LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley
Martin Hofer

Wintersemester 2018/19
27. Januar 2019

Algebra – Lösungsskizzen zu Übungsblatt 10

Aufgabe 1 (6 Punkte).

a) Sei L der Zerfällungskörper von X^4-3. Die Nullstellen von f sind durch die Elemente

$$\pm\sqrt[4]{3}, \pm i\sqrt[4]{3}$$

gegeben. Wir zeigen $L = \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3})$. Die Inklusion „$\supseteq$“ ist klar. Für die andere Richtung bemerke, dass laut Definition $\sqrt[4]{3} \in L$ gilt und außerdem $i = \frac{i\sqrt[4]{3}}{\sqrt[4]{3}} \in L$ gilt.

b) Laut der Gradformel gilt:

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

Um den zweiten Grad zu bestimmen, bemerken wir, dass es sich bei f um ein normiertes Polynom handelt, das $f(\sqrt[4]{3}) = 0$ erfüllt und laut dem Eisensteinkriterium irreduzibel ist. Also ist f das Minimalpolynom von $\sqrt[4]{3}$ über $\mathbb{Q}$ und es gilt $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = \operatorname{grad} f = 4$.
Weiter ist $g = x^2+1$ das Minimalpolynom von i über $\mathbb{Q}(\sqrt[4]{3})$: Das Polynom g ist normiert und hat i als Nullstelle. Da $\mathbb{Q}(\sqrt[4]{3})$ ein Teilkörper der reellen Zahlen ist, hat g über diesem keine Nullstellen, ist wegen $\operatorname{grad} g = 2$ also irreduzibel. Es folgt

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt[4]{3})] \cdot [\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q}] = 2\cdot 4 = 8.$$

c) Wir zeigen $\mathbb{Q}(\sqrt[4]{3}, i) = \mathbb{Q}(\sqrt[4]{3}+i)$.
Die Inklusion '$\supseteq$' ist klar. Für '$\subseteq$' berechnen wir zunächst mit $a = \sqrt[4]{3}+i$:

$$(a-i)^4 = 3 \iff a^4 - 4a^3 i + 6a^2 i^2 - 4ai^3 + i^4 = 3$$
$$\iff a^4 - 4a^3 i - 6a^2 + 4ai + 1 = 3 \iff -4a^3 i + 4ai = -a^4 + 6a^2 + 2.$$

Es gilt $-4a^3 + 4a = 4a(-a^2+1) = 4a(1+a)(1-a) \neq 0$ und somit erhalten wir

$$i = \frac{-a^4+6a^2+2}{-4a^3+4a} \in \mathbb{Q}(a) = \mathbb{Q}(\sqrt[4]{3}+i)$$

Daraus folgt natürlich $\sqrt[4]{3} = a - i \in \mathbb{Q}(a)$ und damit insgesamt die gewünschte Gleichung.

Aufgabe 2 (6 Punkte).

a) Wir zeigen die Aussage über Induktion: Der Fall $n = 1$ ist klar, da $L = K$ und $[L : K] = 1$ gilt. Sei die Aussage nun für $n-1$ bewiesen und sei α Nullstelle von f in L. Es gilt dann $K(\alpha) \subseteq L$. Über $K(\alpha)$ können wir f faktorisieren als $f = (X-\alpha)\cdot g$ mit $g \in K(\alpha)[X]$ und $\deg(g) = n-1$; es ist dann L der Zerfällungskörper von g. Insbesondere gilt nach Induktionsvoraussetzung, dass $[L : K(\alpha)]$ ein Teiler von $(n-1)!$ ist. Wir wollen nun zeigen, dass $[K(\alpha) : K]$ ein Teiler von n ist. Ist f irreduzibel, so ist dies klar, da dann gerade $[K(\alpha) : K] = n$ gilt. Sei nun f reduzibel, d.h. $f = h \cdot l$ für Polynome $h, l \in K[X]$ und $0 < \deg(h) = k < n$, $0 < \deg(l) = n-k < n$. Seien $a_1, \dots, a_k$ die Nullstellen von h in L. Dann ist $K(a_1, \dots, a_k)$ der Zerfällungskörper von h; außerdem macht man sich klar, dass L weiterhin der Zerfällungskörper von $l \in K(a_1, \dots, a_k)[X]$ (!) ist. Nach Induktionsvoraussetzung gilt dann $[K(a_1, \dots, a_k) : K] \mid k!$ und $[L : K(a_1, \dots, a_k)] \mid (n-k)!$; insbesondere folgt $[L : K] = [L : K(a_1, \dots, a_k)][K(a_1, \dots, a_k) : K] \mid k!(n-k)!$. Letzteres ist jedoch ein Teiler von $n!$, da $\frac{n!}{k!(n-k)!}$ gerade der Binomialkoeffizient $\binom{n}{k}$ ist und dieser ist eine natürliche Zahl. Mit dem Gradlemma folgt jetzt die Behauptung.

b) Dies ergibt sich nun von ganz alleine: Ist $f = h \cdot l$, so ist nach obiger Argumentation $[L : K] \leq \deg(h)!\deg(l)! = \deg(h)!(n-\deg(h))! \leq n!$. Gilt nun hier Gleichheit, so folgt $\frac{n!}{\deg(h)!(n-\deg(h))!} = \binom{n}{\deg(h)} = 1$. Dies ist jedoch nur für $\deg(h) = n$ oder $\deg(h) = 0$ möglich und es folgt, dass entweder l eine Einheit (falls $\deg(h) = n$) oder h eine Einheit ist (falls $\deg(h) = 0$).

