Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 9

Jendrik Stelzner

Letzte Änderung: 8. Januar 2018

n

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 algebrasich 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 einen $\mathbb{R}$-Isomorphismus $L \to \mathbb{C}$. Insbesondere gilt

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

(d)

Die Aussage ist *falsch*: Es seien $\alpha := e^{2\pi i/5}$ und $\beta := \alpha + \alpha^{-1}$.

Behauptung. *Die Zahl β erfüllt das Polynom $p(t) := t^2 + t - 1$.*

Beweis. Es gilt $\Phi_5(\alpha) = 0$, da α eine primitive 5-te Einheitswurzel ist. Also gilt

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

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

- Das Polynom $p(t)$ hat keine rationale Nullstelle, denn die beiden komplexen Nullstellen sind $(-1 \pm \sqrt{5})/2$. Somit gilt inbesondere $\beta \notin \mathbb{Q}$. (Man kann hier bereits erkennen, dass $\beta = (-1 + \sqrt{5})/2$ gilt.) (Da $p(t)$ qaudatrisch ist, ergibt sich hieraus auch, dass $p(t)$ irreduzibel ist.)
- Das Polynom $p(t) = t^2 + t - 1 \in \mathbb{Z}[t]$ ist normiert und somit primitiv. Das Polynom $\overline{p}(t) = t^2 + t + 1 \in (\mathbb{Z}/2)[t]$ ist irreduzibel, da es quadratisch ist und keine Nullstellen besitzt (da $\overline{p}(0) = 1 = \overline{p}(1)$ 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. Inbesondere gilt $\beta \notin \mathbb{Q}$.
- Das Minimalpolynom von α über $\mathbb{Q}$ ist $\Phi_5(t)$ (die Irreduziblität 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 somit $\beta \notin \langle 1 \rangle_{\mathbb{Q}} = \mathbb{Q}$.

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

- Nach den ersten beiden der 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 $\beta = \alpha + \alpha^{-1} = \alpha + \overline{\alpha} \in \mathbb{R}$ 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.

Bemerkung 1. Wir werden im weiteren Verlauf der Vorlesung sehen, dass die Körpererweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$ *galoissch* ist, und deshalb die Zwischenkörper $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\alpha)$ auf bijektive Weise den Untergruppen der *Galoisgruppe* $\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$ entsprechen. Dabei gilt $\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}/4$. Da $\mathbb{Z}/4$ genau drei Untergruppen hat, nämlich 0, $2\mathbb{Z}/4$ und $\mathbb{Z}/4$, hat die Erweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$ genau drei Zwischenkörper, nämlich $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ und $\mathbb{Q}$.

(e)

Die Aussage ist *wahr*: Das Minimalpolynom von $\alpha \coloneqq \sqrt[p]{q}$ über $\mathbb{Q}$ ist $p(t) \coloneqq t^p - q$, wobei sich die Irreduziblität 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 2

Wir wollen hier noch einige An- und Bemerkungen zu Polynomringen treffen:

Zusammenkleben von Polynomringen mit endlich vielen Variablen

Man kann die Existenz und die universelle Eigenschaft des Polynomrings in einer beliebigen Menge von Variablen $(t_i)_{i \in I}$ auf die Existenz und universelle Eigenschaft von Polynomringen in endlich vielen Variablen zurückführen:

Konstruktion

Wir wissen bereits, dass sich für jede endliche Menge J einen Polynomring in den Variablen $(t_j)_{j \in J}$ konstruieren lässt. Sind dabei J und K endliche Mengen mit $J \subseteq K$, so lässt sich der Polynomring $R[(t_j)_{j \in J}]$ als ein Unterring des Polynomrings $R[(t_k)_{k \in K}]$ auffassen. Der Polynomring $R[(t_i)_{i \in I}]$ für eine beliebige Menge I lässt sich nun als die Vereinigung

$$R[(t_i)_{i \in I}] \coloneqq \bigcup_{\substack{J \subseteq I \\ J \text{ endlich}}} R[(t_j)_{j \in J}]$$

definieren:

Sind $f, g \in R[(t_i)_{i \in I}]$ zwei Polynome, so gibt es endliche Teilmengen $J_1, J_2 \subseteq I$ mit $f \in R[(t_j)_{j \in J_1}]$ und $g \in R[(t_j)_{j \in J_2}]$. Dann ist auch $J \coloneqq J_1 \cup J_2 \subseteq I$ eine endliche Teilmenge mit $f, g \in R[(t_j)_{j \in J}]$. Somit lassen sich $f + g$ und $f \cdot g$ über die Addition und Multiplikation in $R[(t_j)_{j \in J}]$ definieren.

