2. Der Grad von Körpererweiterungen

Wenn wir untersuchen wollen, ob eine gegebene Konstruktion in der Ebene mit Zirkel und Lineal durchführbar ist, haben wir im vorigen Kapitel gesehen, dass wir dazu herausfinden müssen, ob eine bestimmte komplexe Zahl in einer 2-Radikalerweiterung eines gegebenen Körpers liegt oder nicht.

Wie ihr euch vielleicht schon denken könnt, ist dies aber zunächst einmal nicht so einfach herauszufinden, da wir in der Regel ja nicht wissen können, wie diese 2-Radikalerweiterung genau aussieht. In diesem Kapitel wollen wir daher ein *notwendiges* Kriterium für die Existenz einer solchen Erweiterung (und damit für die Durchführbarkeit der Konstruktion) angeben, das sich wesentlich einfacher nachprüfen lässt. Das wesentliche Konzept hierfür ist das des *Grades* einer Körpererweiterung bzw. von Elementen einer Körpererweiterung. Um dies einzuführen, müssen wir untersuchen, ob die Elemente einer Körpererweiterung L/K Nullstellen von Polynomen über K sind, und wenn ja, welchen Grad diese Polynome haben.

Definition 2.1 (Algebraische und transzendente Elemente)**.** Es sei L/K eine Körpererweiterung.

(a) Ein Element $a \in L$ heißt **algebraisch** über K, wenn es ein Polynom $f \in K[t]$ gibt mit $f \neq 0$ und $f(a) = 0$. Andernfalls heißt a **transzendent** über K.

(b) Die Körpererweiterung L/K heißt algebraisch, wenn jedes $a \in L$ algebraisch über K ist. Andernfalls (also wenn es ein über K transzendentes Element in L gibt) heißt L/K transzendent.

Beispiel 2.2.

(a) Die reelle Zahl $\sqrt{2}$ ist offensichtlich algebraisch über $\mathbb{Q}$, denn sie ist Nullstelle des rationalen Polynoms $t^2 - 2$.

(b) Betrachten wir die Körpererweiterung $\mathbb{R}(t)/\mathbb{R}$ aus Beispiel 1.2 (c), so ist das Element $t \in \mathbb{R}(t)$ transzendent über $\mathbb{R}$, denn für Koeffizienten $a_0, \ldots, a_n \in \mathbb{R}$, die nicht alle Null sind, ist $a_n t^n + \cdots + a_1 t + a_0$ niemals 0 in $\mathbb{R}(t)$ (d. h. nie die Nullfunktion).

(c) Ein einfaches Abzählargument ergibt, dass es sehr viele transzendente Zahlen in $\mathbb{R}/\mathbb{Q}$ gibt: die Menge $\mathbb{Q}$ der rationalen Zahlen ist bekanntlich abzählbar. Ein Polynom in $\mathbb{Q}[t]$ vom Grad kleiner als n ist eindeutig durch seine n Koeffizienten in $\mathbb{Q}$ bestimmt; also ist die Menge aller solcher Polynome bijektiv zu $\mathbb{Q}^n$ und damit auch abzählbar. Da jedes solche Polynom (das nicht das Nullpolynom ist) nur endlich viele Nullstellen hat, ist die Menge aller Nullstellen von Polynomen vom Grad kleiner als n ebenfalls abzählbar für alle n. Nimmt man nun die Vereinigung dieser Nullstellenmengen für alle $n \in \mathbb{N}$, so erhält man die Menge aller algebraischen Zahlen und sieht, dass sie als abzählbare Vereinigung abzählbarer Mengen ebenfalls abzählbar sein muss. Die Menge der reellen Zahlen ist aber bekanntlich nicht abzählbar. Also gibt es transzendente Zahlen in $\mathbb{R}/\mathbb{Q}$ — in der Tat sind „die meisten“ Zahlen in $\mathbb{R}$ transzendent über $\mathbb{Q}$.

Trotz dieser Aussage ist es allerdings erstaunlich schwierig, von einer konkreten reellen Zahl nachzuweisen, dass sie transzendent über $\mathbb{Q}$ ist. Lindemann hat Ende des 19. Jahrhunderts bewiesen, dass π und e transzendent über $\mathbb{Q}$ sind; der Beweis hierfür ist jedoch sehr lang und technisch und benutzt Methoden, die wir erst entwickeln müssten und die wir danach für nichts anderes mehr verwenden könnten. Ich möchte ihn euch und mir daher ersparen. Wir werden die Transzendenz von e in dieser Vorlesung auch nicht benötigen, die von π tritt lediglich im Beweis der Unmöglichkeit der Quadratur des Kreises in Beispiel 2.23 auf.

