KAPITEL 2

Algebraische, endliche und einfache Körpererweiterungen

1. Körpererweiterungen als Vektorräume, endliche Körpererweiterungen

Sei $L|K$ eine Körpererweiterung. Dann kann man L als K-Vektorraum betrachten. Die Dimension von L über K nennt man den **Grad** der Körpererweiterung und schreibt

$$[L : K] = \dim_K L.$$

Der Grad kann endlich oder unendlich sein. Ist der Grad endlich, so spricht man von einer **endlichen Körpererweiterung**.

Beispiele:

(1) $\mathbb{C}$ ist eine endliche Körpererweiterung von $\mathbb{R}$ vom Grad 2, da $1, i$ eine $\mathbb{R}$-Basis von $\mathbb{C}$ ist, also $[\mathbb{C} : \mathbb{R}] = 2$.
(2) $\mathbb{R}$ ist eine unendliche Körpererweiterung von $\mathbb{Q}$.
(3) $\mathbb{Q}(\pi)$ ist eine unendliche Körpererweiterung von $\mathbb{Q}$.

Ist $L|K$ eine endliche Körpererweiterung, ist $\omega_1, \ldots, \omega_n \in L$ eine K-Basis von L, so gilt also

$$L = \{a_1\omega_1 + \cdots + a_n\omega_n : a_1, \ldots, a_n \in K\},$$

wobei die Koeffizienten $a_1, \ldots, a_n$ eindeutig durch das Element von L eindeutig bestimmt sind.

Eine einfache Folgerung erhält man für die Anzahl der Elemente eines endlichen Körpers:

Satz. *Ist K ein endlicher Körper der Charakteristik p, so ist K eine endliche Körpererweiterung von $\mathbb{F}_p$ und es gilt*

$$|K| = p^{[K:\mathbb{F}_p]}.$$

Insbesondere ist $|K|$ eine p-Potenz.

Den folgenden Satz kennen wir bereits. Er zeigt eine einfache Möglichkeit, wie man endliche Körpererweiterungen konstruieren kann.

Satz. *Ist $f \in K[x]$ ein irreduzibles normiertes Polynom vom Grad n und α das Bild von x in $L = K[x]/(f)$, so ist L eine endliche Körpererweiterung von K vom Grad n, also $[L : K] = n$.*

$$1, \alpha, \ldots, \alpha^{n-1}$$

ist eine K-Basis von L, insbesondere

$$L = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in K\} \quad \textit{und} \quad [L : K] = n.$$

Ist $f = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$, so gilt

$$f(\alpha) = 0 \quad \textit{und} \quad \alpha^n = -c_0 - c_1\alpha - \cdots - c_{n-1}\alpha^{n-1}.$$

f ist das Minimalpolynom von α über K.

Hier ist eine weitere Variante, die wir bereits kennen.

Datei: kt_alg.tex. Version vom 6.5.2024

SATZ. *Sei $L|K$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K vom Grad n. Dann ist $K(\alpha)$ eine endliche Körpererweiterung von K vom Grad n, d.h. $[K(\alpha) : K] = n$,*

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$$

ist eine K-Basis von $K(\alpha)$,

$$K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in K\} = K[\alpha].$$

Ist $f(x) = m_{\alpha,K}(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ das Minimalpolynom von α über K, so gilt

$$\alpha^n = -c_0 - c_1\alpha - \cdots - c_{n-1}\alpha^{n-1}.$$

Es ist

$$K(\alpha) \simeq K[x]/(f).$$

Beispiel: Ist $d \in \mathbb{Q} \setminus \{0\}$ nicht das Quadrat einer rationalen Zahl, so ist $x^2 - d \in \mathbb{Q}[x]$ irreduzibel, also hat $\sqrt{d}$ Grad 2 über $\mathbb{Q}$. Es ist

$$[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2 \quad \text{und} \quad \mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\}.$$

2. Die Dimensionsformel für Türme von Körpererweiterungen

Sind K und E Unterkörper eines Körpers F mit

$$K \subseteq E \subseteq F,$$

so haben wir drei Körpererweiterungen: $E|K$, $F|E$ und $F|K$, was wir so graphisch darstellen können:

$$\begin{array}{c} F \\ | \\ E \\ | \\ K \end{array}$$

(Deswegen spricht man auch von einem „Körperturm“.) Wir betrachten die zugehörigen Vektorraumstrukturen: E und F sind K-Vektorräume, F ist ein E-Vektorraum. Der folgende Satz macht eine Aussage über die zugehörigen Dimensionen.

