Kapitel 6

Körpererweiterungen

In den vorigen Kapiteln hatten wir immer wieder gesehen, wie aus einem Ring weitere Ringe konstruiert wurden, etwa Polynomringe über Ringen und Körpern oder Faktorringe, aber auch die Konstruktion des Quotientenkörpers. In bestimmten Fällen entstanden durch diese Konstruktionen neue Körper, die andere Körper enthielten. In solche Situationen wird dieses Kapitel mehr Struktur bringen, etwa durch Begriffe wie algebraische und transzendente Körpererweiterungen oder Primkörper, die in vielen Kontexten (auch über diese Vorlesung hinaus) von Bedeutung sind.

6.1 Grundlegende Definitionen

Zu Beginn des Kapitels betrachen wir 'Unterkörper', die in der Regel als Teilkörper bezeichnet werden, aber strukturell in derselben Weise gebildet werden wie Untergruppen für Gruppen, Untervektorräume für Vektorräume und Unterringe für Ringe. Versuchen Sie einmal, ein Unterkörperkriterium selbst aufzustellen. Dann wissen Sie, ob Sie die allgemeine Idee hinter solchen Unterstrukturen und Unterstrukturkriterien verstanden haben.

Definition 6.1.1 *Sei $(K, +_K, \cdot_K)$ ein Körper und sei $k \subseteq K$ eine nichtleere Teilmenge von K. k heißt* **Teilkörper** *von K, falls $(k, +_K, \cdot_K)$ ein Körper ist. In diesem Fall heißt $K \supseteq k$ eine* **Körpererweiterung** *und K ein* **Erweiterungskörper** *von k.*

Bemerkung 6.1.2 *Ist $k \subseteq K$ eine Körpererweiterung, d.h. ist $(k, +_K, \cdot_K)$ ein Teilkörper von K, so trägt K in natürlicher Weise die Struktur eines k-*

Vektorraums. $(K, +_K)$ *ist wegen der Körpereigenschaften eine abelsche Gruppe, die Skalarmultiplikation ist die Einschränkung der multiplikativen Verknüpfung* $\cdot_K$ *des Körpers auf Elemente von* k *im ersten Argument. Die für einen Vektorraum zugrunde gelegten Eigenschaften der Skalarmultiplikation sind dann direkte Folge der Körpereigenschaften (Nachrechnen!).*
Betrachen wir genau, welche Eigenschaften des Körpers K *für die Vektorraumstruktur über* k *benötigt werden und welche nicht, so zeigt sich, dass bereits ein Integritätsring* R*, der einen Körper* k *enthält, in natürlicher Weise eine Vektorraumstruktur über* k *trägt.*

Definition 6.1.3 *Sei* $k \subseteq K$ *eine Körpererweiterung. Dann heißt die Zahl*

$$[K : k] := \dim_k(K) \in \mathbb{N} \cap \infty$$

der **Grad der Körpererweiterung** $K \supseteq k$*. Ist* $[K : k]$ *endlich, so spricht man von einer* **endlichen** *Körpererweiterung, andernfalls von einer* **unendlichen** *Körpererweiterung.*

Bemerkung 6.1.4 *Natürlich kann man Körpererweiterungen auch mehrfach nacheinander antreffen. Sind* $k \subseteq L \subseteq K$ *Körpererweiterungen, so nennt man* L *auch einen* **Zwischenkörper** *der Körpererweiterung* $k \subseteq K$*. Gilt sogar* $k \subsetneq L \subsetneq K$*, so spricht man von einem* **echten** *Zwischenkörper.*

Betrachtet man die obige Definition des Grades einer Körpererweiterung als Vektorraumdimension, so stellt sich relativ direkt die Frage, wie sich diese im Falle eines Körperturms wie in der Bemerkung verhält. Eigentlich ist das lediglich eine Anwendung von Linearer Algebra, aber aufgrund der Bedeutung des Satzes verdient er tatschlich den Namen 'Satz'.

Satz 6.1.5 *Sei* $k \subseteq K$ *eine Körpererweiterung mit Zwischenkörper* L*, d.h.* $k \subseteq L \subseteq K$*. Dann gilt:*

$$[K : k] = [K : L][L : k].$$

Insbesondere sehen wir in dem Satz, dass $[K : k]$ genau dann endlich ist, wenn $[K : L]$ und $[L : k]$ beide endlich sind.

Beweis: Zum Beweis der Dimensionsformel werden wir eine Basis von K als k-Vektorraum aus Basen von K als L-Vektorraum und L als k-Vektorraum

konstruieren. Damit folgt die gewünschte Dimensionsaussage direkt.

