichter Induktion durchführen zu können, dass sogar $F_n^* = F_n$ gewählt werden kann.

(c) Zeige, dass das regelmäßige 7-Eck nicht aus $M = \{0, 1\}$ konstruierbar ist.

Hinweis: Bestimme den Grad des Minimalpolynoms von $e^{\frac{2\pi \mathring{\imath}}{7}}$ über $\mathbb{Q}$.

Lösungsvorschlag. (b) Sei $a \in \,\bar{\curlywedge}\, M$. Es gibt also $x_1, \ldots, x_m = a \in \mathbb{C}$ derart, dass

$$x_i \in (M \cup \{x_1, \ldots, x_{i-1}\})'$$

also jedes Element in dieser endlichen Folge durch einen Schritt aus seinen Vorgängern zusammen mit M konstruiert wurde. Nun adjungieren wir sukzessive x_i und x_i^* zu K hinzu. Das bedeutet wir setzen $F_0 := K$ und rekursiv $F_{2k-1} := F_{2k-2}(x_k)$ und $F_{2k} := F_{2k-2}(x_k, x_k^*)$ für $k \in \{1, \ldots, m\}$. So mit haben wir für alle $k \in \{1, \ldots, m\}$

$$M \cup \{x_1, \ldots, x_k\} \subseteq F_{2k} = F_{2k}^*$$

und nach Aufgabe 3 des letzten Blattes dass

$$[F_{2k-2}(x_k) : F_{2k-2}] = [F_{2k-2}(x_k^*) : F_{2k-2}] \leq 2.[1]$$

[1] Beachte, dass bei dem Beweis wesentlich einging, dass der Körper, in diesem Fall F_{2k-2}, unter komplexer Konjugation abgeschlossen ist.

Damit ist auch $[F_{2k-1}(x_k^*) : F_{2k-1}] \leq 2$. Insgesamt bekommen wir für alle $k \in \{1, \dots, m\}$ dass $[F_k : F_{k-1}] \leq 2$. Um „$= 2$“ zu bekommen, streichen wir aus der Liste diejenigen Körper, die keine echte Erweiterung liefern.

Für die Rückrichtung nehmen wir an, wir haben eine Folge $F_0 \subseteq \cdots \subseteq F_n$ wie in der Behauptung. Aus Aufgabenteil (a) wissen wir, dass es $a_k \in F_{k-1}$ gibt mit $F_k = F_{k-1}(\sqrt{a})$. Es ist $F_0 = K \subseteq \curlywedge M$ und wieder mit Aufgabe 3 des letzten Blattes folgt induktiv aus $F_{k-1} \subseteq \curlywedge M$ auch $F_k \subseteq \curlywedge M$ für alle $k \in \{1, \dots, n\}$. Somit $a \in F_n \subseteq \curlywedge M$.