SATZ. *Seien $K \subseteq E \subseteq F$ Körper. Sei $(x_i)_{i\in I}$ eine K-Basis von E und $(y_j)_{j\in J}$ eine E-Basis von F. Dann ist $(x_iy_j)_{i\in I, j\in J}$ eine K-Basis von F. Insbesondere folgt*

$$[F : K] = [F : E] \cdot [E : K]$$

und damit:

- $[F : K] < \infty \iff [F : E] < \infty$ *und* $[E : K] < \infty$.
- $[F : K] = \infty \iff [F : E] = \infty$ *oder* $[E : K] = \infty$.

Daher: $F|K$ ist genau dann endlich, wenn die Erweiterungen $F|E$ und $E|K$ endlich sind.

Beweis:

- Sei $z \in F$. Dann existieren $b_j \in E$ - nur endlich viele $\neq 0$ - mit

  $$z = \sum_{j\in J} b_j y_j.$$

  Zu $b_j \in E$ existieren $a_{ji} \in K$ - nur endlich viele $\neq 0$ - mit

  $$b_j = \sum_{i\in I} a_{ji} x_i.$$

  Es folgt

  $$z = \sum_{j\in J} b_j y_j = \sum_{j\in J} (\sum_{i\in I} a_{ji} x_i) y_j = \sum_{i\in I, j\in J} a_{ji} x_i y_j.$$

Dies zeigt, dass $(x_iy_j)_{i\in I,j\in J}$ ein Erzeugendensystem von F über K ist.

- Wir zeigen, dass $(x_iy_j)_{i\in I,j\in J}$ linear unabhängig über K sind. Seien also $a_{ji} \in K$ - fast alle 0 - mit
$$\sum_{i\in I,j\in J} a_{ji}x_iy_j = 0.$$
Wegen
$$0 = \sum_{i\in J}(\sum_{i\in I} a_{ji}x_i)y_j, \quad \sum_{i\in I} a_{ji}x_i \in E$$
und der linearen Unabhängigkeit von $(y_j)_{j\in J}$ über E folgt
$$\sum_{i\in I} a_{ji}x_i = 0 \text{ für alle } i \in I.$$
Die lineare Unabhängigkeit von $(x_i)_{i\in I}$ über K impliziert nun $a_{ji} = 0$ für alle $i \in I$, $j \in J$. Also ist $(x_iy_j)_{i\in I,j\in J}$ linear unabhängig über K.
- Daher ist $(x_iy_j)_{i\in I,j\in J}$ eine K-Basis von F, wie behauptet. Die Formel $[F : K] = [F : E]\cdot[E : K]$ folgt daraus. ■

Bemerkung: Die Dimensionsformel $[F : K] = [F : E] \cdot [E : K]$ heißt „Gradsatz“ bei Bosch und “Gradformel“ bei Fischer.

Beispiel: Wir betrachten $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i)$, was wir auch so darstellen:

$$\begin{array}{c} \mathbb{Q}(\sqrt{2},i) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

$x^2 - 2$ ist das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$, also gilt
$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$
i ist Nullstelle des Polynoms $x^2 + 1$. Wegen $i \notin \mathbb{R}$ ist $i \notin \mathbb{Q}(\sqrt{2})$, also ist $x^2 + 1$ (aus Gradgründen) das Minimalpolynom von i über $\mathbb{Q}(\sqrt{2})$, d.h.
$$[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] = 2.$$
Die Dimensionsformel liefert also
$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$
Da $1, \sqrt{2}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{2})$ und $1, i$ eine $\mathbb{Q}(\sqrt{2})$-Basis von $\mathbb{Q}(\sqrt{2}, i)$ ist, ist
$$1, \sqrt{2}, i, \sqrt{2}i$$
eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{2}, i)$.