Schritt 1: Konstruktion eines Erzeugendensystems
Seien $(a_i)_{i\in I}$ eine Basis von L als k-Vektorraum und $(b_j)_{j\in J}$ eine Basis von K als L-Vektorraum. Sei außerdem $v \in K$ ein beliebiges Element von K. Dann gibt es ein $s \in \mathbb{N}_0$, $j_1, \ldots, j_s \in J$ und $\lambda_1, \ldots, \lambda_s \in L$, so dass

$$v = \sum_{i=1}^{s} \lambda_i b_{j_i}.$$

Für jedes $\lambda_i \in L$ gibt es ausserdem ein $r_i \in \mathbb{N}_0$, $m_1, \ldots, m_{r_i} \in I$ und $\mu_{i,1}, \ldots, \mu_{i,r_i} \in k$, so dass

$$\lambda_i = \sum_{t=1}^{r_i} \mu_{i,t} a_{m_t}.$$

Setzen wir diese in den Ausdruck für v ein, so erhalten wir:

$$v = \sum_{i=1}^{s} \left(\sum_{t=1}^{r_i} \mu_{i,t} a_{m_t} \right) b_{j_i} = \sum_{i=1}^{s} \sum_{t=1}^{r_i} \underbrace{\mu_{i,t}}_{\in k} \left(a_{m_t} b_{j_i}\right).$$

Damit lässt sich also jedes Element von K als k-Linearkombination von Elementen der Familie $(a_m b_j)_{j\in J, m\in I}$ schreiben. Diese Familie ist somit ein Erzeugendensystem von K als k-Vektorraum.

Schritt 2: Lineare Unabhängigkeit
Sei nun

$$\sum_{i\in I_0, j\in J_0} \lambda_{i,j} \left(a_i b_j\right) = 0$$

mit endlichen Teilmengen $I_0 \subseteq I$ und $J_0 \subseteq J$ sowie Koeffizienten $\lambda_{i,j} \in k$ eine k-Linearkombination der Null. Dann liefert eine andere Zusammenfassung der Summe:

$$0 = \sum_{j\in J_0} \underbrace{\left(\sum_{i\in I_0} \lambda_{i,j} a_i \right)}_{\in L} b_j,$$

so dass die lineare Unabhängigkeit der b_j über L sicherstellt, dass für jedes $j \in J_0$ gilt:

$$0 = \sum_{i\in I_0} \lambda_{i,j} a_i.$$

Für jede dieser Summen liefert aber die Lineare Unabhängigkeit der a_i über k, dass die Linearkombination trivial sein muss. Damit sind alle $\lambda_{i,j} = 0$, was für die Lineare Unabhängigkeit des in Schritt 1 gefundenen Erzeugendensystems zu zeigen war.

Schritt 3: Behauptung des Satzes
Die gefundene Basis $(a_i b_j)_{i \in I, j \in J}$ ist eine Familie, deren Indizes gerade die Paare $(i, j) \in I \times J$ sind. Sie besitzt also $\#I \cdot \#J$ Elemente, wie es die Behauptung des Satzes aussagt.

□

Direkt aus der Definition des Grades einer Körpererweiterung bzw. aus dem obigen Satz 6.1.5 kann man noch weitere wichtige Eigenschaften des Grades von Körpererweiterungen folgern:

Lemma 6.1.6 *Sei $k \subseteq L$ und $L \subseteq K$ Körpererweiterungen und sei $[K : k] < \infty$. Dann gilt:*

a) $[K : L] = 1 \iff K = L$

b) $[K : k] = [L : k] \iff K = L$

c) Ist $[K : k]$ prim, so gilt $K = L$ oder $L = k$.

Aussage c) des Lemmas genügt, um zu zeigen, dass es keinen echten Zwischenkörper von $\mathbb{R} \subseteq \mathbb{C}$ gibt. Warum?
Beweis:

a) Ist $[K : L] = 1$, so hat K eine einelementige Basis als L-Vektorraum und ist somit isomorph zu L^1. Da $L \subseteq K$ ein Teilkörper ist, kann $1_L = 1_K$ als dieses Basiselement gewählt werden. Sind umgekehrt die Körper gleich, so ist $K = L^1$ von L-Vektorraumdimension 1.

b) Nach dem obigen Satz 6.1.5 gilt $[K : k] = [K : L][L : k]$. Daher gilt (mittels Kürzen des gemeinsamen ganzzahligen Faktors in der Gleichung) $[K : k] = [L : k]$ genau dann, wenn $1 = [K : L]$, was nach a) genau für $K = L$ erfüllt ist.

c) Ist $[K : k] = p$ prim, so gilt auch hier nach dem Satz 6.1.5 $p = [K : k] = [K : L][L : k]$, wobei p einen der beiden Faktoren teilen muss. Der andere Faktor ist dann offensichtlich 1, womit gerade folgt, dass $K = L$ oder $L = k$.