Diese Definition ist unabhängig von der Wahl von J_1 und J_2: Sind $K_1, K_2 \subseteq I$ weitere endliche Teilmengen mit $f \in R[(t_k)_{k \in K_1}]$ und $g \in R[(t_k)_{k \in K_2}]$, so gilt für die endliche Teilmenge $K \coloneqq K_1 \cup K_2 \subseteq I$, dass $R[(t_j)_{j \in J}]$ und $R[(t_k)_{k \in K}]$ Unterringe von $R[(t_\ell)_{\ell \in L}]$ für die endliche Teilmenge $L \coloneqq K \cup L \subseteq I$ sind, und somit $f + g$ und $f \cdot g$ in $R[(t_j)_{j \in J}]$ und $R[(t_k)_{k \in K}]$ übereinstimmen.

Man bemerke, dass dieses Vorgehen deshalb funktioniert, weil in jedem Polynom $f \in R[(t_i)_{i\in I}]$ tatsächlich nur endlich viele der möglicherweisen unendlich vielen Variablen $(t_i)_{i\in I}$ vorkommen, d.h. es gibt eine (von f abhängende) endliche Teilmenge $J \subseteq I$ mit $f \in R[(t_j)_{j\in J}]$.

Universelle Eigenschaft

Auch die universelle Eigenschaft des Polynomrings $R[(t_i)_{i\in I}]$ ergibt sich dann aus der entsprechenden universellen Eigenschaft für Polynomringe in endlich vielen Variablen:

Ist S ein kommutativer Ring und $(s_i)_{i\in I}$ eine Familie von Elementen $s_i \in S$, so gibt es für jede endliche Teilmenge $J \subseteq I$ nach der universellen Eigenschaft des Polynomrings $R[(t_j)_{j\in J}]$ (der nur endlich viele Variablen hat) einen eindeutigen Ringhomomorphismus

$$f_J \colon R[(t_j)_{j\in J}] \to S$$

mit $f_J(t_j) = s_j$ für alle $j \in J$ und $f_J|_R = \phi$. Sind dabei $J_1, J_2 \subseteq I$ endliche Teilmengen, so folgt für den Schnitt $J \coloneqq J_1 \cap J_2$ aus dieser Eindeutigkeit, dass

$$f_{J_1}|_{R[(t_j)_{j\in J}]} = f_J = f_{J_2}|_{R[(t_j)_{j\in J}]}\,.$$

Deshalb lassen sich die Ringhomomorphismen f_J für endliche Teilmengen $J \subseteq I$ eindeutig zu einem Ringhomomorphismus

$$f \colon R[(t_i)_{i\in I}] = \bigcup_{\substack{J\subseteq I\\ J \text{ endlich}}} R[(t_j)_{j\in J}] \to S$$

zusammenfügen, so dass $f|_{R[(t_j)_{j\in J}]} = f_J$ für jede endliche Teilmenge $J \subseteq I$ gilt. Dann gilt $f(t_i) = s_i$ für alle $i \in I$, sowie $f|_R = \phi$.

Streng genommen ...

ist für Teilmengen $J \subseteq K$ der Polynomring $R[(t_j)_{j\in J}]$ kein Unterring von $R[(t_k)_{k\in K}]$, sondern kann nur mit einem solchen identifiziert werden. Man kann sich deshalb an der Notation

$$\bigcup_{\substack{J\subseteq I\\ J \text{ endlich}}} R[(t_j)_{j\in J}]$$

stören. Dieses Problem lässt sich dadurch umgehen, dass man den Begriff des *Kolimes* einführt (was wir hier nicht tuen werden). Dann erhält man (auf mathematisch saubere Weise), dass

$$R[(t_i)_{i\in I}] \cong \varinjlim_{\substack{J\subseteq I\\ J \text{ endlich}}} R[(t_j)_{j\in J}]\,.$$