Die Dimensionsformel hat auch einige einfache, aber wichtige Anwendungen:

Satz. *Sei $L|K$ eine endliche Körpererweiterung.*

(1) *Ist E ein Zwischenkörper der Körpererweiterung $L|K$, also $K \subseteq E \subseteq L$, so gilt*
$$[L : K] = [L : E] \cdot [E : K], \quad \textit{insbesondere} \quad [E : K] \mid [L : K].$$
(2) *Ist $[L : K] = p$ eine Primzahl, so hat die Erweiterung $L|K$ keine echten Zwischenkörper.*

3. Algebraische Körpererweiterungen

DEFINITION. *Eine Körpererweiterung $L|K$ heißt* **algebraisch**, *wenn jedes $\alpha \in L$ algebraisch über K ist.*

Ein wichtiges Beispiel liefert der folgende Satz:

SATZ. *Jede endliche Körpererweiterung ist algebraisch.*

Beweis: Sei $L|K$ eine Körpererweiterung vom Grad n und $\alpha \in L$. Die $n+1$ Elemente

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

sind dann linear abhängig über K, d.h. es gibt $a_0, a_1, \ldots, a_n \in K$, nicht alle 0 mit

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0.$$

Nach Definition ist daher α algebraisch über K. ■

Beispiel: Für $n \in \mathbb{N}$ betrachten wir

$$\alpha = \cos(\frac{2\pi}{n}).$$

Ist α algebraisch über $\mathbb{Q}$? Es ist

$$\cos(\frac{2\pi}{n}) = \frac{1}{2}(e^{\frac{2\pi i}{n}} + e^{-\frac{2\pi i}{n}}).$$

$e^{\frac{2\pi i}{n}}$ ist Nullstelle des Polynoms $x^n - 1 \in \mathbb{Q}[x]$, ist also algebraisch über $\mathbb{Q}$. Daher ist $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ eine endliche, also algebraische Körpererweiterung von $\mathbb{Q}$. Wegen

$$\cos(\frac{2\pi}{n}) \in \mathbb{Q}(e^{\frac{2\pi i}{n}})$$

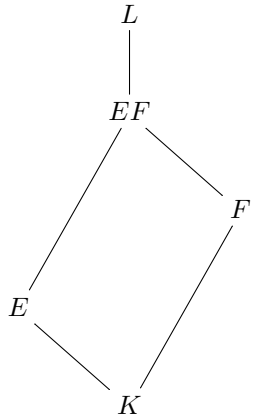
ist $\cos(\frac{2\pi}{n})$ algebraisch über $\mathbb{Q}$.

4. Das Kompositum von Körpererweiterungen

DEFINITION. *K, E und F seien Unterkörper eines Körpers L mit $K \subseteq E$ und $K \subseteq F$. Das* **Kompositum** *EF von E und F über K ist der kleinste Unterkörper von L, der E und F enthält, also*

$$EF = K(E \cup F).$$

Wir skizzieren dies auch so:



Bemerkung: Sind $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \in L$ und

$$E = K(\alpha_1, \ldots, \alpha_m) \quad \text{und} \quad F = K(\beta_1, \ldots, \beta_n),$$

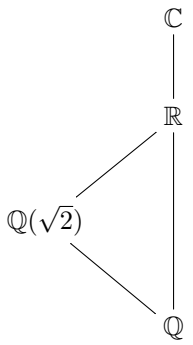
so gilt einfach

$$EF = K(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m).$$

Beispiele:

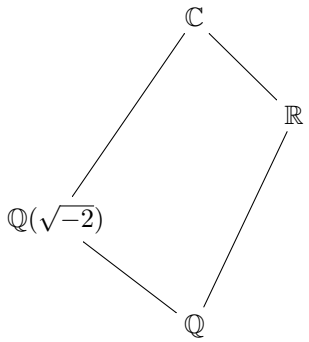
(1) In $\mathbb{C}$ betrachten wir die Unterkörper $\mathbb{Q}(\sqrt{2})$ und $\mathbb{R}$, die Körpererweiterungen von $\mathbb{Q}$ sind. Das Kompositum von $\mathbb{Q}(\sqrt{2})$ und $\mathbb{R}$ über $\mathbb{Q}$ ist offensichtlich $\mathbb{R}$:

$$\mathbb{Q}(\sqrt{2})\,\mathbb{R} = \mathbb{R}.$$



(2) In $\mathbb{C}$ betrachten wir die Unterkörper $\mathbb{Q}(\sqrt{-2})$ und $\mathbb{R}$, die Körpererweiterungen von $\mathbb{Q}$ sind. Das Kompositum von $\mathbb{Q}(\sqrt{-2})$ und $\mathbb{R}$ über $\mathbb{Q}$ ist offensichtlich $\mathbb{C}$:

$$\mathbb{Q}(\sqrt{-2})\,\mathbb{R} = \mathbb{C}.$$



Beispiel: In $\mathbb{C}$ betrachten wir die Zahlen $\zeta = \frac{-1+i\sqrt{3}}{2}$, $\alpha = \sqrt[3]{2}$ und $\beta = \zeta\sqrt[3]{2}$ und die Unterkörper

$$\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{C} \quad \text{und} \quad \mathbb{Q}(\frac{-1+i\sqrt{3}}{2}\sqrt[3]{2}) \subseteq \mathbb{C}.$$