02

Bemerkung 2.3. Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Dann gibt es unter allen Polynomen in $K[t]$, die a als Nullstelle haben, stets ein *eindeutiges* normiertes Polynom (d. h. der Leitkoeffizient ist 1) mit minimalem Grad. Wären nämlich f und g zwei verschiedene

normierte Polynome minimalen Grades mit Nullstelle a, so wäre $f-g$ ein nicht verschwindendes Polynom kleineren Grades in $K[t]$, das ebenfalls a als Nullstelle hätte (und das man natürlich auch normieren kann). Wir können also definieren:

Definition 2.4 (Minimalpolynom und Grad)**.** Es seien L/K eine Körpererweiterung und $a \in L$.

(a) Ist a algebraisch über K, so heißt das (nach Bemerkung 2.3 eindeutig bestimmte) normierte Polynom über K minimalen Grades mit Nullstelle a das **Minimalpolynom** von a. Wir bezeichnen es mit $m_{a,K} \in K[t]$, bzw. einfach mit m_a, wenn aus dem Zusammenhang klar ist, welcher Grundkörper gemeint ist. Sein Grad wird auch der **Grad** von a über K genannt und als $[a:K]$ geschrieben.

(b) Ist a transzendent über K, so setzen wir formal $[a:K] = \infty$.

Bemerkung 2.5 (Alternative Beschreibung des Minimalpolynoms)**.** Wie in Definition 2.4 seien L/K eine Körpererweiterung und $a \in L$. Wir betrachten die Menge

$$I = \{f \in K[t] : f(a) = 0\} \quad \subset K[t]$$

aller Polynome über K, die a als Nullstelle haben. Man prüft sofort nach, dass I ein Ideal ist. In der Tat behaupten wir, dass

$$I = (m_a) \tag{$*$}$$

gilt, also dass I von m_a erzeugt wird. Den Beweis dieser Aussage kennt ihr bereits aus den „Algebraischen Strukturen“: Dort haben wir nämlich gezeigt, dass man ein Ideal I in einem Hauptidealring stets als das Hauptideal schreiben kann, das von einem Element in $I \setminus \{0\}$ mit minimaler euklidischer Funktion erzeugt wird [G, Satz 10.21]. Wir können den Beweis aber auch hier schnell noch einmal geben:

„$\supset$“ Dies ist klar, denn (jedes Vielfache von) m_a hat natürlich a als Nullstelle.

„$\subset$“ Es sei $f \in K[t]$ mit $f(a) = 0$. Division von f mit Rest durch m_a liefert $f = q m_a + r$ für Polynome $q, r \in K[t]$ mit $\deg r < \deg m_a$. Setzen wir hier den Wert a ein, so erhalten wir $f(a) = q(a)m_a(a) + r(a)$, wegen $f(a) = m_a(a) = 0$ also $r(a) = 0$. Damit ist r ein Polynom mit Nullstelle a und kleinerem Grad als m_a — was nach Definition des Minimalpolynoms nur möglich ist, wenn $r = 0$ das Nullpolynom ist. Dann ist aber $f = q m_a \in (m_a)$.

Dies zeigt die Gleichung $(*)$. Beachte, dass man diese Gleichung auch verwenden könnte, um das Minimalpolynom auf eine andere Art zu *definieren*: als den (eindeutig bestimmten) normierten Erzeuger des Hauptideals aller Polynome über K mit Nullstelle a.

In Worten besagt die Gleichung $(*)$ einfach, dass jedes Polynom über K mit Nullstelle a ein Vielfaches von m_a ist, bzw. dass m_a jedes solche Polynom teilt. Dies werden wir später noch häufiger benötigen.

Minimalpolynome algebraischer Elemente werden im Folgenden eine große Rolle spielen. Wir wollen uns daher als Erstes fragen, wie man sie in der Praxis berechnen kann. Natürlich wird man dazu zunächst nach einem Polynom mit der gewünschten Nullstelle suchen und dieses dann normieren. Dies ist in der Regel nicht kompliziert. Es ist aber oft nur schwer zu entscheiden, ob es sich dabei auch um das Polynom *kleinsten Grades* mit dieser Nullstelle handelt, also ob man wirklich das Minimalpolynom gefunden hat. Um das zu entscheiden, ist das folgende Kriterium sehr nützlich.

Lemma 2.6 („Minimalpolynom=irreduzibel“)**.** *Es seien L/K eine Körpererweiterung, $a \in L$, und $f \in K[t]$ ein normiertes Polynom mit $f(a) = 0$. Dann gilt*

$$f = m_a \quad \Leftrightarrow \quad f \text{ ist irreduzibel in } K[t].$$

Beweis. Beide Richtungen dieser Äquivalenz sind einfach zu zeigen:

„$\Rightarrow$“ Angenommen, $f = m_a$ wäre reduzibel, d. h. $m_a = g \cdot h$ für gewisse Polynome $g, h \in K[t]$ mit $\deg g, \deg h < \deg m_a$. Einsetzen von a liefert $g(a)h(a) = m_a(a) = 0$. Da ein Körper keine Nullteiler hat, muss also $g(a) = 0$ oder $h(a) = 0$ sein. Damit hätten wir in jedem Fall ein

nicht-konstantes Polynom mit Nullstelle a, dessen Grad kleiner als der des Minimalpolynoms ist — was ein Widerspruch ist.

