Beweis. Es seien K ein Körper und x ein Element in einer Erweiterung von K, welches über K separabel ist. Es sei y ein beliebiges Element in der von x erzeugten Erweiterung $K(x)$. Dann gilt nach Proposition 5.3.3 und Satz 5.3.4

$$[K(x):K] = [K(x):K]_s = [K(x):K(y)]_s[K(y):K]_s = [K(x):K(y)][K(y):K]_s.$$

Also gilt $[K(y):K] = [K(y):K]_s$, und deshalb muss nach Proposition 5.3.3 auch y separabel über K sein. Nach Definition ist also $K(x)/K$ eine separable Erweiterung. □

5.4 Der Satz vom primitiven Element

Wenn eine Körpererweiterung L/K eine einfache algebraische Körpererweiterung $L = K(x)$ ist, so nennt man x ein *primitives Element* der Erweiterung. Daher stammt der Name des folgenden Satzes.

Satz 5.4.1 (Satz vom primitiven Element). *Es sei $L = K(y,z)/K$ eine endliche Erweiterung und z sei separabel über K. Dann existiert ein Element $x \in L$ mit $L = K(x)$. Insbesondere ist jede endliche separable Erweiterung eine einfach separable Erweiterung.*

Beweis. Für den Beweis dürfen wir ohne Einschränkung annehmen, dass K ein unendlicher Körper ist, da die Aussage für endliche Körper direkt aus Satz 3.3.4 folgt.

Es seien f_y und f_z die zugehörigen Minimalpolynome über K und N ein Zerfällungskörper des Produkts $f_y \cdot f_z$. In $N[X]$ gilt dann $f_y = \prod_{i=1}^{n}(X - y_i)$ und $f_z = \prod_{j=1}^{m}(X - z_j)$, wobei wir ohne Einschränkung annehmen, dass $y = y_1$ und $z = z_1$ gilt.

Wegen der Separabilität von z bzw. f_z sind die z_j paarweise verschieden. Weil K unendlich viele Elemente hat, existiert dann ein $a \in K$ so dass $y_i + az_j \neq y + az$ für alle $j \neq 1$ und alle i gilt. Wir setzen $x := y + az$ und werden zeigen, dass dieses Element die Erweiterung L/K erzeugt.

Weil $f_y(x-az) = f_y(y) = 0$ gilt, ist z Nullstelle von $h := f_y(x-aX) \in K(x)[X]$. Also ist z auch Nullstelle des normierten größten gemeinsamen Teilers von h und f_z in $K(x)[X]$. Für jede andere Nullstelle z_j von f_z (d.h. $j \neq 1$) gilt $h(z_j) = f_y(y + az - az_j) \neq 0$ nach Wahl von a. Dann ist der normierte größte gemeinsame Teiler von h und f_z in $K(x)[X]$ aber gerade $X - z$, insbesondere gilt $z \in K(x)$. Mit z muss dann auch $y = x - az$ in $K(x)$ liegen, was $L = K(x)$ zeigt.

Die zweite Aussage folgt durch Induktion. □

Jetzt können wir Proposition 5.3.3 auf endliche Körpererweiterungen verallgemeinern.

Satz 5.4.2. *Es sei K ein Körper und L/K sei eine endliche Körpererweiterung. Dann gilt $[L:K]_s \leq [L:K]$. Gleichheit gilt genau dann, wenn L/K eine separable Erweiterung ist.*

Beweis. Die erste Aussage haben wir bereits in Korollar 3.1.5 gesehen.

Wenn L/K endlich separabel ist, so ist L/K nach Satz 5.4.1 eine einfach separable Erweiterung und die Gleichheit $[L:K]_s = [L:K]$ folgt sofort aus Proposition 5.3.3.

Umgekehrt gelte $[L:K] = [L:K]_s$. Die endliche Erweiterung L/K ist endlich erzeugt, z.B. $L = K(y_1, \dots, y_n)$ mit $y_i \in L$. Induktiv definieren wir $L_i := L_{i-1}(y_i)$ mit $L_0 := K$. Wegen der Gradformel 1.3.3 und Satz 5.3.4 muss dann für $i = 1, \dots, n$ bereits $[L_i : L_{i-1}] = [L_i : L_{i-1}]_s$ gelten. Nach Proposition 5.3.3 und Korollar 5.3.5 ist die Erweiterung L_i/L_{i-1} für jedes i separabel. Insbesondere ist y_1 separabel über K. Wegen Satz 5.4.1 ist dann $L_2 = K(y_2, y_1)$ eine einfache Erweiterung von K. Weil $[L_2 : K] = [L_2 : K]_s$ gilt, muss diese Erweiterung nach Proposition 5.3.3 und Korollar 5.3.5 separabel sein. Induktiv folgt daraus, dass L/K eine separable Erweiterung ist. □

Auch Korollar 5.3.5 besitzt eine Verallgemeinerung:

Korollar 5.4.3. *Es sei L/K eine algebraische Erweiterung und $y_1, \dots, y_n \in L$ seien separabel über K. Dann ist $K(y_1, \dots, y_n)/K$ separabel.*

Beweis. Es sei $L_i := K(y_1, \dots, y_i)$ und $L_0 := K$. Die Erweiterung L_i/L_{i-1} ist für $i = 1, \dots, n$ erzeugt von einem separablen Element, also gilt $[L_i : L_{i-1}]_s = [L_i : L_{i-1}]$ nach Proposition 5.3.3. Wegen der Gradformel und Satz 5.3.4 folgt

$$\begin{aligned}[K(y_1, \dots, y_n) : K] &= [L_n : L_{n-1}] \cdots [L_1 : L_0] = [L_n : L_{n-1}]_s \cdots [L_1 : L_0]_s \\ &= [K(y_1, \dots, y_n) : K]_s.\end{aligned}$$

Satz 5.4.2 besagt dann, dass $K(y_1, \dots, y_n)/K$ eine separable Erweiterung ist. □

Korollar 5.4.4. *Es seien K ein Körper und N der Zerfällungskörper eines separablen Polynoms $f \in K[X]$. Dann gilt*

$$|\operatorname{Aut}(N/K)| = [N : K].$$

Beweis. Es seien $x_1, \dots, x_n$ die Nullstellen von f in N; es gilt $N = K(x_1, \dots, x_n)$. Nach Definition ist jedes x_i separabel über K. Wegen Korollar 5.4.3 ist dann N/K eine separable Erweiterung. Eine Anwendung von Satz 5.4.2 liefert $[N : K]_s = [N : K]$. Weil N ein Zerfällungskörper ist, gilt aber $|\operatorname{Aut}(N/K)| = [N : K]_s$ nach Satz 3.2.2, was die Behauptung zeigt. □