Für das Kompositum mit $\mathbb{R}$ erhält man

$$\mathbb{Q}(\sqrt[3]{2})\,\mathbb{R} = \mathbb{R} \quad \text{und} \quad \mathbb{Q}(\frac{-1+i\sqrt{3}}{2}\sqrt[3]{2})\,\mathbb{R} = \mathbb{C}.$$

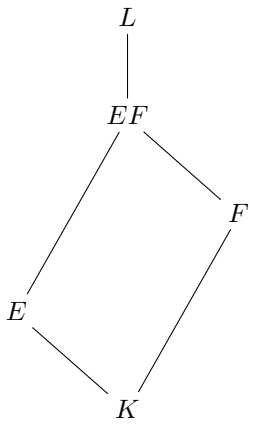
Die Zahlen α und β haben beide das Minimalpolynom $x^3 - 2$ über $\mathbb{Q}$. Der Faktorisierungssatz liefert also

$$\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/(x^3 - 2) \simeq \mathbb{Q}(\beta).$$

Obwohl die Körper $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\beta)$ also isomorph sind, hängt das Kompositum mit $\mathbb{R}$ also davon ab, wie $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\beta)$ in $\mathbb{C}$ liegen.

5. Translation von endlichen Körpererweiterungen

K, E und F seien Unterkörper eines Körpers L mit $K \subseteq E$ und $K \subseteq F$. Dann können wir das Kompositum EF von E und F über K betrachten:



Die Körpererweiterung $EF|F$ nennt man auch die **Translation** von $E|K$ zu F. Welche Eigenschaften der Erweiterung $E|K$ übertragen sich auf die Erweiterung $EF|F$?

SATZ. *K, E und F seien Unterkörper eines Körpers L mit $K \subseteq E$ und $K \subseteq F$. Ist $E|K$ eine endliche Körpererweiterung und $e_1, \ldots, e_n \in E$ eine K-Basis von E, so ist $e_1, \ldots, e_n$ ein F-Erzeugendensystem des F-Vektorraums EF:*

$$E = \{k_1e_1 + \cdots + k_ne_n : k_1, \ldots, k_n \in K\} \quad \Longrightarrow \quad EF = \{f_1e_1 + \cdots + f_ne_n : f_1, \ldots, f_n \in F\}.$$

Insbesondere ist auch $EF|F$ eine endliche Erweiterung und es gilt

$$[EF : F] \leq [E : K].$$

Beweis: Wir nennen die rechte Seite der zu beweisenden Gleichung M, also

$$M = \{f_1e_1 + \cdots + f_ne_n : f_1, \ldots, f_n \in F\}.$$

(1) Wir wollen zeigen, dass M ein Körper ist.
   (a) Natürlich gilt $E \subseteq M$. Da wir o.E. $e_1 = 1$ annehmen können, ist auch $F \subseteq M$ klar.
   (b) Da $e_1, \ldots, e_n$ eine K-Basis von E ist und $e_ie_j \in E$ gilt, gibt es $a_{ijk} \in K$ mit

$$e_ie_j = \sum_{k=1}^{n} a_{ijk}e_k \text{ für alle } i, j \in \{1, \ldots, n\}.$$

   (c) Aus

$$\begin{aligned}(\sum_i f_ie_i) \cdot (\sum_i f'_ie_i) &= (\sum_i f_ie_i) \cdot (\sum_j f'_je_j) = \sum_{i,j} f_if'_je_ie_j = \\ &= \sum_{i,j,k} f_if'_ja_{ijk}e_k = \sum_k \left(\sum_{i,j} f_if'_ja_{ijk} \right) e_k\end{aligned}$$

   sieht man, dass R abgeschlossen unter Multiplikation ist. Da M natürlich ein F-Vektorraum ist, folgt, dass M auch ein Unterring von L ist, der E und F enthält, also

