

Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 9

Jendrik Stelzner

Letzte Änderung: 2. Januar 2018

Aufgabe 1

(a)

Die Aussage ist *wahr*:

Da M/K algebraisch ist, gibt es für jedes $a \in M$ ein Polynom $p(t) \in K[t]$ mit $p(t) \neq 0$ und $p(a) = 0$. Dann gilt auch $p(t) \in L[t]$, weshalb a algebraisch über M ist. Das zeigt, dass auch M/L algebraisch ist.

Jedes Element $a \in M$ ist algebraisch über K , da M/K algebraisch ist. Insbesondere ist jedes $a \in L$ algebraisch über K , und somit L/K algebraisch.

(b)

Die Aussage ist *wahr*, denn nach der Gradformel gilt

$$[M : K] = [M : L][L : K],$$

und nach Annahme gilt $[M : L], [L : K] < \infty$

(c)

Die Aussage ist *wahr*: Per Aufgabenstellung ist L ein algebraischer Abschluss von \mathbb{R} . Außerdem ist \mathbb{C} ein algebraischer Abschluss von \mathbb{R} . Es gibt deshalb nach der Vorlesung einen \mathbb{R} -Isomorphismus $L \rightarrow \mathbb{C}$. Insbesondere gilt

$$[L : \mathbb{R}] = \dim_{\mathbb{R}} L = \dim_{\mathbb{R}} \mathbb{C} = 2.$$

(d)

Die Aussage ist *falsch*: Es sei $\alpha := e^{2\pi i/5}$. Wir bemerken zunächst, dass das Element

$$\beta := \alpha + \alpha^{-1} = \alpha + \bar{\alpha}$$

das Polynom $p(t) := t^2 + t - 1$ erfüllt. Es ist nämlich α eine primitive 5-te Einheitswurzel weshalb $\Phi_5(\alpha) = 0$ gilt. Also gilt

$$\begin{aligned} 0 &= \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^{-1} + \alpha^{-2} + \alpha^2 + \alpha + 1 \\ &= \alpha^{-1} + (\alpha^{-1} + \alpha)^2 - 2 + \alpha + 1 = \beta^2 + \beta - 1. \end{aligned}$$

Es gibt mehrere Möglichkeiten, einzusehen, dass $\mathbb{Q} \subsetneq \mathbb{Q}(\beta)$ gilt:

- Das Polynom hat keine rationale Nullstelle, denn die beiden komplexen Nullstellen sind $(-1 \pm \sqrt{5})/2$. Somit gilt insbesondere $\beta \notin \mathbb{Q}$. (Man kann hier bereits erkennen, dass $\beta = (-1 + \sqrt{5})/2$ gilt.)

Hieraus ergibt sich insbesondere auch, dass $p(t)$ irreduzibel ist, da es quadratisch ist.

- Das Polynom $p(t) = t^2 + t - 1 \in \mathbb{Z}[t]$ ist normiert und somit primitiv. Das Polynom $\bar{p}(t) = t^2 + t + 1 \in (\mathbb{Z}/2)[t]$ ist irreduzibel, da es quadratisch ist und keine Nullstellen besitzt (da $\bar{p}(0) = 1 = \bar{p}(1)$ gilt). Nach dem Reduktionskriterium ist $p(t)$ somit irreduzibel. Somit ist $p(t)$ das Minimalpolynom von β über \mathbb{Q} , weshalb $[\mathbb{Q}(\beta) : \mathbb{Q}] = \deg p = 2$ gilt. Insbesondere gilt $\beta \notin \mathbb{Q}$.
- Das Minimalpolynom von β über \mathbb{Q} ist $\Phi_5(t)$ (die Irreduzibilität ist aus der Vorlesung bekannt), weshalb $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg \Phi_5 = 4$ gilt. Deshalb ist die Familie $(1, \alpha, \alpha^2, \alpha^3)$ eine \mathbb{Q} -Basis von $\mathbb{Q}(\alpha)$. In dieser Basis gilt

$$\beta = \alpha + \alpha^{-1} = \alpha + \alpha^4 = \alpha + (-\alpha^3 - \alpha^2 - \alpha - 1) = -\alpha^3 - \alpha^2 - 1.$$

Inbesondere gilt $\beta \notin \langle 1 \rangle_{\mathbb{Q}} = \mathbb{Q}$.

Es gilt $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$, da $\beta = \alpha + \alpha^{-1} \in \mathbb{Q}(\alpha)$ gilt. Es ergibt sich auch auf verschiedenen Weisen, dass bereits $\mathbb{Q}(\beta) \subsetneq \mathbb{Q}(\alpha)$ gilt.

- Nach den ersten beiden obigen Argumentationen ist $p(t)$ irreduzibel über \mathbb{Q} , und somit das Minimalpolynom von β über \mathbb{Q} . Also gilt $[\mathbb{Q}(\beta) : \mathbb{Q}] = \deg p(t) = 2$. Nach der letzten der obigen Argumentation gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Es gilt somit

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 > 2 = [\mathbb{Q}(\beta) : \mathbb{Q}]$$

und deshalb $\mathbb{Q}(\alpha) \supsetneq \mathbb{Q}(\beta)$.