„⇐“ Es sei f irreduzibel und normiert mit $f(a) = 0$. Nach Bemerkung 2.5 ist f dann ein Vielfaches des Minimalpolynoms, also $f = g \cdot m_a$ für ein $g \in K[t]$. Da f aber irreduzibel ist, kann g nur eine Einheit in $K[t]$, also eine Konstante sein. Weil darüber hinaus sowohl f als auch m_a normiert sind, ist diese Konstante sogar gleich 1, und wir erhalten wie gewünscht $f = m_a$. □

Wenn wir dieses Lemma nun benutzen wollen, um Minimalpolynome zu bestimmen, benötigen wir natürlich noch gute Möglichkeiten, wie man einem Polynom ansehen kann, ob es irreduzibel ist oder nicht. Wir begnügen uns hier für den Moment mit dem folgenden einfachen Kriterium, das ihr vermutlich bereits aus den „Algebraischen Strukturen“ kennt — bessere Kriterien werden wir später noch in Kapitel 3 kennen lernen.

Aufgabe 2.7.

(a) Es sei K ein Körper. Zeige, dass ein Polynom $f \in K[t]$ vom Grad 2 oder 3 genau dann irreduzibel ist, wenn es keine Nullstelle hat.

(b) Zeige, dass das Kriterium aus (a) für jeden Grad größer als 3 falsch ist, d. h. gib für jedes $n \geq 4$ ein Beispiel an für einen Körper K sowie ein reduzibles Polynom $f \in K[t]$ vom Grad n ohne Nullstellen.

Aufgabe 2.8. Es sei p eine Primzahl. Wie viele irreduzible Polynome vom Grad 2 gibt es in $\mathbb{Z}_p[t]$?

Mit diesen Ergebnissen können wir nun ein paar Beispiele von Minimalpolynomen und Graden von Elementen konkret angeben.

Beispiel 2.9.

(a) Es sei L/K eine Körpererweiterung und $a \in L$. Offensichtlich ist $[a : K] = 1$ genau dann, wenn $a \in K$ ist — das Minimalpolynom ist in diesem Fall einfach $t - a \in K[t]$.

(b) Wir wollen den Grad von $a = \sqrt{2} \in \mathbb{R}$ über $\mathbb{Q}$ bestimmen. Natürlich ist $t^2 - 2$ ein normiertes rationales Polynom mit Nullstelle a. Da es offensichtlich keine Nullstellen in $\mathbb{Q}$ besitzt, ist es nach Aufgabe 2.7 (a) irreduzibel in $\mathbb{Q}[t]$ und damit nach Lemma 2.6 das Minimalpolynom von a über $\mathbb{Q}$. Damit ist $[\sqrt{2} : \mathbb{Q}] = 2$.

Beachte, dass es beim Minimalpolynom und Grad eines Elements auch entscheidend auf den Grundkörper ankommt: nach (a) ist z. B. $[\sqrt{2} : \mathbb{R}] = 1$ mit Minimalpolynom $m_{\sqrt{2},\mathbb{R}} = t - \sqrt{2}$.

(c) Analog zu (b) ist $t^3 - 2$ das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$, denn es ist ein normiertes Polynom über $\mathbb{Q}$ mit Nullstelle $\sqrt[3]{2}$, das keine Nullstellen in $\mathbb{Q}$ besitzt und damit wiederum nach Aufgabe 2.7 (a) in $\mathbb{Q}[t]$ irreduzibel ist. Also ist $[\sqrt[3]{2} : \mathbb{Q}] = 3$.

(d) Wir wollen das Minimalpolynom (und den Grad) von $a = e^{\frac{2\pi i}{6}}$ über $\mathbb{Q}$ bestimmen. Auch hier sehen wir sofort ein normiertes Polynom über $\mathbb{Q}$ mit Nullstelle a, nämlich $t^6 - 1$. Ist es das Minimalpolynom von a über $\mathbb{Q}$? Nein, denn es lässt sich offensichtlich als

$$t^6 - 1 = (t^3 - 1)(t^3 + 1)$$

faktorisieren, ist damit nicht irreduzibel in $\mathbb{Q}[t]$ und kann demzufolge nach Lemma 2.6 nicht das Minimalpolynom sein. In der Tat ist a ja eine Nullstelle dieses Produkts und muss damit eine Nullstelle von einem der Faktoren sein (dies ist genau das Argument der Richtung „⇒“ vom Beweis von Lemma 2.6). In unserem konkreten Fall ist $a^3 = e^{\pi i} = -1$ und damit a eine Nullstelle von $t^3 + 1$. Ist also $t^3 + 1$ das gesuchte Minimalpolynom? Auch dies ist nicht der Fall, denn $t^3 + 1$ hat noch die rationale Nullstelle -1, was zur weiteren Faktorisierung