$$K[E \cup F] \subseteq M.$$

   (d) Wir wollen zeigen, dass M auch abgeschlossen unter Inversenbildung ist. Sei also

$$\alpha = \sum_i f_ie_i \neq 0$$

ein beliebiges Element Element von $M \setminus \{0\}$. Es gilt:

$$\alpha e_j = \sum_i f_i e_i e_j = \sum_{i,k} f_i a_{ijk} e_k.$$

Es folgt

$$\alpha \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} \sum_i f_i a_{i11} & \dots & \sum_i f_i a_{i1n} \\ \vdots & & \vdots \\ \sum_i f_i a_{in1} & \dots & \sum_i f_i a_{inn} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix},$$

und damit

$$\begin{pmatrix} \alpha - \sum_i f_i a_{i11} & \dots & -\sum_i f_i a_{i1n} \\ \vdots & & \vdots \\ -\sum_i f_i a_{in1} & \dots & \alpha - \sum_i f_i a_{inn} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0.$$

Daher muss gelten

$$\begin{vmatrix} \alpha - \sum_i f_i a_{i11} & \dots & -\sum_i f_i a_{i1n} \\ \vdots & & \vdots \\ -\sum_i f_i a_{in1} & \dots & \alpha - \sum_i f_i a_{inn} \end{vmatrix} = 0.$$

(Man beachte, dass α nur in der Diagonale vorkommt.) Durch Ausmultiplizieren erhält man $f'_{n-1}, \dots, f'_0 \in F$ mit

$$\alpha^n + f'_{n-1}\alpha^{n-1} + \dots + f'_1\alpha + f'_0 = 0.$$

Wegen $\alpha \neq 0$ können nicht alle f'_i Null sein. Sei l der kleinste Index mit $f'_l \neq 0$. (Es ist $0 \leq l \leq n-1$.) Dann gilt also

$$\alpha^n + f'_{n-1}\alpha^{n-1} + \dots + f'_{l+1}\alpha^{l+1} + f'_l\alpha^l = 0.$$

Division durch α^l liefert

$$\alpha^{n-l} + f'_{n-1}\alpha^{n-l-1} + \dots + f'_{l+1}\alpha + f'_l = 0,$$

und damit

$$\alpha \cdot \left(\alpha^{n-l-1} + f'_{n-1}\alpha^{n-l-2} + \dots + f'_{l+1}\right) + f'_l = 0.$$

Division durch $-f'_l$ ergibt

$$\alpha \cdot \left(-\frac{f'_{l+1}}{f'_l} - \dots - \frac{f'_{n-1}}{f'_l}\alpha^{n-l-2} - \frac{1}{f'_l}\alpha^{n-l-1}\right) = 1,$$

was sofort

$$\alpha^{-1} = -\frac{f'_{l+1}}{f'_l} - \dots - \frac{f'_{n-1}}{f'_l}\alpha^{n-l-2} - \frac{1}{f'_l}\alpha^{n-l-1}$$

liefert. (Im Fall $l = n-1$ bleibt nur der letzte Summand übrig.) Da wir schon gesehen haben, dass M ein Ring ist, folgt mit $\alpha \in M$ und $F \subseteq M$ dann $\alpha^{-1} \in M$. Hieraus ergibt sich schließlich, dass M sogar ein Unterkörper von L ist. Mit $E \cup F \subseteq M$ folgt

$$K(E \cup F) \subseteq M.$$

(e) Da natürlich trivialerweise auch

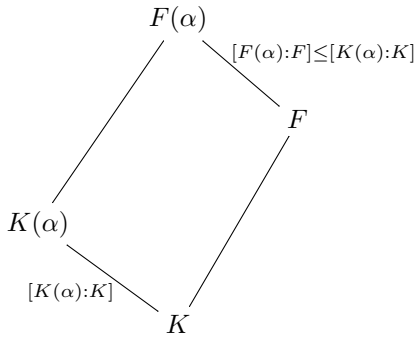
$$M = \{f_1e_1 + \dots + f_ne_n : f_1, \dots, f_n \in F\} \subseteq K(E \cup F)$$

gilt, folgt insgesamt

$$M = K(E \cup F) = EF,$$

wie behauptet. ■

Bemerkung: Wir begründen die Abschätzung $[EF : F] \leq [E : K]$ nochmals im Spezialfall $E = K(\alpha)$, wobei α über K ist.



