4. Zerfällungskörper

In den bisherigen Kapiteln der Vorlesung haben wir sehr ausführlich einfache algebraische Körpererweiterungen behandelt. In der Regel hatten wir dazu eine Körpererweiterung L/K mit einem über K algebraischen Element $a \in L$, und haben dann den Körper $K(a)$ mit Hilfe des Minimalpolynoms von a studiert, also mit dem eindeutig bestimmten normierten irreduziblen Polynom $f \in K[t]$ mit Nullstelle a

Wir wollen in diesem Kapitel nun in gewissem Sinne den umgekehrten Weg gehen und uns fragen: haben wir einen Körper K und ein irreduzibles Polynom $f \in K[t]$, finden wir dann immer einen Erweiterungskörper L von K, in dem f eine Nullstelle $a \in L$ besitzt? Oder vielleicht sogar einen Erweiterungskörper, in dem f komplett in Linearfaktoren zerfällt?

Eine solche Frage ist sehr natürlich und tritt z. B. bei der Konstruktion der komplexen Zahlen auf. Versetzt euch doch einmal in die Zeit zurück, als ihr den Körper der komplexen Zahlen noch nicht kanntet. Ihr stellt fest, dass man in $\mathbb{R}$ aus -1 keine Wurzel ziehen kann, dass eine solche Wurzel für viele Anwendungen aber sehr nützlich wäre. Ihr würdet also gerne von $\mathbb{R}$ zu einem größeren Körper übergehen, in dem eine Wurzel aus -1 existiert, d. h. in dem das Polynom t^2+1 eine Nullstelle besitzt. Aber gibt es so etwas überhaupt? Typischerweise fällt die Antwort auf diese Frage in Form des Körpers $\mathbb{C}$ dann in der Schule oder in den „Grundlagen der Mathematik“ irgendwann vom Himmel; man definiert $\mathbb{C}$ dort in der Regel zunächst als $\mathbb{R}^2$ mit einer recht unmotiviert aussehenden Multiplikation und beweist erst einmal, dass man so einen Erweiterungskörper von $\mathbb{R}$ erhält. Und im Nachhinein stellt man dann irgendwann fest, dass dieser Erweiterungskörper auch „zufällig“ das Problem der Wurzel aus -1 löst – aus der Konstruktion von $\mathbb{C}$ war das aber sicher nicht offensichtlich.

Wir wollen dieses Problem nun systematisch angehen und sehen, wie man ganz gezielt zu einem gegebenen Polynom über einem Körper immer einen Erweiterungskörper finden kann, in dem das Polynom eine Nullstelle hat oder sogar in Linearfaktoren zerfällt. Wir betrachten zunächst einmal den einfacheren Fall einer einzelnen Nullstelle und definieren uns einen Begriff für das, was wir suchen.

Definition 4.1 (Stammkörper)**.** Es sei $f \in K[t]$ ein irreduzibles Polynom über einem Körper K. Ein Erweiterungskörper L von K heißt **Stammkörper** von f (über K), wenn es ein $a \in L$ gibt mit $f(a) = 0$ und $L = K(a)$.

Bemerkung 4.2.

(a) Kennen wir bereits einen Erweiterungskörper Z von K, in dem f eine Nullstelle a besitzt, so ist $L = K(a) \leq Z$ offensichtlich ein Stammkörper von f.

(b) Die Bedingung $L = K(a)$ in Definition 4.1 können wir als eine Art Minimalitätsforderung auffassen: wir wollen zu K nur die gewünschte Nullstelle a und nicht noch weitere unnötige Elemente adjungieren. Dies wird in Bemerkung 4.9 dafür sorgen, dass der Stammkörper eines Polynoms (bis auf Isomorphie) eindeutig bestimmt ist.

(c) Ist L ein Stammkörper von $f \in K[t]$ und a wie in Definition 4.1, so ist f nach Lemma 2.6 bis auf einen konstanten Faktor das Minimalpolynom von a. Insbesondere gilt also

$$[L : K] = [K(a) : K] = [a : K] = \deg f$$

nach der Voraussetzung $L = K(a)$ und Satz 2.14 (a). Wir sehen also bereits, dass alle Stammkörper von f denselben Grad über K haben müssen.

Beispiel 4.3.

(a) Betrachten wir das Polynom $f = t^2 + 1 \in \mathbb{R}[t]$ und gehen wir davon aus, dass wir den Körper $\mathbb{C}$ der komplexen Zahlen bereits kennen, so ist $\mathbb{R}(i) = \mathbb{C}$ nach Bemerkung 4.2 (a) ein Stammkörper von f über $\mathbb{R}$. Genauso ist $\mathbb{Q}(\sqrt{2}) \leq \mathbb{R}$ ein Stammkörper von $t^2 - 2$ über $\mathbb{Q}$.

(b) Es sei $K = \mathbb{Z}_2$. Da das Polynom $t^2 + t + 1 \in \mathbb{Z}_2[t]$ offensichtlich keine Nullstelle in $\mathbb{Z}_2$ hat, ist es nach Aufgabe 2.7 (a) irreduzibel. In diesem Fall kennen wir momentan noch keinen Stammkörper von f – schon allein deswegen, weil wir bisher noch überhaupt keinen Erweiterungskörper von $\mathbb{Z}_2$ kennen.

Wir wollen nun sehen, wie man zu einem gegebenen irreduziblen Polynom mit Hilfe von Faktorringen von Polynomringen stets einen Stammkörper konstruieren kann. Ist $f \in K[t]$ ein Polynom, so bezeichne dazu wie üblich $(f) = \{af : a \in K[t]\}$ das von f erzeugte Ideal in $K[t]$ und $K[t]/(f)$ den zugehörigen Faktorring [G, Beispiel 8.8 (a) und Satz 8.10].

Lemma 4.4 (Existenz von Stammkörpern)**.** *Es sei $f \in K[t]$ ein nicht-konstantes Polynom über einem Körper K. Dann gilt:*

(a) *Der Ring $K[t]/(f)$ ist genau dann ein Körper, wenn f irreduzibel ist.*

(b) *Ist f irreduzibel, so ist $L = K[t]/(f)$ ein Stammkörper von f; in ihm ist $\bar{t}$ ein Element mit $f(\bar{t}) = 0$ und $L = K(\bar{t})$.*

Beweis.

(a) „⇒“: Angenommen, f wäre reduzibel, d. h. es wäre $f = g \cdot h$ für nicht-konstante Polynome $g, h \in K[t]$. Im Faktorring $K[t]/(f)$ wäre dann $\overline{g} \cdot \overline{h} = \overline{f} = \overline{0}$, während $\overline{g}$ und $\overline{h}$ ungleich $\overline{0}$ sind, da g und h offensichtlich keine Vielfachen von f sind. Also besitzt $K[t]/(f)$ nicht-triviale Nullteiler und kann damit kein Körper sein [G, Lemma 7.8 (c)].