- Es gilt $\mathbb{Q}(\beta) \subseteq \mathbb{R}$, da $\beta = \alpha + \bar{\alpha} \in \mathbb{R}$ gilt (sowie $\mathbb{Q} \subseteq \mathbb{R}$). Es gilt aber auch $\alpha \notin \mathbb{R}$, und somit $\alpha \notin \mathbb{Q}(\beta)$. Also gilt $\mathbb{Q}(\beta) \subsetneq \mathbb{Q}(\alpha)$.

Insgesamt ergibt sich, dass $\mathbb{Q}(\beta)$ ein echtere Zwischenkörper $\mathbb{Q} \subsetneq \mathbb{Q}(\beta) \subsetneq \mathbb{Q}(\alpha)$ ist.

(e)

Die Aussage ist *wahr*: Das Minimalpolynom von $\alpha := \sqrt[p]{q}$ über \mathbb{Q} ist $p(t) := t^p - q$, wobei sich die Irreduzibilität aus dem Eisenstein-Kriterium ergibt. Folglich ist der Grad $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ prim. Für jeden Zwischenkörper $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\alpha)$ gilt nun

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

und somit

$$[\mathbb{Q}(\alpha) : K] = 1 \quad \text{oder} \quad [K : \mathbb{Q}] = 1,$$

und somit

$$K = \mathbb{Q}(\alpha) \quad \text{oder} \quad K = \mathbb{Q}.$$

Aufgabe 3

(b)

Im Tutorium haben wir genutzt, dass

$$K^{\text{alg}} = \{x \in K \mid x \text{ ist algebraisch über } K\}$$

ein Unterkörper von K ist, und wegen $L_1, L_2 \subseteq K$ damit auch $L_1 L_2 \subseteq K$ gilt. Es gibt auch noch alternative Argumentationsmöglichkeiten:

- Jedes $x \in L_2$ ist nach Annahme algebraisch über K , und somit auch algebraisch über L_1 . Also ist die Körpererweiterung $L_1(L_2)/L_1$ algebraisch, also $L_1 L_2/L_1$ algebraisch. Nach Annahme ist auch L_1/K algebraisch. Wegen der Transitivität von Algebraizität ist damit auch $L_1 L_2/K$ algebraisch.
- Es seien $L_1 = K(\alpha_i \mid i \in I)$ und $L_2 = K(\beta_j \mid j \in J)$. Alle α_i und β_j sind algebraisch über K , da L_1/K und L_2/K algebraisch sind. Dann gilt

$$L_1 L_2 = K(\{\alpha_i \mid i \in I\} \cup \{\beta_j \mid j \in J\}),$$

weshalb $L_1 L_2$ von Elementen erzeugt wird, die algebraisch über K sind. Also ist auch $L_1 L_2/K$ algebraisch.

- Da L_1/K und L_2/K algebraisch sind, lässt sich der Körper $L_1 L_2$ auch explizit beschreiben: Es sei

$$L := \left\{ \sum_{i=1}^n x_i y_i \mid \begin{array}{l} n \geq 0, \\ x_i \in L_1, y_i \in L_2 \end{array} \right\}.$$

Dann ist L der von L_1 und L_2 erzeugte Unterring von L : Es gilt $1 = 1 \cdot 1 \in L$. Für alle $z_1, z_2 \in L$ mit $z_1 = \sum_{i=1}^n x_i y_i$ und $z_2 = \sum_{i=n+1}^m x_i y_i$ gilt dann auch

$z_1 + z_2 = \sum_{i=1}^m x_i y_i \in L$. Für alle $z_1, z_2 \in L$ mit $z_1 = \sum_{i=1}^n x_i y_i$ und $z_2 = \sum_{j=1}^m x'_j y'_j$ gilt auch

$$z_1 z_2 = \left(\sum_{i=1}^n x_i y_i \right) \left(\sum_{j=1}^m x'_j y'_j \right) = \sum_{i=1}^n \sum_{j=1}^m \underbrace{(x_i x'_j)}_{\in L_1} \underbrace{(y_i y'_j)}_{\in L_2} \in L.$$

Nach Annahme sind alle $x \in L_1$ und $y \in L_2$ algebraisch über K , weshalb auch L algebraisch über K ist. Außerdem ist L als Unterring von M ein Integritätsbereich. Nach Aufgabe 2 (c) von Zettel 8 ist L somit bereits ein Körper. Also ist L bereits der von L_1 und L_2 erzeugte Unterkörper, also $L = L_1 L_2$. Insbesondere sind alle Elemente von $L_1 L_2$ algebraisch über K .