Sei $m_{\alpha,K} \in K[x]$ das Minimalpolynom von α über K und $m_{\alpha,F} \in F[x]$ das Minimalpolynom von α über F. Wegen $K[x] \subseteq F[x]$ und $m_{\alpha,K}(\alpha) = 0$ folgt nach Definition des Minimalpolynoms $m_{\alpha,F}$ von α über F

$$m_{\alpha,F} \mid m_{\alpha,K} \text{ in } F[x].$$

Daher gilt

$$\operatorname{grad}(m_{\alpha,F}) \leq \operatorname{grad}(m_{\alpha,K}),$$

und damit

$$[F(\alpha) : F] = \operatorname{grad}(m_{\alpha,F}) \leq \operatorname{grad}(m_{\alpha,K}) = [K(\alpha) : K],$$

was wir zeigen wollten.

Bemerkung: Natürlich kann in der Abschätzung $[EF : F] \leq [E : K]$ das $<$-Zeichen gelten. Triviales Beispiel: Man wähle $F = E$. Dann ist $EF = E$ und $[FE : F] = 1$.

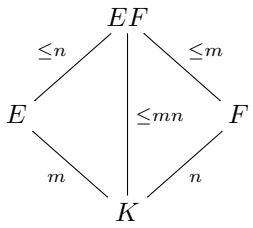
6. Der Grad des Kompositums endlicher Erweiterungen

Satz. *Sind $E|K$ und $F|K$ endliche Körpererweiterungen, wobei alle Körper Unterkörper eines Körpers L sind, so ist auch $EF|K$ eine endliche Körpererweiterung und es gilt*

$$[EF : K] \leq [E : K] \cdot [F : K].$$

Außerdem gilt die Implikation

$$\operatorname{ggT}([E : K], [F : K]) = 1 \quad \Longrightarrow \quad [EF : K] = [E : K] \cdot [F : K].$$



Beweis:

(1) Da $E|K$ endlich ist, ist auch $EF|F$ endlich, und es gilt

$$[EF : F] \leq [E : K].$$

Da $EF|F$ und $F|K$ endlich sind, ist auch $EF|K$ endlich, und es gilt

$$[EF : K] = [EF : F] \cdot [F : K] \leq [E : K] \cdot [F : K].$$

(2) Wir kommen zur zweiten Aussage: Wegen

$$[EF : K] = [EF : E] \cdot [E : K] \text{ gilt } [E : K] \mid [EF : K].$$

Wegen

$$[EF : K] = [EF : F] \cdot [F : K] \text{ gilt } [F : K] \mid [EF : K].$$

Wegen der Voraussetzung $\mathrm{ggT}([E:K],[F:K])=1$ folgt

$$[E:K]\cdot[F:K] \mid [EF:K].$$

Zusammen mit der Abschätzung aus (1) ergibt sich sofort

$$[EF:K]=[E:K]\cdot[F:K],$$

wie behauptet. ■

Beispiele:

(1) Wir betrachten die komplexen Zahlen $\alpha=\sqrt{2}$ und $\beta=\sqrt[3]{2}$. Dann gilt

$$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2 \quad \text{und} \quad [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3.$$

Wegen $\mathrm{ggT}(2,3)=1$ folgt

$$[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}]=2\cdot 3=6.$$

(2) Wir betrachten die komplexen Zahl $\zeta=\frac{-1+\sqrt{-3}}{2}$, $\alpha=\sqrt[3]{2}$ und $\beta=\zeta\alpha$. Es gilt

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=3, \quad [\mathbb{Q}(\beta):\mathbb{Q}]=3, \quad \text{aber} \quad [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=6.$$

7. Zum Verhalten algebraischer Körpererweiterungen

Wir hatten eine Körpererweiterung $L|K$ algebraisch genannt, wenn jedes $\alpha\in L$ algebraisch über K ist. Wir haben gesehen, dass endliche Körpererweiterungen algebraisch sind. Wir werden sehen, dass nicht jede algebraische Körpererweiterung endlich sein muss. Einige Eigenschaften lassen sich aber leicht von endlichen Körpererweiterungen auf algebraische Körpererweiterungen übertragen.