□

Proposition 6.1.7 *Sei R ein Integritätsring, $K = Quot(R)$ und L ein beliebiger Körper mit $R \subseteq L$. Dann existiert ein injektiver Körperhomomorphismus $\varphi : K \longrightarrow L$ mit $\varphi(a) = a$ für alle $a \in R$.*

Beweis: Offensichtlich stimmt φ auf R mit der Inklusion überein. Insbesondere sind damit $0_R = 0_L$ und $1_R = 1_L$.

Schritt 1: Definition von φ
Setze

$$\varphi(\frac{a}{b}) := \frac{\varphi(a)}{\varphi(b)}$$

für $a, b \in R$ mit $b \neq 0$. Zum Nachweis der Wohldefiniertheit der Abbildung betrachten wir zwei Repräsentanten $\frac{a}{b}, \frac{c}{d}$ mit $a, b, c, d \in R$, $b \neq 0 \neq d$, desselben Elementes $f \in K$. Es gilt also $ad - bc = 0_R$ und somit nach

$$0_L = \varphi(0_R) = \varphi(ad - bc) = \varphi(a)\varphi(d) - \varphi(b)\varphi(c).$$

Daher repräsentieren auch $\frac{\varphi(a)}{\varphi(b)}$ und $\frac{\varphi(c)}{\varphi(d)}$ dasselbe Element von L, weswegen φ mit obiger Zuweisung wohldefiniert ist.

Schritt 2: Homomorphismuseigenschaft von φ
Da schon nach Voraussetzung $\varphi(1_R) = 1_R = 1_L$ gilt, müssen wir lediglich die Verträglichkeit mit der Addition und Multiplikation betrachten: Seien $f, g \in K$ repräsentiert durch $f = \frac{a}{b}$ und $g = \frac{c}{d}$ mit $a, b, c, d \in R$, $b \neq 0 \neq d$.

Wir rechnen

$$\begin{aligned}
\varphi(f+g) &= \varphi(\frac{ad+bc}{bd}) \\
&= \frac{\varphi(a)\varphi(d)+\varphi(b)\varphi(c)}{\varphi(b)\varphi(d)} \\
&= \frac{\varphi(a)}{\varphi(b)}+\frac{\varphi(c)}{\varphi(d)} \\
&= \varphi(f)+\varphi(g) \\
\varphi(fg) &= \varphi(\frac{ac}{bd}) \\
&= \frac{\varphi(a)\varphi(c)}{\varphi(b)\varphi(d)} \\
&= \frac{\varphi(a)}{\varphi(b)}\frac{\varphi(c)}{\varphi(d)} \\
&= \varphi(f)\varphi(g)
\end{aligned}$$

Schritt 3: Injektivität von φ
Seien $f, g \in K$, repräsentiert durch $f = \frac{a}{b}$ und $g = \frac{c}{d}$ mit $a, b, c, d \in R$, $b \neq 0 \neq d$, zwei Elemente mit gleichem Bild unter φ. Dann gilt:

$$0_R = 0_L = \varphi(f-g) = \varphi(\frac{ad-bc}{bd}),$$

weswegen auch $ad - bc = 0_R$ gelten muss. Daher sind die beiden Brüche Repräsentanten derselben Klasse, d.h. $f = g$.

□

Korollar 6.1.8 *Seien R, K, L wie in der vorigen Proposition. Dann enthält L eine isomorphe Kopie von K. Insbesondere ist K bis auf Isomorphie der kleinste Körper, der R enthält.*

Beweis: Betrachte erneut die Abbildung φ aus dem Satz. Dann gilt nach dem Homomorphiesatz:

$$K = K/\ker(\varphi) \cong \mathrm{Im}(\varphi).$$

Die zweite Aussage ist dann offensichtlich, da jeder solche Körper eine isomorphe Kopie von K enthalten muss.