„⇐“: Es sei nun f irreduzibel. Da $K[t]/(f)$ in jedem Fall bereits ein Ring ist, bleibt nur noch zu zeigen, dass jedes Element $\overline{g} \neq \overline{0}$ in $K[t]/(f)$ ein multiplikatives Inverses besitzt. Beachte dazu, dass f und g in $K[t]$ teilerfremd sind: Da f nach Voraussetzung irreduzibel und damit prim ist [G, Bemerkung 11.6], könnte ohnehin nur f selbst der einzige gemeinsame Primfaktor von f und g sein – aber dann wäre g ein Vielfaches von f und damit $\overline{g} = \overline{0}$ in $K[t]/(f)$. Nach dem Lemma von Bézout [G, Satz 10.13 (b)] gibt es also Polynome p und q mit $pf + qg = 1$ in $K[t]$, d. h. $\overline{q} \cdot \overline{g} = \overline{1}$ in $K[t]/(f)$. Damit besitzt $\overline{g}$ wie gewünscht ein multiplikatives Inverses $\overline{q}$ in $K[t]/(f)$.

(b) Nach (a) ist L ein Körper. Der offensichtliche Morphismus $K \to L$, $a \mapsto \overline{a}$ ist nach Bemerkung 1.3 (b) injektiv und macht L damit zu einem Erweiterungskörper von K. Weiterhin gilt nach Konstruktion natürlich $f(\bar{t}) = \overline{f} = \overline{0} \in L$. Darüber hinaus erzeugen K und t zusammen den Polynomring $K[t]$ und damit auch $L = K[t]/(f)$, d. h. es ist $L = K(\bar{t})$. □

Beispiel 4.5. Wir betrachten noch einmal den Körper $K = \mathbb{Z}_2$ mit dem irreduziblen Polynom $f = t^2 + t + 1 \in \mathbb{Z}_2[t]$ aus Beispiel 4.3 (b). Nach Lemma 4.4 (b) ist dann $L := \mathbb{Z}_2[a]/(a^2 + a + 1)$ ein Stammkörper von f, in dem $\overline{a}$ eine Nullstelle von f ist. Beachte, dass wir hier im Polynomring eine andere formale Variable a als sonst üblich gewählt haben, damit gleich keine Verwirrung auftritt, wenn wir auch Polynome über L betrachten, die wir dann wieder mit der formalen Variablen t schreiben wollen: im Polynomring $L[t]$ über dem Koeffizientenkörper $L = \mathbb{Z}_2[a]/(a^2 + a + 1)$ ist $\overline{a}$ nun eine Konstante und kein lineares Polynom!

Wenn $\overline{a}$ eine Nullstelle von f über L ist, muss man diese natürlich abspalten und f damit über L als Produkt von zwei linearen Faktoren schreiben können. In der Tat zeigt eine einfache Rechnung in

$L[t]$, dass

$$\begin{aligned}(t-\overline{a})\,(t-\overline{a}-\overline{1}) &= t^2-(\overline{2}\cdot\overline{a}+\overline{1})t+\overline{a^2+a}\\ &= t^2-(\overline{2}\cdot\overline{a}+\overline{1})t-\overline{1} && (\overline{a^2+a+1}=\overline{0}\text{ in }L)\\ &= t^2+t+\overline{1} && (\operatorname{char}L=\operatorname{char}K=2\text{ nach Beispiel 1.7 (b)})\\ &= f.\end{aligned}$$

Damit zerfällt f also in der Tat über L in Linearfaktoren; die Nullstellen von f in L sind $\overline{a}$ und $\overline{a}+\overline{1}$.

Bemerkung 4.6. Bei Rechnungen in Stammkörpern der Form $L=K[t]/(f)$ wie in Lemma 4.4 lässt man in der Notation oft die Querstriche zur Bezeichnung der Restklassen im Faktorring weg, wenn dies nicht zu Verwirrungen führen kann. In Beispiel 4.5 wären mit dieser Konvention also alle Querstriche überflüssig, und a (statt $\overline{a}$) wäre dort dann ein Element in dem Erweiterungskörper L mit $a^2+a+1=0$ (statt $\overline{a^2+a+1}=\overline{0}$). Dies macht die Formeln einfacher lesbar und kann auch durch die Tatsache motiviert werden, dass wir ja K als Unterkörper von L identifizieren wollen und es dann merkwürdig wäre, Elemente von K ohne und solche von L mit Querstrich zu schreiben.

Aufgabe 4.7. In dieser Aufgabe wollen wir eine Verallgemeinerung der Aussage aus Lemma 4.4 (a) herleiten, die allgemein die Frage beantwortet, wann ein Faktorring R/I sogar ein Körper ist.

Dazu heiße ein Ideal $I\neq R$ in einem Ring R ein **maximales Ideal**, wenn für jedes Ideal $J\supsetneq I$ bereits folgt, dass $J=R$. Man zeige:

(a) Der Ring R/I ist genau dann ein Körper, wenn I ein maximales Ideal ist.

(b) Ist R ein Hauptidealring, so ist ein Ideal $I=(a)$ für eine Nichteinheit $a\neq 0$ genau dann ein maximales Ideal, wenn a irreduzibel ist.

Im Fall des Polynomrings $R=K[t]$ über einem Körper K ergibt sich aus (a) und (b) offensichtlich genau Lemma 4.4 (a). Welche euch bereits bekannte Aussage ergibt sich im Fall $R=\mathbb{Z}$?

Nach der Existenz von Stammkörpern wollen wir nun auch deren Eindeutigkeit (bis auf Isomorphie) zeigen. Wir beweisen dazu eine etwas allgemeinere Aussage, die wir später noch mehrfach benötigen werden.

Lemma 4.8 (Eindeutigkeit von Stammkörpern)**.** *Es seien $\sigma: K\to K'$ ein Körperisomorphismus, $f\in K[t]$ ein irreduzibles Polynom über K und $f'=\sigma(f)\in K'[t]$ das zugehörige Polynom über K'. Ferner seien $L=K(a)$ ein Stammkörper von f über K mit $f(a)=0$ und $L'=K'(a')$ ein Stammkörper von f' über K' mit $f'(a')=0$.*

Dann gibt es genau einen Körperisomorphismus $\tau: L\to L'$ mit $\tau|_K=\sigma$ und $\tau(a)=a'$.

$$\begin{array}{ccc} L=K(a) & \overset{\tau}{\dashrightarrow} & L'=K'(a') \\ \vee\mid & & \vee\mid \\ K & \xrightarrow{\ \sigma\ } & K' \end{array}$$

Beweis. Die Eindeutigkeit von τ sieht man schnell ein: jedes Element von $L=K(a)$ lässt sich nach Lemma 2.10 als Polynom $\sum_n \lambda_n a^n$ mit Koeffizienten in K schreiben. Da τ ein Körperhomomorphismus ist und auf K sowie a durch $\tau|_K=\sigma$ und $\tau(a)=a'$ festgelegt ist, muss ein solches Element von τ zwangsläufig auf

$$\tau\Big(\sum_n \lambda_n a^n\Big)=\sum_n \tau(\lambda_n)\,\tau(a)^n=\sum_n \sigma(\lambda_n)\,(a')^n$$

abgebildet werden. Damit ist τ also eindeutig festgelegt, d. h. es kann höchstens einen Körperhomomorphismus mit den geforderten Eigenschaften geben.