Satz. *Seien K, E, F Unterkörper eines Körpers L.*

(1) *Seien $K\subseteq E\subseteq F$ Körpererweiterungen. Dann gilt:*

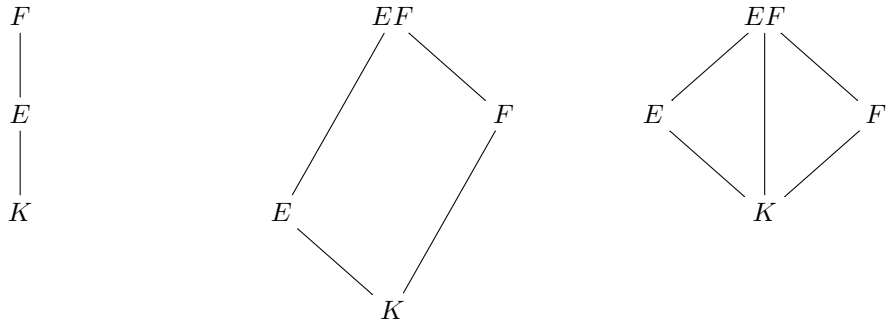
$$F|K \text{ ist algebraisch} \iff F|E \text{ und } E|K \text{ sind algebraisch.}$$

(2) *Seien $E|K$ und $F|K$ Körpererweiterungen. Dann gilt:*

$$E|K \text{ algebraisch} \implies EF|F \text{ algebraisch.}$$

(3) *Es gilt:*

$$E|K \text{ und } F|K \text{ algebraisch} \implies EF|K \text{ algebraisch.}$$



Beweis: Wir beweisen beispielhaft $\Longleftarrow$ von (1): Seien die Erweiterungen $F|E$ und $E|K$ algebraisch. Sei $\alpha\in F$ ein beliebiges Element. Wir müssen zeigen, dass α algebraisch über K. Nach Voraussetzung ist α algebraisch über E, d.h. es gibt $n\in\mathbb{N}$ und $\beta_1,\dots,\beta_n\in E$ mit

$$\alpha^n+\beta_{n-1}\alpha^{n-1}+\cdots+\beta_1\alpha+\beta_0=0.$$

Die Elemente $\beta_0,\dots,\beta_{n-1}$ von E sind algebraisch über K. Daher ist $K(\beta_0,\dots,\beta_{n-1})$ eine endliche Erweiterung von K. Obige Gleichung zeigt, dass α algebraisch über $K(\beta_0,\dots,\beta_{n-1})$ ist. Daher ist $K(\beta_0,\dots,\beta_{n-1},\alpha)$ eine endliche Erweiterung von K. Insbesondere ist α algebraisch über K. ■

SATZ. *Sei $L|K$ eine Körpererweiterung. Wir betrachten*

$$\overline{K} = \{\alpha \in L : \alpha \text{ ist algebraisch über } K\}.$$

Dann ist $\overline{K}$ ein Körper und $\overline{K}|K$ eine algebraische Körpererweiterung.

Beweis: Wir müssen zeigen, dass $\overline{K}$ ein Unterkörper von L ist. Sind $\alpha, \beta \in \overline{K}$, so sind $K(\alpha)$, $K(\beta)$ und $K(\alpha, \beta)$ endliche, also algebraische Körpererweiterungen von K. Daher gilt $K(\alpha, \beta) \subseteq \overline{K}$. Wegen $\alpha + \beta \in K(\alpha, \beta)$ und $\alpha\beta \in K(\alpha, \beta)$ folgt $\alpha + \beta \in \overline{K}$ und $\alpha\beta \in \overline{K}$. Ist $\alpha \neq 0$, so ist $\frac{1}{\alpha} \in K(\alpha)$, also $\frac{1}{\alpha} \in \overline{K}$. Es folgt, dass $\overline{K}$ ein Unterkörper von L ist. Nach Definition ist jedes Element von $\overline{K}$ algebraisch über K. Also ist $\overline{K}$ eine algebraische Körpererweiterung von K. ■

Bemerkungen:

(1) Die Menge

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ algebraisch über } \mathbb{Q}\}$$

der über $\mathbb{Q}$ algebraischen komplexen Zahlen ist ein Unterkörper von $\mathbb{C}$. Man sieht leicht, dass er unendlichen Grad über $\mathbb{Q}$ hat.

8. Zwischenkörper einfacher algebraischer Erweiterungen

Eine Körpererweiterung $L|K$ wird **einfach** genannt, wenn es ein $\alpha \in L$ gibt mit $L = K(\alpha)$. Das Element α wird dann auch ein **primitives Element** der Körpererweiterung $L|K$ genannt. Wir werden im Fall, dass α algebraisch über K ist, Aussagen über die Zwischenkörper der Erweiterung $L|K$ machen.