□

Definition 6.1.9 *Sei K ein Körper (mit mindestens 2 Elementen). Die Menge*

$$P_K := \bigcap_{\substack{T \subseteq K \\ T \text{ Teilkörper}}} T$$

heißt der **Primkörper** *von K.*

Haben Sie es gemerkt? In der Definition sind 2 Behauptungen versteckt, die bewiesen werden müssen: zuerst ist zu zeigen, dass P_K überhaupt ein Körper ist, danach muss geklärt werden, dass P_K bei gegebenem K eindeutig bestimmt ist. Das ist der Inhalt des folgenden Beweises:
Beweis: P_K ist nicht leer, da 0_K und $1_K \neq 0_K$ in jedem Teilkörper von K liegt.
Sind $a, b \in P_K$ so liegen sie in jedem der Teilkörper von K und damit liegen auch deren Summe, Produkt und Inverse bzgl. Addition sowie (für von Null verschiedene Elemente) auch die multiplikativen Inversen von a und b in jedem der Teilkörper. Damit liegen sie auch in P_K und P_K ist nach Untergruppenkriterium angewandt auf $(P_K, +_K)$ und $(P_K \setminus \{0\}, \cdot_K)$ ein Körper.
Sind P_1 und P_2 zwei Körper, die der Definition eines Primkörpers von K entsprechen, so muss für den Primkörper P_1 gelten $P_1 \subseteq P_2$ und umgekehrt für den Primkörper P_2 auch $P_2 \subseteq P_1$. Die beiden Körper sind also gleich, was die Eindeutigkeit des Primkörpers beweist.

□

Satz 6.1.10 *Sei K ein Körper (mit mindestens 2 Elementen) und sei $P_K \subseteq K$ der zugehörige Primkörper. Dann gilt*

a) $char(K) = p > 0 \iff P_K \cong \mathbb{Z}/\langle p \rangle$

b) $char(K) = 0 \iff P_K \cong \mathbb{Q}$

Beweis: Erinnern wir uns an die Definition der Charakteristik eines Integritätsrings (was natürlich auch jeder Körper ist): $char(R)$ ist nicht-negativer Erzeuger des Ideals $\ker(\chi)$ für den Ringhomomorphismus $\chi : \mathbb{Z} \longrightarrow R$ mit $\chi(1) = 1_R$. Nach dem Homomorphiesatz gilt:

$$\mathbb{Z}/\ker(\chi) \cong \mathrm{Im}(\chi) \subseteq K.$$

Ist χ injektiv, so befinden wir uns in der Situation von Proposition 6.1.7 und K enthält wegen $\mathbb{Z} \subseteq K$ auch $Quot(\mathbb{Z}) = \mathbb{Q}$.
Ist χ nicht injektiv, so ist $\ker(\chi)$ wegen der Nullteilerfreiheit des Körpers K ein Primideal, d.h. es gibt ein $p \in \mathbb{Z}$, prim, mit $\ker(\chi) = \langle p \rangle$ und $char(K) = p$. Damit enthält K gerade den gewünschten Körper entsprechend der Charakteristik. Da jeder Teilkörper L von K die 1_K und damit auch alle Summen $\sum_{i=1}^{r} 1_k$ enthält, enthält er auch als Unterring $\mathbb{Z}$ (im Falle von Charakteristik Null) bzw. $\mathbb{Z}/\langle p \rangle$ (im Falle von Charakteristik p) und damit nach 6.1.7 auch den zugehörigen Quotientenkörper dieses Ringes, was zeigt, dass es sich bei diesen Körpern wegen Minimalität um Primkörper handelt.
Enthält K umgekehrt einen dieser Primkörper, so ist dadurch schon die Charakteristik bestimmt, da dann der Kern von χ bekannt ist.

□

Haben Sie bemerkt, dass der Satz auch aussagt, dass es außer $\mathbb{Z}/\langle p \rangle$ mit p prim und $\mathbb{Q}$ keine Primkörper gibt.

Satz 6.1.11 *Sei K ein Körper mit genau $q \in \mathbb{N}$ Elementen. Dann gibt es eine Primzahl $p \in \mathbb{Z}$ und eine natürliche Zahl d, so dass $char(K) = p$ und $q = p^d$.*

Beweis: Sei P_K der Primkörper von K. Da K nicht unendlich ist, muss auch P_K endlich sein, weswegen $char(K) = p$ für eine Primzahl p.
Auch $d = [K : P_K]$ muss endlich sein, da K nur endlich viele Elemente enthält. Als Vektorraum der Dimension d über einem Körper mit p Elementen hat K dann genau p^d Elemente.

□

Damit haben wir eine gute Vorstellung davon, welche Anzahlen von Elementen bei endlichen Körpern vorkommen können. Wir würden sie aber auch gerne explizit beschreiben oder sogar aus Primkörpern konstruieren können. Dafür sollten wir uns zuerst an den Einsetzungshomomorphismus für Polynome – zugeschnitten auf unsere Situation – erinnern.