Für die Existenz von τ betrachten wir den Ringhomomorphismus $F: K[t]\to L$, $g\mapsto g(a)$. Wiederum nach Lemma 2.10 ist F surjektiv; der Kern hingegen ist

$$\operatorname{Ker}F=\{g\in K[t]: g(a)=0\}=(f)$$

nach Bemerkung 2.5, da f wegen Bemerkung 4.2 (c) bis auf einen konstanten Faktor das Minimalpolynom von a ist. Nach dem Homomorphiesatz [G, Satz 8.12] ist die Abbildung

$$G : K[t]/(f) \to L, \quad \overline{g} \mapsto g(a)$$

also ein Körperisomorphismus; offensichtlich bildet er $\overline{t}$ auf a und Elemente von $K \leq K[t]/(f)$ auf sich selbst ab. Genauso gibt es auf der anderen Seite einen Körperisomorphismus $G' : K'[t]/(f') \to L'$ mit $G'(\overline{t}) = a'$ und $G'|_{K'} = \mathrm{id}$. Die Verkettung τ der drei Isomorphismen

$$K(a) \xrightarrow{G^{-1}} K[t]/(f) \longrightarrow K'[t]/(f') \xrightarrow{G'} K'(a')$$

hat dann die gewünschten Eigenschaften, wobei der mittlere Isomorphismus einfach die Abbildung $\overline{g} \mapsto \overline{\sigma(g)}$ ist, die ein Polynom über K mit σ in ein Polynom über K' umwandelt. □

Bemerkung 4.9. Der wichtigste Fall von Lemma 4.8 ist der, in dem σ die Identität, also $K = K'$ und $f = f'$ ist. Das Lemma besagt dann, dass es zu zwei beliebigen Stammkörpern $L = K(a)$ und $L' = K(a')$ eines irreduziblen Polynoms $f \in K[t]$ immer einen Isomorphismus $\tau : K(a) \to K(a')$ gibt mit $\tau|_K = \mathrm{id}$ und $\tau(a) = a'$. Der Stammkörper eines Polynoms ist also bis auf Isomorphie eindeutig bestimmt; wir können damit in Zukunft von *dem* Stammkörper anstatt von *einem* Stammkörper von f sprechen. In der Tat haben wir sogar etwas mehr gesehen, nämlich dass es einen Isomorphismus zwischen den Stammkörpern gibt, *der auf dem Ursprungskörper K die Identität ist*. Man sagt dafür auch, dass die Stammkörper **K-isomorph** bzw. **isomorph über** K sind.

Beispiel 4.10.

(a) Wir betrachten in Lemma 4.8 (bzw. Bemerkung 4.9) den Fall $K = K' = \mathbb{R}$ mit $\sigma = \mathrm{id}$ und $f = f' = t^2 + 1$. Nach Beispiel 4.3 (a) ist $L = L' = \mathbb{C}$ dann ein Stammkörper von f. Allerdings hat f die zwei Nullstellen i und $-i$, und damit können wir im Lemma $a = i$ und $a' = -i$ wählen. Wir erhalten so die Aussage, dass es genau einen Körperisomorphismus $\tau : \mathbb{C} \to \mathbb{C}$ mit $\tau|_{\mathbb{R}} = \mathrm{id}$ und $\tau(i) = -i$ gibt. Diesen Körperisomorphismus kennt ihr natürlich bereits: es ist einfach die komplexe Konjugation $\tau(z) = \overline{z}$.

(b) Es sei $f = t^3 - 2 \in \mathbb{Q}[t]$. Drei Stammkörper von f sind dann z. B.

(i) $\mathbb{Q}(\sqrt[3]{2})$ (als Teilkörper von $\mathbb{R}$) nach Bemerkung 4.2 (a);

(ii) $\mathbb{Q}\left(\sqrt[3]{2}e^{\frac{2\pi i}{3}}\right)$ (als Teilkörper von $\mathbb{C}$) mit demselben Argument;

(iii) $\mathbb{Q}[t]/(t^3 - 2)$ nach Lemma 4.4 (b).

Diese drei Körper sehen zunächst alle verschieden aus: (i) und (ii) sind verschiedene Teilkörper von $\mathbb{C}$ (da (i) nur reelle Zahlen enthält, (ii) jedoch nicht), und der Körper (iii) ist ohnehin auf eine ganz andere Art definiert. Dennoch sagt Bemerkung 4.9, dass diese drei Körper als Stammkörper von f isomorph über $\mathbb{Q}$ sind.

Die algebraische Art, sich diese Aussage vorzustellen, ist einfach, dass es sich in allen drei Fällen um den Körper handelt, der aus $\mathbb{Q}$ entsteht, indem man ein Element adjungiert, dessen dritte Potenz gleich 2 ist. Wo dieses Element herkommt, spielt dabei keine Rolle – es kann ein konkretes Element in einem schon bekannten Erweiterungskörper von $\mathbb{Q}$ sein (wie $\sqrt[3]{2} \in \mathbb{R}$ oder $\sqrt[3]{2}e^{\frac{2\pi i}{3}} \in \mathbb{C}$ in (i) bzw. (ii)), oder einfach ein formales Element t wie in (iii), von dem man durch Übergang zu einem geeigneten Faktorring einfach verlangt, dass $t^3 - 2 = 0$ gilt.

Bemerkung 4.11 (Konstruktion von $\mathbb{C}$ aus $\mathbb{R}$)**.** Mit unserem Wissen über Stammkörper wollen wir noch einmal das Problem aus der Einleitung dieses Kapitels betrachten, wie man aus dem Körper $\mathbb{R}$ der reellen Zahlen den Körper $\mathbb{C}$ der komplexen Zahlen konstruieren kann, ohne dass die Definition von $\mathbb{C}$ dabei vom Himmel fällt und man erst im Nachhinein überprüfen muss, dass sie wirklich das Gewünschte leistet, nämlich eine Wurzel aus -1 einführt.