Monoidringe

Eine wichtige Verallgemeinerung von Polynomringen (mit nahezu unveränderter Konstruktion) bilden sogenannte Monoidringe:

Definition 2. *Ein* Monoid *ist eine Menge M zusammen mit einer assoziativen, binären Verknüpfung $\cdot\colon M \times M \to M$, $(m_1, m_2) \mapsto m_1 \cdot m_2$, so dass es ein neutrales Element $1 \in M$ gibt, d.h. es gilt*

$$1 \cdot m = m = m \cdot 1 \qquad \text{für alle } m \in M\,.$$

Gilt zusätzlich $m_1 \cdot m_2 = m_2 \cdot m_1$ für alle $m_1, m_2 \in M$, so heißt M abelsch.

Beispiel 3.

1. Die natürlichen Zahlen $\mathbb{N}$ bilden zusammen mit der üblichen Addition ein kommutatives Monoid. Das neutrale Element ist 0.

2. Allgemeiner ist für jede Indexmenge I auch

$$\mathbb{N}^{(I)} = \{(\alpha_i)_{i \in I} \mid \alpha_i \in \mathbb{N}, \alpha_i = 0 \text{ für fast alle } i \in I\}$$

   ein Monoid bezüglich der komponentenweise Addition. Das neutrale Element ist das Nulltupel $0 = (0)_{i \in I}$.

3. Ist R ein Ring, so bildet R bezüglich der Multiplikation $\cdot$ ein Monoid $(R, \cdot)$ mit neutralen Element 1. Die Kommutavität von R ist gerade die Kommutativität dieses Monoids.

4. Gruppen sind genau jene Monoide, in denen jedes Element ein Inverses besitzt.

Ist M ein kommutativer Monoid, additiv geschrieben (wie man es von abelschen Gruppen gewohnt ist), und R ein kommutativer Ring, so lässt sich der *Monoidring* $R[M]$ konstruieren:

- Die Elemente von $R[M]$ sind formale Linearkombinationen $\sum_{m \in M} r_m t^m$ wobei $r_m = 0$ für fast alle $m \in M$ gilt.

- Zwei formale Linearkombinationen $\sum_{m \in M} r_m t^m$ und $\sum_{m \in M} r'_m t^m$ sind genau dann gleich, wenn $r_m = r'_m$ für alle $m \in M$ gilt.

- Die Addition auf $R[M]$ ist durch

$$\left(\sum_{m \in M} r_m t^m\right) + \left(\sum_{m \in M} r'_m t^m\right) = \sum_{m \in M} (r_m + r'_m) t^m$$

  definiert.

- Die Multiplikation auf $R[M]$ ist durch

$$\left(\sum_{m\in M} r_m t^m\right) \cdot \left(\sum_{m\in M} r'_m t^m\right) = \sum_{m_1,m_2\in M} (r_{m_1} r'_{m_2}) t^{m_1+m_2}$$

definiert; alternativ lässt sie sich dadurch ausdrücken, dass

$$\left(\sum_{m\in M} r_m t^m\right) \cdot \left(\sum_{m\in M} r'_m t^m\right) = \sum_{m\in M} s_m t^m$$

gilt, wobei die Koeffizienten s_m durch

$$s_m = \sum_{\substack{m_1,m_2\in M\\ m_1+m_2=m}} r_{m_1} r_{m_2} \qquad \text{für alle } m \in M$$

gegeben sind.

Der so entstehende Ring hat das Nullelement $0 = \sum_{m\in M} 0 \cdot t^m$, und das Einselement $1 = \sum_{m\in M} \delta_{0m} t^m = t^0$. Außerdem ist die Abbildung

$$R \to R[M]\,, \quad r \mapsto rt^0$$

ein injektiver Ringhomomorphismus, wodurch sich R als ein Unterring von $R[M]$ auffassen kann. Die notwendigen Rechnungen lassen sich unverändert aus dem Tutorium übernehmen.

Beispiel 4.

1. Der Monoidring $R[\mathbb{N}]$ ist der übliche Polynomring $R[t]$ in einer Variablen.
2. Der Monoidring $R[\mathbb{N}^{(I)}]$ ist der Polynomring $R[(t_i)_{i\in I}]$.