$$t^3 + 1 = (t + 1)(t^2 - t + 1)$$

in $\mathbb{Q}[t]$ führt. Hier ist a offensichtlich keine Nullstelle von $t + 1$, also muss es eine von $t^2 - t + 1$ sein. Und dieses Polynom ist nun tatsächlich irreduzibel nach Aufgabe 2.7 (a), denn

es hat in $\mathbb{Q}$ keine Nullstellen mehr (wie eine einfache Berechnung der Nullstellen zeigt). Demnach ist das gesuchte Minimalpolynom $m_a = t^2 - t + 1$ nach Lemma 2.6, es ist also $[e^{\frac{2\pi i}{6}} : \mathbb{Q}] = 2$.

Wir sehen an diesem Beispiel schon, dass wir bei der Berechnung eines Minimalpolynoms aufpassen müssen — das Minimalpolynom eines Elements a ist nicht immer das „erstbeste" oder „einfachste" normierte Polynom mit Nullstelle a, das einem einfällt!

Als erste Anwendung des Gradkonzepts wollen wir nun eine sehr praktische Darstellung einfacher algebraischer Körpererweiterungen zeigen. Wir hatten ja bereits in Bemerkung 1.14 gesehen, dass sich die Elemente einer einfachen Körpererweiterung $K(a)$ immer als Quotienten von Polynomausdrücken in a mit Koeffizienten in K schreiben lassen. Diese explizite Darstellung von $K(a)$ ist jedoch recht kompliziert. Für den konkreten Fall der Körpererweiterung $\mathbb{Q}(\sqrt{2})$ haben wir in Beispiel 1.15 eine viel einfachere Darstellung gefunden, nämlich die Menge aller Ausdrücke der Form $a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$. Eine solche schöne Darstellung gibt es in der Tat für jede einfache algebraische Körpererweiterung:

Lemma 2.10 (Explizite Darstellung von einfachen algebraischen Körpererweiterungen)**.** *Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch vom Grad $n = [a : K]$. Dann gilt*

$$K(a) \quad = \quad \{f(a) : \ f \in K[t]\} \quad = \quad \{f(a) : \ f \in K[t] \text{ mit } \deg f < n\}.$$

Beweis. Nach Bemerkung 1.14 ist $K(a)$ gleich der Menge $M_0 = \left\{\frac{f(a)}{g(a)} : \ f, g \in K[t] \text{ mit } g(a) \neq 0\right\}$ aller rationalen Ausdrücke in a (mit Koeffizienten in K). Es seien nun $M_1 = \{f(a) : \ f \in K[t]\}$ die Menge aller Polynomausdrücke in a und $M_2 = \{f(a) : \ f \in K[t] \text{ mit } \deg f < n\}$ die Menge aller Polynomausdrücke in a vom Grad kleiner als n. Wir müssen zeigen, dass $M_0 = M_1 = M_2$.

$M_0 = M_1$: Die Inklusion „$\supset$" ist offensichtlich, da jeder Polynomausdruck auch ein rationaler Ausdruck ist. Für die Inklusion „$\subset$" sei $b \in M_0$, also $b = \frac{f(a)}{g(a)}$ für $f, g \in K[t]$ mit $g(a) \neq 0$. Wir wollen den größten gemeinsamen Teiler der Polynome g und m_a mit Hilfe ihrer Primfaktorzerlegungen bestimmen [G, Kapitel 11]. Da das Minimalpolynom m_a nach Lemma 2.6 irreduzibel und damit auch prim ist [G, Bemerkung 11.6], ist m_a selbst der einzige Primfaktor, der in beiden Primfaktorzerlegungen von g und m_a auftreten könnte. Aber m_a kann kein Primfaktor von g sein, da g sonst ein Vielfaches von m_a wäre und somit genau wie m_a den Wert a als Nullstelle haben müsste. Also sind g und m_a teilerfremd, und daher gibt es nach dem Lemma von Bézout Polynome $p, q \in K[t]$ mit $pg + qm_a = 1$ in $K[t]$ [G, Satz 10.13 (b)]. Einsetzen von a liefert dann $p(a)\,g(a) = 1$ in L wegen $m_a(a) = 0$, und wir erhalten wie gewünscht

$$b = \frac{f(a)}{g(a)} = f(a)\,p(a) \in M_1.$$

$M_1 = M_2$: Auch hier ist die Inklusion „$\supset$" wieder klar. Für die Inklusion „$\subset$" sei $b \in M_1$, also $b = f(a)$ für ein $f \in K[t]$. Division von f durch m_a mit Rest [G, Satz 10.19] liefert $f = qm_a + r$ für gewisse $q, r \in K[t]$ mit $\deg r < \deg m_a$. Wegen $m_a(a) = 0$ ist dann $b = f(a) = r(a) \in M_2$. □