Wenn man in ingenieurswissenschaftliche Bücher schaut, werden die komplexen Zahlen dort oft so eingeführt: man nehme einfach an, dass es ein Element i mit $i^2 = -1$ gibt, und rechne damit dann ganz normal weiter, als wäre nichts Besonderes passiert. Als angehende Mathematiker würdet ihr dazu nun vermutlich sagen, dass das so nicht geht: wenn man bisher nur die reellen Zahlen kennt,

ist $i^2 = -1$ einfach nur eine widersprüchliche und damit unerlaubte Annahme und keinesfalls eine Definition. Das stimmt natürlich eigentlich auch, und daher definiert man die komplexen Zahlen in den „Grundlagen der Mathematik“ ja auch nicht so.

Der Algebraiker hingegen sieht die Sache etwas anders und kann die Sichtweise der Ingenieure zu einer mathematisch korrekten Definition $\mathbb{C} := \mathbb{R}[i]/(i^2+1)$ machen – denn dies ist haargenau die Übersetzung ins Algebraische der Idee „man nehme zu $\mathbb{R}$ ein formales Element i hinzu, für das $i^2 = -1$ gelte, und rechne damit ganz normal (mit den Körperaxiomen) weiter“. Und in der Tat wissen wir ja jetzt auch, dass wir auf diese Art exakt die üblichen komplexen Zahlen erhalten: denn $\mathbb{R}[i]/(i^2+1)$ ist nach Lemma 4.4 (b) ein Stammkörper des Polynoms t^2+1, der zum Stammkörper $\mathbb{C}$ (siehe Beispiel 4.3 (a)) nach Bemerkung 4.9 isomorph ist.

06

Wir wollen die Idee von Stammkörpern nun dahingehend ausweiten, dass wir Erweiterungskörper suchen, in denen ein gegebenes Polynom nicht nur eine Nullstelle hat, sondern sogar komplett in Linearfaktoren zerfällt. Die Definition, die in diesem Sinne Definition 4.1 entspricht, ist die folgende.

Definition 4.12 (Zerfällungskörper)**.** Es sei $f \in K[t]$ mit $f \neq 0$ ein Polynom über einem Körper K. Ein Erweiterungskörper L von K heißt **Zerfällungskörper** von f (über K), wenn es $\lambda \in K$ und $a_1, \ldots, a_n \in L$ gibt mit

$$f = \lambda\,(t-a_1)\cdot\cdots\cdot(t-a_n) \in L[t] \quad \text{und} \quad L = K(a_1,\ldots,a_n).$$

Bemerkung 4.13. Die folgenden beiden Eigenschaften sind völlig analog zu denen von Stammkörpern in Bemerkung 4.2:

(a) Kennen wir bereits einen Erweiterungskörper Z von K, in dem f in Linearfaktoren zerfällt, also $f = \lambda\,(t-a_1)\cdot\cdots\cdot(t-a_n)$ mit $\lambda \in K$ und $a_1,\ldots,a_n \in Z$ gilt, so ist $L = K(a_1,\ldots,a_n) \leq Z$ offensichtlich ein Zerfällungskörper von f über K. Dies ist z. B. in der Regel der Fall, wenn $K = \mathbb{Q}$ ist und wir eine Zerlegung in Linearfaktoren über $Z = \mathbb{C}$ hinschreiben können.

(b) Die Bedingung $L = K(a_1,\ldots,a_n)$ in Definition 4.12 ist eine Art Minimalitätsforderung, die besagt, dass wir zu K nicht noch mehr Elemente adjungieren wollen, als wir für die Zerlegung in Linearfaktoren unbedingt benötigen. Wie schon bei den Stammkörpern wird dies in Satz 4.16 zur Eindeutigkeit von Zerfällungskörpern führen.

Beispiel 4.14.

(a) Das Polynom $f = t^3 - 2 \in \mathbb{Q}[t]$ hat offensichtlich die komplexen Nullstellen $\sqrt[3]{2}\cdot e^{\frac{2\pi i k}{3}}$ für $k = 0,1,2$. Nach Bemerkung 4.13 (a) ist also

$$\mathbb{Q}\big(\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{4\pi i}{3}}\big) = \mathbb{Q}\big(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\big) \leq \mathbb{C}$$

ein Zerfällungskörper von f über $\mathbb{Q}$.

(b) Es sei $f \in K[t]$ ein irreduzibles Polynom vom Grad 2 und L sein Stammkörper. Da f in L eine Nullstelle hat und diese dann natürlich als Linearfaktor abspaltet, zerfällt f damit in L auch bereits in Linearfaktoren. Für irreduzible quadratische Polynome fallen die Begriffe Stammkörper und Zerfällungskörper also zusammen. So ist z. B. für das in Beispiel 4.5 betrachteten Polynom $f = t^2+t+1 \in \mathbb{Z}_2[t]$ sein Stammkörper $L = \mathbb{Z}_2[a]/(a^2+a+1)$ auch bereits ein Zerfällungskörper.

Für Polynome höheren Grades ist dies natürlich nicht so – hier kann man im Stammkörper zwar eine oder evtl. auch mehrere Nullstellen abspalten, aber es bleibt in der Regel noch ein Restpolynom übrig, auf das man die Stammkörperkonstruktion rekursiv erneut anwenden muss, bis schließlich das gesamte Polynom in Linearfaktoren zerfällt. Auf diese Art kann man dann wie im folgenden Satz zu jedem Polynom einen Zerfällungskörper konstruieren.

Satz 4.15 (Existenz von Zerfällungskörpern)**.** *Es seien K ein Körper und $f \in K[t]$ ein Polynom mit $f \neq 0$ und $n = \deg f$. Dann besitzt f einen Zerfällungskörper vom Grad höchstens $n!$.*

Beweis. Wir zeigen die Aussage mit Induktion über n; für $n = 0$ ist K selbst offensichtlich ein Zerfällungskörper von f.

Für den Induktionsschritt sei nun f ein Polynom vom Grad n. Wir wählen einen irreduziblen Faktor g von f; in seinem Stammkörper $L = K(a)$ ist a dann eine Nullstelle von g und damit auch von f. Beachte, dass $[L:K] = \deg g \leq \deg f = n$ nach Bemerkung 4.2 (c).

In L spaltet f also die Nullstelle a ab, d. h. wir können $f = (t-a)h$ für ein $h \in L[t]$ mit $\deg h = n-1$ schreiben. Nach Induktionsvoraussetzung besitzt h nun einen Zerfällungskörper Z über L, d. h. es ist $h = \lambda(t-a_2) \cdot \cdots \cdot (t-a_n)$ für gewisse $\lambda \in K$ und $a_2, \ldots, a_n \in Z$ mit $Z = L(a_2, \ldots, a_n)$ und $[Z:L] \leq (n-1)!$. Damit ist aber $f = \lambda(t-a)(t-a_2) \cdot \cdots \cdot (t-a_n) \in Z[t]$, d. h. $Z = L(a_2, \ldots, a_n) = K(a, a_2, \ldots, a_n)$ ist ein Zerfällungskörper von f über K. Nach der Gradformel aus Satz 2.17 gilt ferner wie behauptet $[Z:K] = [Z:L] \cdot [L:K] \leq (n-1)! \cdot n = n!$. □

Genau wie bei Stammkörpern wollen wir nun auch für Zerfällungskörper noch ihre Eindeutigkeit zeigen. Ganz analog zum Beweis ihrer Existenz in Satz 4.15 zeigt man auch diese Eindeutigkeit rekursiv aus der entsprechenden Aussage über Stammkörper in Lemma 4.8.