Aufgabe 3 (6 Punkte).

Wir erkennen zuerst, dass 1 und -1 Nullstellen von f sind. Polynomdivision liefert dann die Zerlegung:

$$f = (X-1)(X+1)(X^4 - 6X^2 - 3)$$

a) Die ersten beiden Faktoren sind als Polynome von Grad 1 irreduzibel und mit Eisenstein ($p = 3$) folgt, dass der letzte Faktor irreduzibel über $\mathbb{Q}$ ist. Die Nullstellen von $X^4 - 6X^2 - 3$ berechnen sich (bspw. durch Substitution und die Formel für quadratische Gleichungen) als

$$\pm\sqrt{3+2\sqrt{3}}, \pm\sqrt{3-2\sqrt{3}}.$$

Insbesondere erhalten wir z.B. $\mathbb{Q}(\sqrt{3+2\sqrt{3}}, \sqrt{3-2\sqrt{3}})$ als Zerfällungkörper von f, denn es ist eine Körpererweiterung von $\mathbb{Q}$, die von den Nullstellen von f erzeugt wird, und nach Konstruktion zerfällt f dort in Linearfaktoren.

NB: Es hätte nicht gereicht, bspw. nur $\mathbb{Q}(\sqrt{3+2\sqrt{3}})$ zu betrachten, denn es ist $\sqrt{3+2\sqrt{3}}$ reell und somit gilt $\mathbb{Q}(\sqrt{3+2\sqrt{3}}) \subset \mathbb{R}$. Insbesondere ist die Nullstelle $\sqrt{3-2\sqrt{3}} \in \mathbb{C} \setminus \mathbb{R}$ nicht in $\mathbb{Q}(\sqrt{3+2\sqrt{3}})$ und f zerfällt dort nicht in Linearfaktoren.

b) Wir schreiben die obige Faktorisierung als $f = (X+12)(X+1)(X^4 + 7X^2 + 10)$. Ein schneller Koeffizientenvergleich liefert $X^4 + 7X^2 + 10 = (X^2+5)(X^2+2)$ und diese beiden Faktoren sind irreduzibel über $\mathbb{F}_{13}$, da sie dort keine Nullstellen haben. Aus der Vorlesung ist nun bekannt, dass das Polynom $X^2 + 2$ eine Nullstelle in $\mathbb{F}_{13^2} = \mathbb{F}_{13}[Y]/(Y^2+2)$ hat; aus Gradgründen zerfällt es dort also in Linearfaktoren. Bleibt der Faktor $X^2 + 5$: Die Elemente in $\mathbb{F}_{13^2}$ kann man identifizieren mit den Polynomen von Grad kleiner gleich 1 über $\mathbb{F}_{13}$. Wir müssen uns also Polynome $aY + b \in \mathbb{F}_{13}[Y]$ suchen, sodass $(aY + b)^2 + 5$ ein Vielfaches von $Y^2 + 2$ ist. Koeffizientenvergleich liefert dabei als Kandidaten das Polynom $3Y$. Tatsächlich gilt $(3Y)^2 + 5 = 9Y^2 + 5 = 9Y^2 + 2 \cdot 9 = 9(Y^2 + 2) = 0$ und die Klasse $3Y \in \mathbb{F}_{13^2}$ ist Nullstelle von $X^2 + 5 \in \mathbb{F}_{13^2}[X]$. Insbesondere zerfällt damit f vollständig in Linearfaktoren und $\mathbb{F}_{13^2}$ ist der Zerfällungskörper von f.

Aufgabe 4 (6 Punkte).

a) Sei $a \in L$ und $\sigma : L \to E_1$ so dass $\sigma_{|K} = \mathrm{id}_K$. Da L eine algebraische Erweiterung von K ist, exisiert ein Minimalpolynom f von a über K für das natürlich gilt $f(a) = 0$. Wir bekommen
$$f(\sigma(a)) = \sigma(f(a)) = \sigma(0) = 0,$$
was impliziert, dass $\sigma(a)$ algebraisch über K ist, also gilt $a \in \overline{K}_1$.

b) Durch Restriktion des Zielbereichs kann man nun die Elemente von $G(L/K, E_i/K)$ mit den Elementen von $G(L/K, \overline{K}_i/K)$ identifzieren und wir erhalten so eine Bijektion
$$\beta : G(L/K, E_i/K) \xrightarrow{\simeq} G(L/K, \overline{K}_i)$$
Da algebraische Abschlüsse bis auf Isomorphie eindeutig sind, gibt es einen Isomorphismus $\phi : \overline{K}_1 \to \overline{K}_2$, der die Abbildung
$$\begin{aligned} \phi^* : G(L/K, \overline{K}_1/K) &\to G(L/K, \overline{K}_2/K) \\ \tau &\mapsto \phi \circ \tau \end{aligned}$$
induziert, wobei man sofort sieht, dass $\sigma \mapsto \phi^{-1} \circ \sigma$ die Umkehrabbildung ist. Also bekommen wir die folgende Kette von Bijektionen
$$G(L/K, E_1/K) \xrightarrow{\simeq} G(L/K, \overline{K}_1/K) \xrightarrow{\simeq} G(L/K, \overline{K}_2/K) \xrightarrow{\simeq} G(L/K, E_2/K)$$
und gilt auch die Aussage über die Anzahl der K-Körperhomomorphismen aus der Angabe.