Beispiel 2.11. Da $\sqrt{2}$ nach Beispiel 2.9 (b) Grad 2 über $\mathbb{Q}$ hat, ist $\mathbb{Q}(\sqrt{2})$ nach Lemma 2.10 die Menge aller höchstens linearen Polynomausdrücke in $\sqrt{2}$ mit Koeffizienten in $\mathbb{Q}$, also wie in Beispiel 1.15

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}.$$

Analog ergibt sich aus $[\sqrt[3]{2} : \mathbb{Q}] = 3$ (siehe Beispiel 2.9 (c))

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b, c \in \mathbb{Q}\}.$$

Diese Darstellung erinnert stark an Linearkombinationen, wie sie in der Linearen Algebra auftreten. In der Tat sieht man sofort, dass man in jeder Körpererweiterung L/K den großen Körper L als einen Vektorraum über dem kleinen Körper K auffassen kann: es gibt ja eine Addition in L (die Vektoraddition), und man kann Elemente von K mit Elementen von L multiplizieren (die Skalarmultiplikation), weil K in L liegt und es in L die Körpermultiplikation gibt. Natürlich folgt aus den Körperaxiomen

auch, dass für diese Vektoraddition und Skalarmultiplikation die für einen Vektorraum geforderten Rechenregeln gelten. Wir können daher definieren:

Definition 2.12 (Grad einer Körpererweiterung)**.** Es sei L/K eine Körpererweiterung. Die Dimension von L als K-Vektorraum wird der **Grad** von L/K genannt und als $[L:K]$ geschrieben. Offensichtlich ist $[L:K] \in \mathbb{N} \cup \{\infty\}$. Ist dieser Grad endlich, also L ein endlich-dimensionaler K-Vektorraum, so nennt man die Körpererweiterung L/K **endlich**.

Beispiel 2.13.

(a) Offensichtlich ist der Grad einer Körpererweiterung L/K genau dann gleich 1, wenn $L = K$ ist.

(b) Nach Beispiel 2.11 ist $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, denn $\{1, \sqrt{2}\}$ ist eine Basis von $\mathbb{Q}(\sqrt{2})$ als $\mathbb{Q}$-Vektorraum. Genauso ist natürlich $[\mathbb{C} : \mathbb{R}] = 2$, denn $\{1, i\}$ ist eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum.

(c) Es sei L/K eine transzendente Körpererweiterung. Dann gibt es ein Element $a \in L$, das transzendent über K ist. Dies bedeutet, dass die Menge $\{1, a, a^2, a^3, \dots\}$ linear unabhängig über K ist, da es ja sonst eine nicht-triviale Linearkombination $\sum_{i=0}^{n} \lambda_i a^i = 0$ mit $\lambda_0, \dots, \lambda_n \in K$ gäbe und a damit Nullstelle eines Polynoms mit Koeffizienten in K wäre. Also ist dann $[L:K] = \infty$.

Anders ausgedrückt bedeutet dies, dass jede endliche Körpererweiterung algebraisch ist. Die Umkehrung gilt hier jedoch nicht, wie wir in Aufgabe 3.11 (b) sehen werden.

Wir können unsere Ergebnisse von Lemma 2.10 und Beispiel 2.11 nun sofort auf den Begriff des Grades einer Körpererweiterung übertragen.

Satz 2.14. *Es seien L/K eine Körpererweiterung und $a \in L$. Dann gilt:*

(a) $[K(a) : K] = [a : K]$.

(b) *Ist a algebraisch vom Grad n über K, so ist $\{1, a, a^2, \dots, a^{n-1}\}$ eine Basis von $K(a)$ als K-Vektorraum.*

(c) *Ist a algebraisch über K, so ist auch $K(a)/K$ algebraisch, d. h. jedes Element von $K(a)$ ist algebraisch über K.*

Beweis. Ist a und damit auch $K(a)$ transzendent über K, so ist $[K(a) : K] = [a : K] = \infty$ nach Beispiel 2.13 (c).