Satz 4.16 (Eindeutigkeit von Zerfällungskörpern)**.** *Es seien $\sigma : K \to K'$ ein Körperisomorphismus, $f \in K[t]$ ein Polynom mit $f \neq 0$ und $f' = \sigma(f) \in K'[t]$ das zugehörige Polynom über K'. Ferner seien L und L' Zerfällungskörper von f bzw. f' über K bzw. K'.*

Dann gibt es einen Isomorphismus $\tau : L \to L'$ mit $\tau|_K = \sigma$.

$$\begin{array}{ccc} L & \overset{\tau}{\dashrightarrow} & L' \\ \vee| & & \vee| \\ K & \xrightarrow{\sigma} & K' \end{array}$$

Beweis. Wir zeigen die Aussage wieder mit Induktion über $n = \deg f = \deg f'$. Für $n = 0$ haben f und f' keine Nullstellen, also muss $L = K$ und $L' = K'$ gelten und wir können $\tau = \sigma$ wählen.

Für den Induktionsschritt sei nun n beliebig. Wir wählen einen irreduziblen Faktor g von f. Nach Voraussetzung zerfällt f und damit auch g über L in Linearfaktoren; insbesondere gibt es also ein $a \in L$ mit $f(a) = g(a) = 0$. Genauso ist $g' = \sigma(g)$ ein irreduzibler Faktor von f', und es gibt ein $a' \in L'$ mit $f'(a') = g'(a') = 0$.

Nach Bemerkung 4.2 (a) sind nun $K(a) \leq L$ und $K'(a') \leq L'$ Stammkörper von g bzw. g'. Aufgrund von Lemma 4.8 finden wir also einen Isomorphismus $\varphi : K(a) \to K'(a')$ mit $\varphi|_K = \sigma$ und $\varphi(a) = a'$, d. h. wir können das untere Rechteck im Diagramm unten rechts vervollständigen.

Da a eine Nullstelle von f in $K(a)$ ist, können wir nun $f = (t-a)h \in K(a)[t]$ für ein Polynom h vom Grad $n-1$ schreiben. Dann ist L als Zerfällungskörper von f über K offensichtlich auch ein Zerfällungskörper von h über $K(a)$, denn beide entstehen aus K durch Adjunktion von a sowie der Nullstellen von h. Genauso ist L' ein Zerfällungskörper über $K'(a')$ vom entsprechenden Polynom $h' = \varphi(h)$ mit $f' = (t-a')h' \in K'(a')[t]$. Nach Induktionsvoraussetzung, angewendet auf den Isomorphismus φ und das Polynom h, können wir also auch das obere Rechteck im Diagramm rechts vervollständigen, d. h. wir finden wie gewünscht einen Isomorphismus $\tau : L \to L'$ mit $\tau|_{K(a)} = \varphi$, insbesondere also mit $\tau|_K = \sigma$.

$$\begin{array}{ccc} L & \overset{\tau}{\dashrightarrow} & L' \\ \vee| & & \vee| \\ K(a) & \overset{\varphi}{\dashrightarrow} & K'(a') \\ \vee| & & \vee| \\ K & \xrightarrow{\sigma} & K' \end{array}$$

□

Bemerkung 4.17.

(a) Wenden wir Satz 4.16 auf den Fall $K = K'$, $\sigma = \mathrm{id}$ und damit $f = f'$ an, so sehen wir wie in Bemerkung 4.9 im Fall von Stammkörpern, dass es zu zwei Zerfällungskörpern L und L' eines Polynoms $f \in K[t]$ mit $f \neq 0$ stets einen K-Isomorphismus $\tau : L \to L'$ gibt. Der Zerfällungskörper eines Polynoms ist also bis auf K-Isomorphie eindeutig bestimmt. Wir können in diesem Sinne damit in Zukunft von *dem* Zerfällungskörper statt von *einem* Zerfällungskörper von f reden.

(b) Im Gegensatz zur analogen Aussage über Stammkörper in Lemma 4.8 ist der K-Isomorphismus $\tau : L \to L'$ in Satz 4.16 nicht eindeutig. Dies liegt daran, dass wir im Beweis des Satzes für das Element $a \in L$ eine Nullstelle $a' \in L'$ von g' als das Bild von a unter τ

wählen konnten – wofür es in der Regel natürlich mehrere Möglichkeiten gibt. In der Tat ist die Nichteindeutigkeit dieses Isomorphismus einer der Schlüsselpunkte der Galoistheorie, die wir in Kapitel 5 untersuchen werden (siehe z. B. Definition 5.1 (b)).

Aufgabe 4.18. Berechne für die folgenden Polynome $f \in K[t]$ ihren Zerfällungskörper L sowie den Grad $[L : K]$:

(a) $t^p - q \in \mathbb{Q}[t]$ für zwei Primzahlen p und q;

(b) $t^{15} + 6 \in \mathbb{Q}[t]$;

(c) $t^4 + 2 \in \mathbb{Z}_3[t]$.

Aufgabe 4.19. Es sei L der Zerfällungskörper eines Polynoms $f \in K[t]$ mit $f \neq 0$ über einem Körper K. Ferner seien $g \in K[t]$ ein irreduzibles Polynom und Z der Zerfällungskörper von $f \cdot g$. Da dann offensichtlich auch f und g in Z in Linearfaktoren zerfallen, können wir insbesondere L als Teilkörper von Z auffassen.

Man zeige:

(a) Sind $a, b \in Z$ zwei Nullstellen von g, so sind die Teilkörper $L(a)$ und $L(b)$ von Z isomorph über K.

(b) Hat g eine Nullstelle in L, so zerfällt g in L bereits in Linearfaktoren.

Zum Abschluss dieses Kapitels wollen wir noch zwei Anwendungen von Zerfällungskörpern behandeln. Die erste besteht darin, dass wir nun endliche Körper, also Körper mit nur endlich vielen Elementen, besser untersuchen können. Bisher kannten wir als „systematische Beispiele“ für solche endlichen Körper nur die Körper $\mathbb{Z}_p$ für eine Primzahl p. Wir hatten allerdings in Beispiel 4.5 mit dem Stammkörper $K = \mathbb{Z}_2[a]/(a^2 + a + 1)$ von $t^2 + t + 1 \in \mathbb{Z}_2[t]$ auch schon ein Beispiel für einen endlichen Körper gesehen, der nicht von dieser Form ist: nach Bemerkung 4.2 (c) ist $[K : \mathbb{Z}_2] = 2$, d. h. K ist ein 2-dimensionaler $\mathbb{Z}_2$-Vektorraum. Als $\mathbb{Z}_2$-Vektorraum ist K also isomorph zu $\mathbb{Z}_2^2$ und hat demzufolge 4 Elemente. Damit ist K ein endlicher Körper, der sicher nicht von der Form $\mathbb{Z}_p$ für eine Primzahl p sein kann.