Erinnerung 6.1.12 *Sei $k \subseteq K$ ein Körpererweiterung und $\alpha \in K$. Dann ist α einsetzbar in Polynome aus $k[t]$ und der Einsetzungshomomorphismus*

ist

$$\begin{array}{rcl} E_\alpha : k[t] & \longrightarrow & K \\ f = \sum_{i=0}^{n} a_i t^i & \longmapsto & \sum_{i=0}^{n} a_i \alpha^i = f(\alpha). \end{array}$$

Dabei wird $\mathrm{Im}(E_\alpha)$ *mit* $k[\alpha]$ *bezeichnet und ist als Bild eines Ringhomomorphismus selbst ein Ring.*

Lemma 6.1.13 *Sei* $k \subseteq K$ *ein Körpererweiterung und* $\alpha \in K$*. Dann gilt*

$$k[\alpha] = \bigcap_{\substack{k \leq R \leq K \text{ als Unterringe} \\ \alpha \in R}} R.$$

$k[\alpha]$ ist also der kleinste Unterring von K, der α und k enthält.

Beweis: Da $k[\alpha]$ ein Unterring von K ist, der k als Unterring und α als Element enthält, taucht $k[\alpha]$ bei den Ringen R auf. Daher ist der Durchschnitt in $k[\alpha]$ enthalten. Jeder Unterring von K, der k und α enthält muss wegen der Abgeschlossenheit unter Addition und Multiplikation auch jeden polynomialen Ausdruck in α mit Koeffizienten in k enthalten, was genau $\mathrm{Im}(E_\alpha) = k[\alpha]$ ist. Damit ist $k[\alpha]$ im Durchschnitt und die Behauptung ist bewiesen.

□

Notation 6.1.14 *Man sagt auch, dass* $k[\alpha]$ *der* **durch Adjunktion von** α **an** k *erzeugte Unterring von* K *ist.*

Definition 6.1.15 *Sei* $k \subseteq K$ *ein Körpererweiterung und* $\alpha \in K$*. Dann definieren wir*

$$k(\alpha) := Quot(k[\alpha]).$$

Lemma 6.1.16 *Sei* $k \subseteq K$ *ein Körpererweiterung und* $\alpha \in K$*. Dann gilt*

$$k(\alpha) = \bigcap_{\substack{k \leq T \leq K \text{ als Teilkörper} \\ \alpha \in T}} T.$$

Beweis: Jeder Teilkörper T von K, der k und α enthält, ist auch ein Unterring von K mit diesen Eigenschaften und enthält damit nach Lemma 6.1.13 auch $k[\alpha]$. Nach Proposition 6.1.7 enthält T damit auch $k(\alpha) = Quot(k[\alpha])$. Andererseits taucht $k(\alpha)$ offensichtlich in der Liste solcher T auf, womit die Behauptung bewiesen ist.

□

Notation 6.1.17 *Allgemeiner kann man für beliebige Teilmengen $A \subseteq K$ auch $k[A]$ bzw. $k(A)$ definieren als kleinster Unterring bzw. kleinster Teilkörper, der k und A enthält, also*

$$k[A] := \bigcap_{\substack{k \leq R \leq K \text{ als Unterringe} \\ A \subseteq R}} R \quad \textit{und} \quad k(A) := \bigcap_{\substack{k \leq T \leq K \text{ als Teilkörper} \\ A \subseteq T}} T.$$

Im Fall einer endlichen Menge $A = \{\alpha_1, \ldots, \alpha_n\}$ schreibt man in Verallgemeinerung der Adjunktion eines Elements auf endlich viele auch gerne $k[\alpha_1, \ldots, \alpha_n]$ bzw. $k(\alpha_1, \ldots, \alpha_n)$.

Betrachten wir einmal $k = \mathbb{Q}$ und die Elemente $\alpha = \sqrt{2}$ und $\beta = \pi$. Dann sagt uns schon die Intuition, dass hierbei $k(\alpha)$, also die Adjunktion einer Quadratwurzel, also der Lösung einer quadratischen Gleichung, an den Körper k andere Eigenschaften haben dürfte als die Adjunktion von β, das keine polynomiale Gleichung über $\mathbb{Q}$ erfüllt, wie wir alle zumindest in der Schule schonmal in einer Randbemerkung gehört hatten. Aber was macht den Unterschied, sofern einer besteht, dann aus? Damit befasst sich der folgende Abschnitt.