Auch der Monoidring hat eine universelle Eigenschaft: Ist S ein weiterer kommutativer Ring, $\phi\colon R \to S$ ein Ringhomomorphismus und $f\colon M \to (S, \cdot)$ ein Monoidhomomorphismus, so gibt es einen eindeutigen Ringhomomorphismus $F\colon R[M] \to S$ mit $F|_R = \varphi$ und $F(t^m) = f(m)$ für alle $m \in M$. Hieraus lässt sich auch die universelle Eigenschaft des Polynomrings $R[(t_i)_{i\in I}]$ herleiten.

Bemerkung 5. Tatsächlich wird an keine Stelle die Kommutativität der Ringe R, S oder des Monoids M benötigt: Der Monoidring $R[M]$ lässt sich für jeden Ring R und jedes Monoid M bilden, und die obige universelle Eigenschaft gilt dann für ebenfalls beliebige Ringe S.

Häufig schreibt man dann die Element des Monoidrings $R[M]$ nicht als Polynome $\sum_{m\in M} r_m t^m$, sondern als $\sum_{m\in M} r_m e_m$, oder auch direkt als $\sum_{m\in M} r_m m$. Man stellt sich die Elemente von $R[M]$ dann als formale Linearkombinationen der Elemente von M vor, und die Multiplikation von $R[M]$ als die eindeutige R-bilineare Fortsetzung der Multiplikation von M.

Ist insbesondere G eine Gruppe, so ist

$$R[G] = \left\{ \sum_{g \in G} r_g g \,\middle|\, r_g \in R, r_g = 0 \text{ für fast alle } g \in G \right\}$$

der *Gruppenring*, bzw. die *Gruppenalgebra* von R über G. Diese Konstruktion spielt eine wichtige Rolle in vielen Bereichen der Mathematik.

Aufgabe 3

(b)

Im Tutorium haben wir genutzt, dass

$$K^{\mathrm{alg}} = \{x \in K \,|\, x \text{ ist algebraisch über } K\}$$

ein Unterkörper von K ist, und wegen $L_1, L_2 \subseteq K$ deshalb 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 (denn $L_1(L_2) = L_1 L_2$). Nach Annahme ist auch L_1/K algebraisch. Wegen der Transitivität von Algebraizität ist damit auch $L_1 L_2/K$ algebraisch.

- Es seien $L_1 = K(\alpha_i \,|\, i \in I)$ und $L_2 = K(\beta_j \,|\, j \in J)$. Alle α_i und β_j sind algebraisch über K, da L_1/K und L_2/K algebraisch sind. Dann gilt

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

  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

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

  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 6. Setzt man nicht voraus, dass L_1/K und L_2/K algebraisch sind, so gilt mit der obigen Definition von L, dass

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

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

Beispiel 7. 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

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

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 aus K-Basen von L_1 und L_2 ein K-Erzeugendensystem von $L_1 L_2$ konstruieren. Hierfür seien $x_1, \dots, x_n \in L_1$ und $y_1, \dots, y_m \in L_2$ jeweils endliche K-Basen.

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

$$L_1 L_2 = \left\{ \sum_i \tilde{x}_i \tilde{y}_i \,\middle|\, \begin{gathered} n \geq 0, \\ \tilde{x}_i \in L_1, \tilde{y}_i \in L_2 \end{gathered} \right\}.$$

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

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

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

  Damit gilt dann auch

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

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

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

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

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

  erzeugt. Dabei gilt $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in L_1$, weshalb $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ eine K-Linearkombination der x_i ist; analog ergibt sich auch, dass $y_1^{\beta_1} \cdots y_m^{\beta_m}$ eine K-Linearkombination der y_j ist. Damit ist das Monom $x_1^{\alpha_1} \cdots x_n^{\alpha_n} y_1^{\beta_1} \cdots y_m^{\beta_m}$ 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 $L_1 L_2$.

$\square$

Bemerkung 8. Sind allgemeiner L_1/K und L_2/K nur algebraisch mit K-Basen $(x_i)_{i \in I}$ und $(y_j)_{j \in J}$, so ergibt sich aus der obigen Argumentation, dass die $x_i y_j$ ein K-Erzeugendensystem von $L_1 L_2$ bilden.