Mit unseren Ergebnissen über Zerfällungskörper können wir nun in der Tat bis auf Isomorphie *alle* endlichen Körper konkret angeben. Wir benötigen dazu zuerst ein kleines Lemma, das die mögliche Anzahl $|K|$ von Elementen eines endlichen Körpers K wesentlich einschränkt.

Lemma 4.20. *Es sei K ein endlicher Körper. Dann ist $|K| = p^r$ für eine Primzahl p und ein $r \in \mathbb{N}_{>0}$, und die Charakteristik von K ist p.*

Beweis. Es sei $P(K) \leq K$ der Primkörper von K aus Definition 1.4. Nach Aufgabe 1.11 ist dieser Primkörper durch die Charakteristik von K eindeutig bestimmt:

- Ist $\operatorname{char} K = 0$, so ist $P(K) = \mathbb{Q}$. Also ist K dann ein Erweiterungskörper von $\mathbb{Q}$ und kann damit insbesondere nicht endlich sein. Dieser Fall tritt also für endliche Körper nicht auf.
- Ist $\operatorname{char} K = p$ eine Primzahl, so ist $P(K) = \mathbb{Z}_p$, d. h. K ist ein Erweiterungskörper von $\mathbb{Z}_p$ und damit auch ein $\mathbb{Z}_p$-Vektorraum der Dimension $r := [K : \mathbb{Z}_p]$. Natürlich muss diese Dimension endlich sein, da K sonst kein endlicher Körper wäre. Damit ist K als $\mathbb{Z}_p$-Vektorraum (nicht jedoch als Ring!) isomorph zu $\mathbb{Z}_p^r$, und es folgt $|K| = p^r$. □

Das bemerkenswerte Resultat ist nun, dass es zu jeder Primzahlpotenz wie in Lemma 4.20 *genau einen* Körper mit dieser Anzahl von Elementen gibt. Wir definieren diese Körper zunächst, und zeigen danach, dass dies wirklich die Körper sind, die wir suchen.

Definition 4.21 (Endliche Körper)**.** Es sei $q = p^r$ für eine Primzahl p und ein $r \in \mathbb{N}_{>0}$. Wir definieren $\mathbb{F}_q$ als den Zerfällungskörper des Polynoms $t^q - t$ über $\mathbb{Z}_p$ (der Buchstabe F steht für „field“, das englische Wort für Körper).

Beispiel 4.22.

(a) Ist p eine Primzahl, so ist $\mathbb{F}_p$ nach Definition der Zerfällungskörper von $f = t^p - t$ über $\mathbb{Z}_p$. Nun gilt nach Lemma 3.23 (b) aber $a^p = a$ für alle $a \in \mathbb{Z}_p$, d. h. jedes Element $a \in \mathbb{Z}_p$ ist Nullstelle von f. Da f Grad p hat, zerfällt f damit schon über $\mathbb{Z}_p$ in Linearfaktoren – es ist nämlich $f = \prod_{a \in \mathbb{Z}_p} (t-a)$. Also ist $\mathbb{Z}_p$ bereits der Zerfällungskörper von f, d. h. es ist $\mathbb{F}_p \cong \mathbb{Z}_p$.

(b) Der Körper $\mathbb{F}_4$ ist nach Definition der Zerfällungskörper von

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

über $\mathbb{Z}_2$, und damit auch der Zerfällungskörper von t^2+t+1 über $\mathbb{Z}_2$. Mit Beispiel 4.14 (b) ist also $\mathbb{F}_4 = \mathbb{Z}_2[a]/(a^2+a+1)$. Beachte, dass (wie vor Lemma 4.20 schon bemerkt) $[\mathbb{F}_4 : \mathbb{Z}_2] = 2$ und damit $|\mathbb{F}_4| = |\mathbb{Z}_2^2| = 4$ gilt, d. h. $\mathbb{F}_4$ ist ein Körper mit 4 Elementen.

Aufgabe 4.23. Berechne eine Multiplikationstafel für den Körper $\mathbb{F}_4$.

Wir wollen nun sehen, dass $\mathbb{F}_q$ in der Tat für jede Primzahlpotenz q ein Körper mit q Elementen ist. Beachte, dass dies ganz und gar nicht offensichtlich ist, da wir für den Grad des Zerfällungskörpers im Allgemeinen ja nur die Abschätzung aus Satz 4.15 haben.

Lemma 4.24. *Für jede Primzahlpotenz q gilt $|\mathbb{F}_q| = q$.*

Beweis. Ist $q = p^r$, so ist $\mathbb{F}_q$ zunächst einmal nach Definition der Zerfällungskörper von $f = t^q - t$ über $\mathbb{Z}_p$, d. h. wir haben eine Zerlegung

$$t^q - t = \prod_{i=1}^{q} (t - a_i),$$

wobei $N := \{a_1, \dots, a_q\} \subset \mathbb{F}_q$ genau die Menge der Nullstellen von f in $\mathbb{F}_q$ ist. Wir wollen zunächst zeigen, dass diese Nullstellen auch wirklich alle verschieden sind. Nach Lemma 3.24 (b) genügt es dazu zu sehen, dass f teilerfremd zu seiner formalen Ableitung f' ist. Da diese formale Ableitung in unserem konkreten Fall gleich $f' = qt^{q-1} - 1 = -1$ ist (beachte, dass $q = 0$ in $\mathbb{Z}_p$ gilt), ist dies aber offensichtlich. Also sind die Nullstellen von f alle verschieden, d. h. es ist $|N| = q$.