Wir können nun also annehmen, dass a algebraisch vom Grad n über K ist. Nach Lemma 2.10 ist $K(a)$ dann die Menge aller Polynomausdrücke in a vom Grad kleiner als n mit Koeffizienten in K. Dies bedeutet genau, dass $\{1, a, a^2, \dots, a^{n-1}\}$ ein Erzeugendensystem von $K(a)$ als K-Vektorraum ist. In der Tat ist diese Familie auch linear unabhängig über K, denn andernfalls gäbe es ja eine nicht-triviale Linearkombination $\lambda_0 + \lambda_1 a + \dots + \lambda_{n-1} a^{n-1} = 0$ mit $\lambda_0, \dots, \lambda_{n-1} \in K$, d. h. a wäre im Widerspruch zur Definition des Grades eine Nullstelle eines Polynoms über K, dessen Grad kleiner als der des Minimalpolynoms ist. Dies zeigt (b), und damit auch (a).

Für (c) sei $b \in K(a)$ beliebig. Ist wieder $n = [a : K]$, so ist die Familie $\{1, b, b^2, \dots, b^n\}$ dann notwendigerweise linear abhängig über K, denn dies sind $n+1$ Elemente in dem nach (a) n-dimensionalen K-Vektorraum $K(a)$. Es muss also $\lambda_0, \dots, \lambda_n \in K$ geben, die nicht alle Null sind und für die $\lambda_0 + \lambda_1 b + \dots + \lambda_n b^n = 0$ gilt. Dies bedeutet aber genau, dass b algebraisch ist. □

Bemerkung 2.15. Für eine einfache Körpererweiterung $K(a)/K$ gilt also

$$a \text{ algebraisch} \quad \Leftrightarrow \quad K(a)/K \text{ algebraisch} \quad \Leftrightarrow \quad K(a)/K \text{ endlich}$$

(die Äquivalenz der ersten Aussage mit der zweiten ist Satz 2.14 (c), die der ersten mit der dritten Satz 2.14 (a)). Darüber hinaus ist in diesem Fall der Grad von a über K nach Satz 2.14 (a) gleich dem Grad der Körpererweiterung $K(a)$ über K. Die Begriffe „algebraisch“ und „Grad“, die wir sowohl für Elemente als auch für Körpererweiterungen definiert haben, passen in diesem Sinne also zusammen.

Beispiel 2.16. Es sei L/K eine einfache n-Radikalerweiterung, also $L = K(a)$ für ein $a \in L$ mit $a^n \in K$. Dann ist $t^n - a^n$ ein Polynom über K (und nicht nur über L!) mit Nullstelle a. Das Minimalpolynom von a hat also höchstens Grad n. Mit Satz 2.14 (a) folgt demnach $[L:K] = [a:K] \leq n$.

Um mit Graden von Körpererweiterungen rechnen zu können, benötigen wir den folgenden wichtigen Satz, der die Grade zweier „verketteter Körpererweiterungen" miteinander vergleicht.

Satz 2.17 (Gradformel). *Sind $K \leq Z \leq L$ Körper, so gilt $[L:K] = [L:Z] \cdot [Z:K]$.*

03

Beweis. Es seien $\{v_i : i \in I\}$ eine Basis von Z als K-Vektorraum und $\{w_j : j \in J\}$ eine Basis von L als Z-Vektorraum. Wir behaupten, dass $\{v_i \cdot w_j : i \in I, j \in J\}$ eine Basis von L als K-Vektorraum ist (woraus dann offensichtlich die Aussage des Satzes folgt).

Erzeugendensystem: Es sei $a \in L$ beliebig. Da die w_j ein Erzeugendensystem von L als Z-Vektorraum sind, gibt es $\lambda_j \in Z$ mit $a = \sum_j \lambda_j w_j$ (von denen nur endlich viele ungleich Null sind). Andererseits sind die v_i ein Erzeugendensystem von Z als K-Vektorraum, also gibt es auch $\mu_{i,j} \in K$ mit $\lambda_j = \sum_i \mu_{i,j} v_i$. Damit folgt $a = \sum_{i,j} \mu_{i,j} v_i w_j$, d. h. die Produkte $v_i w_j$ erzeugen L über K.

Lineare Unabhängigkeit: Es sei nun $\sum_{i,j} \lambda_{i,j} v_i w_j = 0$ für gewisse $\lambda_{i,j} \in K$ (von denen wieder nur endlich viele ungleich Null sind). Wir schreiben dies als $\sum_j (\sum_i \lambda_{i,j} v_i) w_j = 0$. Weil die Ausdrücke $\sum_i \lambda_{i,j} v_i$ in Z liegen und die w_j eine Basis von L als Z-Vektorraum sind, folgt $\sum_i \lambda_{i,j} v_i = 0$ für alle j. Da nun aber die $\lambda_{i,j}$ in K liegen und die v_i eine Basis von Z als K-Vektorraum sind, folgt sogar $\lambda_{i,j} = 0$ für alle i, j. Also sind die Produkte $v_i w_j$ linear unabhängig. □

Folgerung 2.18. *Es seien L/K eine endliche Körpererweiterung und $a \in L$. Dann ist $[a:K]$ (endlich und) ein Teiler von $[L:K]$.*

Beweis. Die Gradformel für $K \leq K(a) \leq L$ liefert $[L:K] = [L:K(a)] \cdot [K(a):K]$. Nach Satz 2.14 (a) ist nun $[K(a):K] = [a:K]$, also folgt die Behauptung. □

Aufgabe 2.19. Es seien L/K eine Körpererweiterung und $a, b \in L$ algebraisch über K.