Bemerkung 1. Für beliebige, nicht notwendigerweise algebraische Körpererweiterungen L_1/K und L_2/K gilt

$$\begin{aligned} L_1 L_2 &= \left\{ \frac{x}{x'} \mid x, x' \in L, x' \neq 0 \right\} \\ &= \left\{ \frac{\sum_{i=1}^n x_i y_i}{\sum_{j=1}^m x'_j y'_j} \mid \begin{array}{l} n, m \geq 0, \\ x_i, x'_i \in L_1, y_j, y'_j \in L_2, \\ \sum_{j=1}^m x'_j y'_j \neq 0 \end{array} \right\}. \end{aligned}$$

Dies entspricht dem Quotientenkörper $\text{Quot}(L)$ sofern man diesen in M einbettet.

Beispiel 2. Es sei $K(X, Y)$ der Funktionenkörper in zwei Variablen X und Y , und es seien $K(X), K(Y) \subseteq K(X, Y)$ die Funktionenkörper in jeweils einer Variable, aufgefasst als Unterkörper von $K(X, Y)$. Dann gilt $K(X)K(Y) = K(X, Y)$. Aber

$$\langle K(X) \cup K(Y) \rangle_{\text{Ring}} = \left\{ \frac{f(X, Y)}{g(X)h(Y)} \mid \begin{array}{l} f(X, Y) \in K[X, Y], \\ g(X) \in K[X], h(Y) \in K[Y] \end{array} \right\} \subsetneq K(X, Y).$$

So gilt etwa $1/(1 + XY) \notin \langle K(X) \cup K(Y) \rangle_{\text{Ring}}$.

(c)

Wir haben im Tutorium bereits einen Beweis gesehen, und geben hier noch einen weiteren, indem wir konkret ein K -Erzeugendensystem von $L_1 L_2$ aus K -Basen von L_1 und L_2 konstruieren. Hierfür seien $x_1, \dots, x_n \in L_1$ und $y_1, \dots, y_m \in L_2$ jeweils endliche K -Basen; da L_1/K und L_2/K endlich sind, gibt es diese.

Behauptung. Die Produkte $x_i y_j \in L_1 L_2$ bilden ein K -Erzeugendensystem von $L_1 L_2$.

Aus dieser Behauptung erhalten wir dann direkt, dass

$$[L_1 L_2 : K] = \dim_K(L_1 L_2) \leq nm = (\dim_K L_1)(\dim_K L_2) = [L_1 : K][L_2 : K].$$

Beweis der Behauptung. Wir geben zwei Beweise für die Behauptung an:

- Die Erweiterungen L_1/K und L_2/K sind algebraisch, da sie endlich sind. Wie bereits oben gesehen, gilt deshalb

$$L_1 L_2 = \left\{ \sum_i \tilde{x}_i \tilde{y}_i \mid \begin{array}{l} n \geq 0, \\ \tilde{x}_i \in L_1, \tilde{y}_i \in L_2 \end{array} \right\}.$$

Dabei lässt sich jedes \tilde{x}_i als K -Linearkombination der x_j schreiben, und jedes \tilde{y}_i als Linearkombination der y_j . Damit ist dann $\sum_i \tilde{x}_i \tilde{y}_i$ eine K -Linearkombination der $x_{j_1} y_{j_2}$.

- Da $x_1, \dots, x_n \in L_1$ und $y_1, \dots, y_m \in L_2$ jeweils K -Erzeugendensysteme sind, gelten insbesondere

$$L_1 = K(x_1, \dots, x_n) \quad \text{und} \quad L_2 = K(y_1, \dots, y_m).$$

Damit gilt dann auch

$$L_1 L_2 = K(x_1, \dots, x_n, y_1, \dots, y_m).$$

Da die x_i und y_j algebraisch über K sind (da L_1/K und L_2/K als endliche Körpererweiterungen insbesondere algebraisch sind), gilt dabei bereits

$$L_1 L_2 = K(x_1, \dots, x_n, y_1, \dots, y_m) = K[x_1, \dots, x_n, y_1, \dots, y_m].$$

Also wird $L_1 L_2$ als K -Vektorraum von den Monomen

$$x_1^{\alpha_1} \dots x_n^{\alpha_n} y_1^{\beta_1} \dots y_m^{\beta_m}$$

erzeugt. Dabei gilt $x_1^{\alpha_1} \dots x_n^{\alpha_n} \in L_1$, weshalb $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ eine K -Linearkombination der x_i ist; analog ergibt sich auch, dass $y_1^{\beta_1} \dots y_m^{\beta_m}$ eine K -Linearkombination der y_j ist. Damit ist das Monom $x_1^{\alpha_1} \dots x_n^{\alpha_n} y_1^{\beta_1} \dots y_m^{\beta_m}$ insgesamt eine K -Linearkombination der $x_i y_j$. Da dies für jedes der Monome gilt, und $L_1 L_2$ diese Monome als K -Erzeugendensystem hat, sind die $x_i y_j$ bereits ein K -Erzeugendensystem von $L_1 L_2$.

□