6.2 Algebraische und transzendente Erweiterungen

In diesem Abschnitt werden wir vornehmlich solche Körpererweiterungen betrachten, die von einem Element erzeugt werden und dabei Eigenschaften des Elements mit Eigenschaften des durch dessen Adjunktion entstandenen Ringes oder Körpers verbinden. Generell läßt sich unsere Situation also wie folgt darstellen:

$$\underbrace{k}_{\text{Körper}} \subseteq \underbrace{k[\alpha]}_{\text{Integritätsring}} \subseteq \underbrace{k(\alpha)}_{\text{Körper}} \subseteq \underbrace{K}_{\text{Körper}},$$

wobei gerade die beiden mittleren Objekte im Fokus der Überlegungen stehen.

Definition 6.2.1 *Eine Körpererweiterung $k \subseteq K$ heißt* **einfach**, *falls es ein $\alpha \in K$ gibt mit $K = k(\alpha)$. In diesem Fall nennt man α ein* **primitives Element** *der Körpererweiterung.*

Definition 6.2.2 *Sei $k \subseteq K$ eine Körpererweiterung und $\alpha \in K$. Dann heißt α* **algebraisch** *über k, falls es ein $f \in k[t] \setminus \{0\}$ gibt mit $f(\alpha) = 0$, andernfalls heißt α* **transzendent** *über k.*

Betrachten wir die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{R}$, so ist $\sqrt{2}$ algebraisch über $\mathbb{Q}$, da es die Gleichung $t^2 - 2 = 0$ erfüllt. Die Transzendenz von e über $\mathbb{Q}$ wurde erstmals von Charles Hermite 1873 beweisen, die von π über $\mathbb{Q}$ wurde erstmals von Ferdinand von Lindemann 1882 gezeigt. David Hilbert lieferte 1893 einen weiteren, eleganteren Beweis, der aber noch immer vom Umfang her den Rahmen eines Randkommentars einer Vorlesung Algebra I sprengen würde, so dass wir an dieser Stelle darauf verzichten müssen.

Definition 6.2.3 *Eine Körpererweiterung $K \supseteq k$ heißt* **algebraisch**, *falls jedes Element von K algebraisch über k ist. Existiert ein Element von K, das transzendent über k ist, so heißt die Körpererweiterung* **transzendent**.

Bemerkung 6.2.4 *Eine transzendente Körpererweiterung $K \supseteq k$ kann natürlich in K Elemente enthalten, die algebraisch über k sind. Allein die Existenz eines transzendenten Elementes macht die Körpererweiterung schon transzendent. Ist jedes Element von $K \setminus k$ transzendent über k, so sagt man auch, dass $K \supseteq k$ eine rein transzendente Erweiterung ist. Darauf werden wir aber hier in der Vorlesung nicht im Detail eingehen.*

Nun haben wir für den am Ende des letzten Abschnitts mit einem Beispiel angedeuteten Unterschied der beiden Situationen das nötige Vokabular und können uns der Charakterisierung der Situationen zuwenden.

Satz 6.2.5 *Sei $K \supseteq k$ eine Körpererweiterung und sei $\alpha \in K \setminus k$. Dann gilt:*

a) Ist α transzendent über k, so gilt

$$k[\alpha] \cong k[t] \quad \textit{und} \quad k(\alpha) \cong k(t),$$

wobei $k[t]$ hier den Polynomring in einer Variable bezeichnet und $k(t)$ dessen Quotientenkörper.

b) Ist α algebraisch über k, so gilt

$$k[\alpha] = k(\alpha)$$

und es gibt ein normiertes, irreduzibles Polynom $f_{\alpha,k} \in k[t] \setminus k$ mit

$$k[\alpha] \cong k[t]/\langle f_{\alpha,k}\rangle.$$

Definition 6.2.6 *Das soeben eingeführte Polynom $f_{\alpha,k}$ bezeichnet man als* **Minimalpolynom** *von α über k.*

Bemerkung 6.2.7 *In Fall a) des obigen Satzes ist $k[\alpha]$ ein Integritätsring, der kein Körper ist. In Fall b) ist $k[\alpha] = k(\alpha)$ dagegen ein Körper (und als solcher natürlich immer noch ein Integritätsring).*