Wir müssen also nur noch sehen, dass $N = \mathbb{F}_q$ gilt. Dazu zeigen wir mit dem Kriterium aus Bemerkung 1.3 (a) zunächst, dass N ein Körper ist:

- $0, 1 \in N$, denn diese beiden Elemente sind offensichtlich Nullstellen von f.
- Es seien $a_i, a_j \in N$, also $a_i^q = a_i$ und $a_j^q = a_j$. Beachte, dass wegen $\operatorname{char} \mathbb{F}_q = p$ mit demselben Argument wie im Beweis von Lemma 3.23 (a) gilt, dass

  $$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p$$

  für alle $x, y \in \mathbb{F}_q$, denn $p \mid \binom{p}{i}$ und damit $\binom{p}{i} = 0 \in \mathbb{F}_q$ für $0 < i < p$. Damit erhalten wir

  $$\begin{aligned}
  (a_i + a_j)^q &= (((a_i + a_j)^p)^p \cdots)^p = a_i^q + a_j^q = a_i + a_j && \text{und damit } a_i + a_j \in N;\\
  (-a_i)^q &= -a_i^q = -a_i && \text{und damit } -a_i \in N;\\
  (a_i a_j)^q &= a_i^q a_j^q = a_i a_j && \text{und damit } a_i a_j \in N;\\
  (a_i^{-1})^q &= (a_i^q)^{-1} = a_i^{-1} && \text{und damit } a_i^{-1} \in N \text{ für } a_i \neq 0.
  \end{aligned}$$

Also ist N ein Körper. Natürlich muss er damit den Primkörper $\mathbb{Z}_p$ enthalten und ist daher der kleinste Körper, der $\mathbb{Z}_p$ und $a_1, \dots, a_q$ enthält, d. h. gleich $\mathbb{Z}_p(a_1, \dots, a_q) = \mathbb{F}_q$. Damit ist $|\mathbb{F}_q| = |N| = q$. □

Mit diesen Ergebnissen erhalten wir nun die angekündigte vollständige Klassifikation der endlichen Körper.

Folgerung 4.25 (Klassifikation endlicher Körper)**.** *Die endlichen Körper sind bis auf Isomorphie genau die Körper $\mathbb{F}_q$ für eine Primzahlpotenz q.*

Beweis. Die Körper $\mathbb{F}_q$ sind nach Lemma 4.24 natürlich endliche Körper, die paarweise verschieden sind, da sie unterschiedlich viele Elemente haben.

Ist umgekehrt K ein beliebiger endlicher Körper, so gilt zunächst $|K| = q = p^r$ für eine Primzahl p und ein $r \in \mathbb{N}_{>0}$ nach Lemma 4.20, und der Primkörper von K ist $\mathbb{Z}_p$ nach Aufgabe 1.11 (b). Ferner hat die Einheitengruppe $K^* = K\setminus\{0\}$ von K dann $q-1$ Elemente. Nach dem kleinen Satz von Fermat [G, Folgerung 5.12 (b)] gilt also $a^{q-1} = 1$ für alle $a \in K^*$ und damit $a^q = a$ für alle $a \in K$.

Insgesamt ist K also ein Erweiterungskörper von $\mathbb{Z}_p$, in dem das Polynom $t^q - t$ in Linearfaktoren zerfällt, da es ja alle q Elemente $a_1, \ldots, a_q$ von K als Nullstellen hat. Weil in K natürlich auch $\mathbb{Z}_p(a_1, \ldots, a_q) = K$ gilt, ist K damit der (nach Bemerkung 4.17 (a) eindeutig bestimmte) Zerfällungskörper $\mathbb{F}_q$ von $t^q - t$ über $\mathbb{Z}_p$. □

Aufgabe 4.26. Es seien p eine Primzahl und $m, n \in \mathbb{N}_{>0}$. Zeige, dass $\mathbb{F}_{p^m}$ genau dann (bis auf Isomorphie) in $\mathbb{F}_{p^n}$ enthalten ist, wenn $m \mid n$ gilt.

Aufgabe 4.27. Es sei $f \in \mathbb{Z}_p[t]$ ein irreduzibles Polynom vom Grad n. Man zeige:

(a) In $\mathbb{F}_{p^n}$ zerfällt f in Linearfaktoren.

(b) $f \mid t^{p^n} - t$ in $\mathbb{Z}_p[t]$.

Für die zweite Anwendung von Zerfällungskörpern erinnern wir uns noch einmal an Aufgabe 1.17, in der wir gezeigt haben, dass man die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, bei der man eigentlich zwei Elemente zu $\mathbb{Q}$ adjungiert hat, auch als einfache Körpererweiterung $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ schreiben kann. Da einfache Körpererweiterungen oft schöner zu behandeln sind als allgemeine (siehe z. B. Satz 2.14), wollen wir uns fragen, ob man vielleicht *jede* Körpererweiterung als einfache Körpererweiterung schreiben kann. In der Tat stellt sich heraus, dass dies zumindest für endliche Erweiterungen in Charakteristik 0 immer möglich ist.

Satz 4.28 (Satz vom primitiven Element). *Es sei L/K eine endliche Körpererweiterung mit $\operatorname{char} K = 0$. Dann ist L/K einfach, d. h. es gibt ein $c \in L$ mit $L = K(c)$. (Ein solches c wird dann oft auch primitives Element genannt.)*

07

Bevor wir diesen Satz beweisen, benötigen wir noch eine Vorbemerkung.

Bemerkung 4.29 (ggt von Polynomen über verschiedenen Körpern)**.** Es seien $f, g \in K[t]$ zwei Polynome über einem Körper K, die nicht beide gleich 0 sind. Ferner sei $L \geq K$ ein Erweiterungskörper von K, so dass wir f und g also auch als Polynome über L auffassen können.

In dieser Situation können wir den (nach [G, Notation 10.31 (b)] eindeutig bestimmten) normierten größten gemeinsamen Teiler $\operatorname{ggt}(f, g)$ dieser beiden Polynome natürlich sowohl über K als auch über L ausrechnen. Da sich $\operatorname{ggt}(f, g)$ aber mit Hilfe des euklidischen Algorithmus durch fortgesetzte Polynomdivision berechnen lässt [G, Satz 10.27] und die Division zweier Polynome in $K[t]$ mit Rest nach Konstruktion offensichtlich nicht davon abhängt, ob man sie als Elemente von $K[t]$ oder $L[t]$ auffasst [G, Satz 10.19], sehen wir, dass der größte gemeinsame Teiler $\operatorname{ggt}(f, g)$ in der Tat davon unabhängig ist, ob man ihn über K oder L berechnet hat.

Beachte, dass dieses Ergebnis nicht mehr ganz so offensichtlich ist, wenn man sich $\operatorname{ggt}(f, g)$ als Produkt der sowohl in f als auch in g auftretenden Primfaktoren (mit den entsprechenden Potenzen) vorstellt, da die Primfaktorzerlegungen von f und g natürlich durchaus davon abhängen, ob man sie über K oder über L betrachtet.