(a) Man zeige: Sind $[a:K]$ und $[b:K]$ teilerfremd, so gilt $[K(a,b):K] = [a:K] \cdot [b:K]$.

(b) Bestimme $[K(a,b):K]$, $[a:K]$ und $[b:K]$ für den Fall $L = \mathbb{C}$, $K = \mathbb{Q}$, $a = \sqrt[3]{2}$ und $b = \sqrt[3]{2} e^{\frac{2\pi i}{3}}$.
(Hinweis: Man zeige und benutze $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2} e^{\frac{2\pi i}{3}}) = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$.)

Aufgabe 2.20. Bestimme die Minimalpolynome der folgenden reellen Zahlen über $\mathbb{Q}$:

(a) $a = \sqrt{2} + \sqrt{3}$;

(b) $a = \sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}$. (Was sagt euer Taschenrechner zu dieser Zahl?)

Aufgabe 2.21. Es sei L/K eine endliche Körpererweiterung. Man zeige:

(a) Ist $[L:K]$ eine Primzahl, so gilt $L = K(a)$ für jedes $a \in L \backslash K$. Insbesondere ist L/K dann also eine einfache Körpererweiterung.

(b) Ist $[L:K] = 2$ und $\operatorname{char} K \neq 2$, so ist L/K sogar eine einfache 2-Radikalerweiterung.

Wir wollen unsere Ergebnisse nun auf die Fragen nach der Konstruierbarkeit mit Zirkel und Lineal aus Problem 0.3 anwenden. Da wir in Beispiel 1.23 bereits gesehen hatten, dass wir dazu entscheiden müssen, ob gewisse Zahlen in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegen, müssen wir uns dazu also anschauen, was die Gradformel über 2-Radikalerweiterungen aussagt.

Folgerung 2.22. *Es sei L/K eine 2-Radikalerweiterung. Dann gilt:*

(a) *$[L:K]$ ist (endlich und) eine Zweierpotenz.*

(b) *Für alle $a \in L$ ist $[a:K]$ (endlich und) eine Zweierpotenz.*

Beweis.

(a) Nach Definition 1.18 einer 2-Radikalerweiterung gibt es eine Körperkette

$$K = K_0 \leq K_1 \leq \cdots \leq K_n = L,$$

in der jede Erweiterung K_i/K_{i-1} eine einfache 2-Radikalerweiterung ist, nach Beispiel 2.16 also Grad 1 oder 2 hat. Mit der Gradformel folgt damit

$$[L:K] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot \cdots \cdot [K_1 : K_0] = 2^m,$$

wobei m die Anzahl der $i = 1, \ldots, n$ ist mit $[K_i : K_{i-1}] = 2$.

(b) ergibt sich mit Folgerung 2.18 unmittelbar aus (a), da jeder Teiler einer Zweierpotenz wieder eine Zweierpotenz ist. □

Beispiel 2.23 (Anwendung auf Konstruktionen mit Zirkel und Lineal)**.**

(A) (Quadratur des Kreises) Wir hatten in Beispiel 2.2 (c) bereits erwähnt, dass π transzendent über $\mathbb{Q}$ ist (was in dieser Vorlesung nicht bewiesen werden soll). Da demnach $[\pi : \mathbb{Q}] = \infty$ gilt, kann π nach Folgerung 2.22 (b) also in keiner 2-Radikalerweiterung von $\mathbb{Q}$ liegen. Aus Beispiel 1.23 wissen wir bereits, dass dies bedeutet, dass die Quadratur des Kreises mit Zirkel und Lineal nicht möglich ist.

(B) (Würfelverdoppelung) Analog zu (A) ist auch $[\sqrt[3]{2} : \mathbb{Q}] = 3$ nach Beispiel 2.9 (c) keine Zweierpotenz. Also kann auch $\sqrt[3]{2}$ nach Folgerung in keiner 2-Radikalerweiterung von $\mathbb{Q}$ liegen, womit sich wiederum aus Beispiel 1.23 ergibt, dass auch die Würfelverdoppelung mit Zirkel und Lineal unmöglich ist.