Beweis: Betrachte $E_\alpha : k[t] \longrightarrow k[\alpha]$. Nach dem Homomorphiesatz gilt

$$k[t]/\ker(E_\alpha) \cong \mathrm{Im}(E_\alpha) = k[\alpha].$$

Da $k[t]$ ein Hauptidealring ist und $\ker(E_\alpha)$ ein Ideal in $k[t]$, existiert ein Polynom $f \in k[t]$ mit $\ker(E_\alpha) = \langle f\rangle$.
Ist E_α injektiv, so erfüllt α keine polynomiale Gleichung über k, d.h. ist transzendent, und $f = 0$, d.h. $k[t] \cong k[\alpha]$. Damit sind auch die zugehörigen Quotientenkörper isomorph, was bereits a) beweist.
Ist E_α nicht injektiv, so ist $\ker(E_\alpha) = \langle f\rangle$ für ein Polynome $f \in k[t] \setminus \{0\}$, da $k[t]$ Hauptidealring ist, und α erfüllt damit die polynomiale Gleichung $f(\alpha) = 0$. Damit ist α algebraisch über k und wir befinden uns in b). Da $\mathrm{Im}(E_\alpha)$ als Unterring eines Körpers insbesondere Integritätsring sein muss, ist auch der nach Homomorphiesatz dazu isomorphe Ring $k[t]/\langle f\rangle$ Integritätsring, was nach Satz 4.6.11 impliziert, dass $k[t]/\langle f\rangle \cong k[\alpha]$ ein Körper und f prim und damit irreduzibel ist. Daher ist $f_{\alpha,k} := \frac{1}{LC(f)} f$ ist das gesuchte irreduzible normierte Polynom.

□

Bemerkung 6.2.8 *Das Minimalpolynom ist zu gegebener Körpererweiterung $K \supseteq k$ und gegebenem $\alpha \in K$ eindeutig bestimmt, da das Ideal $\ker(E_\alpha)$ von einem Element einer eindeutig bestimmten Assoziiertheitsklasse in $k[t]$ erzeugt wird und durch Normierung ein eindeutiger Repräsentant der Klasse festgelegt wird. Jedes andere Polynom $g \in k[t]$ mit $g(\alpha) = 0$ liegt in $\ker(E_\alpha) = \langle f_{\alpha,k}\rangle$ und ist somit ein Vielfaches von $f_{\alpha,k}$.*

Korollar 6.2.9 *Sei $K \supseteq k$ eine Körpererweiterung und sei $\alpha \in K$ algebraisch über k mit Minimalpolynom $f_{\alpha,k}$ vom Grad n. Dann ist $(1, \alpha, \ldots, \alpha^{n-1})$ eine Basis des k-Vektorraums $k[\alpha]$.*
Insbesondere ist dann $[k[\alpha] : k] = n = \deg(f_{\alpha,k})$.

Beweis: Wir wissen aus dem vorigen Satz, dass $k[\alpha] \cong k[t]/\langle f_{\alpha,k}\rangle$ ein Körper ist, wobei nach Voraussetzung dieses Lemmas $f_{\alpha,k} = t^n + g$ für ein geeignetes $g \in k[t]$ von Grad höchstens $n-1$. Damit ist $(1, t, \ldots, t^{n-1})$ eine Basis von $k[t]/\langle f_{\alpha,k}\rangle$ und deren Bild $(1, \alpha, \ldots, \alpha^{n-1})$ (unter dem Isomorphismus) eine Basis von $k[\alpha]$. Der Rest der Aussage läßt sich dann direkt aus den Daten ablesen.

□

Betrachten wir nun den Umgang mit einem algebraischen Element $\alpha \in K \setminus k$ in den beiden folgenden Bemerkungen etwas genauer:

Bemerkung 6.2.10 *(Rechnen in $k[\alpha]$)*
Auch wenn wir bereits wissen, dass $k[\alpha]$ ein Körper ist, haben wir wegen der abstrakten Herangehensweise an den Beweis der Tatsache bisher noch nicht konkret beschrieben, wie ein Element $\beta \in k[\alpha] \setminus \{0\}$ invertiert werden kann. Auch dazu verwenden wir wieder den Isomorphismus $k[t]/\langle f_{\alpha,k}\rangle \cong k[\alpha]$ und verwenden für β dessen eindeutigen Repräsentanten g vom Grad $\leq n-1$. Dann sind wegen der Irreduzibilität von $f_{\alpha,k}$ und wegen des niedrigeren Grades von g die beiden Polynome $f_{\alpha,k}$ und g teilerfremd in dem euklidischen Ring $k[t]$, so dass es nach der Bézout-Identität Elemente $x, y \in k[t]$ gibt mit

$$x \cdot g + y \cdot f_{\alpha,k} = 1.$$

Damit repäsentiert x die Klassen des Inversen von g in $k[t]/\langle f_{\alpha,k}\rangle$ und dessen Bild ist die gesuchte Inverse in $k[\alpha]$.