Durch Kombination dieses Ergebnisses mit Lemma 3.24 (b) erhalten wir nun ein einfaches und wichtiges Kriterium dafür, dass ein Polynom in seinem Zerfällungskörper keine mehrfachen Nullstellen hat:

Folgerung 4.30. *Es sei f ein nicht-konstantes irreduzibles Polynom über einem Körper K mit $\operatorname{char} K = 0$. Dann hat f in keinem Erweiterungskörper von K mehrfache Nullstellen.*

Beweis. Wegen $\operatorname{char} K = 0$ ist die formale Ableitung f' von f nicht das Nullpolynom (beachte, dass dies in positiver Charakteristik im Allgemeinen falsch ist, da z. B. das Polynom t^p über $\mathbb{Z}_p$ die formale Ableitung 0 hat). Damit sind f und f' in K teilerfremd: da f irreduzibel ist, könnte höchstens f ein gemeinsamer Teiler von f und f' sein – was aber unmöglich ist, da $f' \neq 0$ kleineren Grad als f hat und somit nicht f als Teiler haben kann. Also ist $\operatorname{ggt}(f, f') = 1$ in K, und nach Bemerkung 4.29 daher auch in jedem Erweiterungskörper $L \geq K$. Damit hat f nach Lemma 3.24 (b) keine mehrfachen Faktoren, insbesondere also auch keine mehrfachen Nullstellen in L. □

Kommen wir nun aber zum Beweis des Satzes vom primitiven Element:

Beweis von Satz 4.28. Da L/K eine endliche Körpererweiterung ist, können wir in jedem Fall $L = K(a_1, \dots, a_n)$ für gewisse Erzeuger $a_1, \dots, a_n \in L$ schreiben, die algebraisch über K sind. Mit Induktion über n genügt es dann offensichtlich zu zeigen, dass wir stets zwei Erzeuger zu einem zusammenfassen können. Mit anderen Worten können wir also annehmen, dass $L = K(a,b)$ von zwei Elementen erzeugt wird, und müssen dann zeigen, dass es ein $c \in L$ gibt mit $K(a,b) = K(c)$.

Dazu seien f und g die Minimalpolynome von a bzw. b sowie Z der Zerfällungskörper von $f \cdot g$. Dann zerfallen in Z auch f und g in Linearfaktoren, d. h. wir können

$$f = \prod_{i=1}^{r} (t - a_i) \qquad \text{und} \qquad g = \prod_{j=1}^{s} (t - b_j)$$

für gewisse $a_1, \dots, a_r, b_1, \dots, b_s \in Z$ schreiben. Beachte, dass die $a_1, \dots, a_r$ sowie die $b_1, \dots, b_s$ nach Folgerung 4.30 verschieden sind, da f und g als Minimalpolynome irreduzibel sind. Außerdem können wir diese Nullstellen so nummerieren, dass $a_1 = a$ und $b_1 = b$ gilt.

Wir wählen nun ein $\lambda \in K$, so dass

$$a_1 + \lambda b_1 \neq a_i + \lambda b_j \qquad \text{für alle } i = 1, \dots, r \text{ und } j = 2, \dots, s \tag{$*$}$$

gilt. Beachte, dass dies immer möglich ist: es sind ja nur die endlich vielen Werte $\frac{a_i - a_1}{b_1 - b_j}$ für λ ausgeschlossen, aber K enthält wegen $\operatorname{char} K = 0$ nach Aufgabe 1.11 (a) den Primkörper $P(K) = \mathbb{Q}$ und hat damit unendlich viele Elemente. Für ein solches λ setzen wir dann

$$c := a + \lambda b \quad \in L$$

und behaupten, dass dann $K(a,b) = K(c)$ gilt. Die Inklusion $K(c) \subset K(a,b)$ ist dabei natürlich offensichtlich.

Um die andere Inklusion zu sehen, betrachten wir das aus f durch Variablensubstitution entstehende Hilfspolynom

$$h(t) := f(c - \lambda t) \quad \in K(c)[t]$$

(beachte, dass c in der Regel nicht in K liegt und h damit nur über $K(c)$ definiert ist). Für dieses Polynom gilt nach Konstruktion einerseits

$$h(b_1) = f(c - \lambda b_1) = f(a_1) = f(a) = 0,$$

andererseits aber

$$h(b_j) = f(c - \lambda b_j) = f(\underbrace{a_1 + \lambda b_1 - \lambda b_j}_{\neq a_i \text{ für alle } i \text{ nach } (*)}) \neq 0$$

für $j = 2, \dots, s$, da die $a_1, \dots, a_r$ ja die einzigen Nullstellen von f sind. Damit können wir nun leicht den größten gemeinsamen Teiler von g und h in Z ablesen: die Primfaktorzerlegung von g enthält die (verschiedenen) Faktoren $t - b_j$ für $j = 1, \dots, s$ jeweils einfach, während die von h den Faktor $t - b_1$ wegen $h(b_1) = 0$ enthält, die anderen $t - b_j$ für $j = 2, \dots, s$ wegen $h(b_j) \neq 0$ jedoch nicht. Also ist $\operatorname{ggt}(g,h) = t - b_1 = t - b$ in Z.

Da g und h beide über $K(c)$ definiert sind, gilt nach Bemerkung 4.29 damit aber auch $\operatorname{ggt}(g,h) = t - b$ über $K(c)$. Insbesondere ist damit $t - b$ ein Polynom über $K(c)$, d. h. es ist $b \in K(c)$ und damit auch $a = c - \lambda b \in K(c)$. Also ergibt sich auch die Inklusion $K(a,b) \subset K(c)$ und somit wie behauptet $K(a,b) = K(c)$. □

Beispiel 4.31. Der Beweis von Satz 4.28 ist konstruktiv: er besagt, dass wir zu einer Körpererweiterung $K(a,b)$ in Charakteristik 0 konkret ein Element c mit $K(a,b) = K(c)$ finden, indem wir eine „nahezu beliebige" Linearkombination $c = a + \lambda b$ für ein $\lambda \in K$ wählen – wir müssen lediglich die Bedingung $(*)$ im Beweis des Satzes sicher stellen, wobei $a_1 = a, a_2, \ldots, a_r$ und $b_1 = b, b_2, \ldots, b_s$ die Nullstellen der Minimalpolynome von a und b in einem geeigneten Erweiterungskörper sind.

Betrachten wir einmal konkret das Beispiel $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ aus Aufgabe 1.17, d. h. $a = \sqrt{2}$ und $b = \sqrt{3}$, dann sind die Minimalpolynome dieser Elemente gleich $f = t^2 - 2$ bzw. $g = t^2 - 3$, und davon die Nullstellen in $\mathbb{C}$ wiederum $a_1 = \sqrt{2}$, $a_2 = -\sqrt{2}$, $b_1 = \sqrt{3}$, $b_2 = -\sqrt{3}$. Nach $(*)$ müssen wir also nur überprüfen, dass

$$\lambda \neq \frac{\pm\sqrt{2} - \sqrt{2}}{2\sqrt{3}}$$

ist – was bei $\lambda \in \mathbb{Q}$ für alle $\lambda \neq 0$ erfüllt ist. Damit gilt

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \lambda\sqrt{3})$$

für alle $\lambda \in \mathbb{Q}\backslash\{0\}$. Für den Spezialfall $\lambda = 1$ hatten wir dies in Aufgabe 1.17 bereits direkt überprüft.