(C) (Konstruktion des n-Ecks) Um mit unseren bisherigen Ergebnissen Aussagen über die Konstruierbarkeit des regelmäßigen n-Ecks machen zu können, müssten wir nach Beispiel 1.23 den Grad $[e^{\frac{2\pi i}{n}} : \mathbb{Q}]$ bestimmen und überprüfen, für welche n er eine Zweierpotenz ist. Wir haben jedoch in Beispiel 2.9 (d) bereits gesehen, dass dieser Grad nicht so einfach zu berechnen ist. Erst im nächsten Kapitel werden wir in Satz 3.27 (b) und 3.29 in der Lage sein, das Minimalpolynom und damit den Grad von $e^{\frac{2\pi i}{n}}$ über $\mathbb{Q}$ zu bestimmen.

Bemerkung 2.24. Beachte, dass Folgerung 2.22 nur eine *notwendige* Bedingung für die Konstruierbarkeit mit Zirkel und Lineal liefert: der Grad der zu konstruierenden Zahl über $\mathbb{Q}$ muss eine Zweierpotenz sein. Die Umkehrung gilt im Allgemeinen nicht — nicht jede Körpererweiterung, deren Grad eine Zweierpotenz ist, ist eine 2-Radikalerweiterung. Haben wir also eine Zahl, deren Grad über $\mathbb{Q}$ eine Zweierpotenz ist (und dies wird bei manchen Zahlen der Form $e^{\frac{2\pi i}{n}}$ aus Beispiel 2.23 (C) vorkommen), so können wir mit den bisherigen Methoden noch keine Aussage über die Konstruierbarkeit dieser Zahl machen. Dies wird erst später mit Hilfe der Galoistheorie möglich sein (siehe Folgerung 7.8).

Aufgabe 2.25. Diese Aufgabe soll zeigen, wie das Minimalpolynom aus Definition 2.4 (a) mit dem aus den „Grundlagen der Mathematik“ bekannten Minimalpolynom von Matrizen zusammenhängt.

Es seien dazu L/K eine Körpererweiterung und $a \in L$ algebraisch vom Grad n mit Minimalpolynom m_a.

Nach Satz 2.14 (b) ist $K(a)$ ein n-dimensionaler K-Vektorraum mit Basis $B = \{1, a, a^2, \ldots, a^{n-1}\}$. Weiterhin ist $f : K(a) \to K(a)$, $x \mapsto ax$ offensichtlich eine lineare Abbildung.

Bestimme (im Sinne der „Grundlagen der Mathematik“) die Abbildungsmatrix von f bezüglich B sowie das charakteristische Polynom, das Minimalpolynom und alle Eigenwerte dieser Matrix.

(Hinweis: Dies ist eine Nachdenkaufgabe und keine Rechenaufgabe; wenn man sie geschickt angeht, hat sie eine sehr kurze Lösung! Ergebnisse aus den „Grundlagen der Mathematik“ dürfen natürlich verwendet werden.)

Aufgabe 2.26 (Unmöglichkeit der Winkeldreiteilung mit Zirkel und Lineal)**.** Neben den Konstruktionsaufgaben aus Problem 0.3 ist auch die sogenannte **Winkeldreiteilung** ein klassisches Problem,

d. h. die Fragestellung, ob und wie man zu einem gegebenen Winkel φ in der Zeichenebene mit Zirkel und Lineal einen Winkel der Größe $\frac{\varphi}{3}$ konstruieren kann. Wir wollen in dieser Aufgabe sehen, dass diese Winkeldreiteilung im Allgemeinen nicht möglich ist.

Dazu seien in der Zeichenebene die Punkte $M = \{0, 1, e^{i\varphi}\}$, d. h. ein Winkel der Größe φ, gegeben. Man zeige:

(a) Die Dreiteilung des Winkels φ ist mit Zirkel und Lineal genau dann durchführbar, wenn die Lösungen der kubischen Gleichung $4t^3 - 3t = \cos\varphi$ in einer 2-Radikalerweiterung von $\mathbb{Q}(e^{i\varphi})$ liegen.

(b) Die kubische Gleichung $4t^3 - 3t = \frac{1}{3}$ hat keine rationalen Lösungen. *(Hinweis: Mache den Ansatz $t = \frac{p}{q}$ mit teilerfremden $p, q \in \mathbb{Z}$, $q \neq 0$, und führe diese Annahme zu einem Widerspruch.)*

(c) Die Dreiteilung des Winkels $\varphi = \arccos\frac{1}{3}$ ist mit Zirkel und Lineal nicht durchführbar.

Aufgabe 2.27. Es sei L/K eine Körpererweiterung. Man zeige:

(a) Ist $M \subset L$ eine Menge algebraischer Elemente über K, so ist die Körpererweiterung $K(M)/K$ algebraisch.

(b) Sind $a_1, \ldots, a_n \in L$ endlich viele algebraische Elemente über K, so ist die Körpererweiterung $K(a_1, \ldots, a_n)/K$ sogar endlich.

(c) Ist Z ein Körper mit $K \leq Z \leq L$ und sind die Erweiterungen L/Z und Z/K algebraisch, so auch L/K.