Bemerkung 6.2.11 *(Ausnutzen von $k(\alpha) = k[\alpha]$)*
Ein Element von $k(\alpha)$ ist nach unseren Überlegungen stets auch ein Element von $k[\alpha]$ und kann somit in der Basis $(1, \ldots, \alpha^{n-1})$ dargestellt werden. Konkret findet man die Basisdarstellung über Koeffizientenvergleich wie in folgendem Ansatz mit gesuchtem $\sum_{i=0}^{n-1} x_i\alpha^i$ zu gegebenem $\gamma = \frac{g(\alpha)}{h(\alpha)} \in k(\alpha)$ mit geeigneten $g(\alpha), h(\alpha) \in k[\alpha]$:

$$g(\alpha) = h(\alpha)\left(\sum_{i=0}^{n-1} x_i\alpha^i\right).$$

Satz 6.2.12 *Sei $k \subseteq K$ ein Körpererweiterung und sei $\alpha \in K$. Dann sind äquivalent:*

a) α *algebraisch über* k

b) $[k[\alpha] : k] < \infty$

c) $k[\alpha]$ *Körper*

d) $k[\alpha] = k(\alpha)$

Dies ist eine Zusammenfassung der Ergebnisse der letzten Sätze, Lemmata und Bemerkungen und bleibt hier deswegen ohne Beweis. Es ist allerdings instruktiv, sich konkret zu überlegen, welche Argumente dabei für welche Implikation verwendet werden müssen.

Satz 6.2.13 *Jede endliche Körpererweiterung ist algebraisch.*

Beweis: Sei $K \supseteq k$ eine Körpererweiterung und sei $\beta \in K$ transzendent über k, so enthält K insbesondere den Integritätsring $k[\beta]$, der isomorph zu einem Polynomring $k[t]$ über k ist. Die k-Vektorraumdimension von $k[t]$ ist jedoch nicht endlich, da z.B. $(t^i \mid i \in \mathbb{N}_0)$ eine unendliche Basis von $k[t]$ ist. Damit kann auch $K \supseteq k$ keine endliche Körpererweiterung sein.

□

Korollar 6.2.14 *Sei $K \supseteq k$ eine Körpererweiterung und seien $\alpha, \beta \in K$ algebraisch über k. Dann ist $k(\alpha, \beta)$ eine endliche (und damit algebraische) Körpererweiterung.*

Beweis: Betrachte $k \subseteq k[\alpha] \subseteq k[\alpha, \beta]$. Da α algebraisch über k ist, ist die erste Körpererweiterung endlich, also insbesondere ein endlicher k-Vektorraum. Da β algebraisch über k ist, ist es auch algebraisch über $k[\alpha]$, da es ja noch immer Nullstelle derselben polynomialen Gleichung ist (auch wenn das Minimalpolynom vielleicht ein anderes ist). Somit ist $k[\alpha, \beta]$ ein endlich-dimensionaler $k[\alpha]$-Vektorraum und damit nach Linearer Algebra auch ein endlich-dimensionaler k-Vektorraum.

□

Bemerkung 6.2.15 *Durch Iteration des vorigen Korollars gilt die analoge Aussage auch für endlich viele algebraische Elemente von K.*

Satz 6.2.16 *Seien $k \subseteq L \subseteq K$ Körpererweiterungen. Dann gilt:*

$$K \supseteq k \text{ algebraisch } \Longleftrightarrow K \supseteq L \text{ und } L \supseteq k \text{ algebraisch.}$$

Beweis: Die Implikation "$\Longrightarrow$" ist offensichtlich, denn damit ist jedes Element von K bereits algebraisch über k und unter Verwendung derselben Gleichung auch über dem Zwischenkörper L. Ausserdem ist jedes Element des Zwischenkörpers algebraisch über k, da es als Element von K eine polynomiale Gleichung mit Koeffizienten in k erfüllt.
Ist umgekehrt für die Implikation "$\Longleftarrow$" ein $\alpha \in K$ gegeben, so erfüllt α als algebraisches Element über k eine polynomiale Gleichung mit Koeffizienten in L. Diese Gleichung besitzt nur endlich viele Koeffizienten, sagen wir $\beta_1, \ldots, \beta_s$, die alle algebraisch über k sind. Damit ist nach den vorangegangenen Sätzen

$$\begin{array}{lcl} \dim_k(k[\alpha]) & \leq & \dim_k(k[\alpha, \beta_1, \ldots, \beta_s]) \\ & \overset{Gradformel}{=} & \dim_{k[\beta_1,\ldots,\beta_s]}(k[\alpha, \beta_1, \ldots, \beta_s]) \cdot \dim_k(k[\beta_1, \ldots, \beta_s]) \\ & < & \infty. \end{array}$$

Nach den äquivalenten Beschreibungen für die Eigenschaft algebraisch, ist damit α algebraisch über k.

□

Ende des Stoffs für das Modul mat200