LEMMA. *Sei $L|K$ algebraisch und $\alpha \in L$ mit $L = K(\alpha)$. Sei $f = m_{\alpha,K} \in K[x]$ das Minimalpolynom von α über K. Sei E ein Zwischenkörper der Erweiterung, d.h. $K \subseteq E \subseteq L$, und $g_E = m_{\alpha,E} \in E[x]$ das Minimalpolynom von α über E.*

(1) *Schreibt man*

$$g_E = x^m + \beta_1 x^{m-1} + \cdots + \beta_{m-1}x + \beta_m \in E[x],$$

so gilt

$$E = K(\beta_1, \ldots, \beta_m).$$

(2) *Es gilt $g_E \mid f$.*

(3) *Ist*

$$f(x) = (x - \alpha) \cdot \prod_{i=1}^{r} f_i(x) \in K(\alpha)[x]$$

die Zerlegung von f in irreduzible (normierte) Faktoren in $K(\alpha)[x]$, so gibt es eine Teilmenge $I_E \subseteq \{1, \ldots, r\}$ mit

$$g_E(x) = (x - \alpha) \cdot \prod_{i \in I_E} f_i(x).$$

Außerdem gilt $[L : E] = 1 + \sum_{i \in I_E} \operatorname{grad}(f_i)$.

Beweis:

(1) Es ist $m = \operatorname{grad}(g_E) = [K(\alpha) : E]$. Wegen $g_E(\alpha) = 0$ genügt α einer Gleichung vom Grad m über $K(\beta_1, \ldots, \beta_m)$. Daher gilt

$$K(\beta_1, \ldots, \beta_m, \alpha) : K(\beta_1, \ldots, \beta_m)] \leq m.$$

Damit folgt

$$m \geq [L : K(\beta_1, \ldots, \beta_m)] = [L : E] \cdot [E : K(\beta_1, \ldots, \beta_m)] = m \cdot [E : K(\beta_1, \ldots, \beta_m)],$$

woraus sofort $[E : K(\beta_1, \ldots, \beta_m)] = 1$, also

$$E = K(\beta_1, \ldots, \beta_m)$$

folgt

(2) Es gilt $g_E(\alpha) = f(\alpha) = 0$ und $g_E, f \in E[x]$. Da g_E das Minimalpolynom von α über E ist, folgt $g_E \mid f$.

(3) Aus $g_E \mid f$ folgt

$$g_E(x) \mid (x-\alpha) \cdot \prod_{i=1}^{r} f_i(x).$$

Wegen $g_E(\alpha) = 0$ gibt es dann eine Teilmenge $I_E \subseteq \{1, \ldots, r\}$ mit

$$g_E(x) = (x-\alpha) \cdot \prod_{i \in I_E} f_i(x).$$

Da g_E das Minimalpolynom von α über E ist, folgt mit $L = K(\alpha)$

$$[L:K] = [K(\alpha):K] = \operatorname{grad}(g_E) = 1 + \sum_{i \in I_E} \operatorname{grad}(f_i).$$

Damit ist alles gezeigt. ■

Da man aus dem Minimalpolynom $m_{\alpha,E}$ wieder den Zwischenkörper rekonstruieren kann, ergibt sich sofort folgender Satz:

SATZ. *Sei $L = K(\alpha)$ mit einem über K algebraischen Element. Sei $f \in K[x]$ das Minimalpolynom von α über K. Dann ist die Abbildung*

$$\{E \text{ Körper mit } K \subseteq E \subseteq L\} \to \{g \in L[x] \text{ normiert mit } g(\alpha) = 0 \text{ und } g \mid f\}, \quad E \mapsto m_{\alpha,E}$$

injektiv. Insbesondere gibt es nur endlich viele Zwischenkörper.

Beispiele: Sei $K(\alpha)$ vom Grad 4 über K und $f \in K[x]$ das Minimalpolynom von α über K. Wir betrachten die Faktorzerlegung von f über $K(\alpha)$. Ist E ein echter Zwischenkörper $K \subseteq E \subseteq K(\alpha)$, so gilt $[K(\alpha):E] = [E:K] = 2$, wir brauchen also Teiler g_E von f vom Grad 2 mit $g_E(\alpha) = 0$.

- **Fall $f(x) = (x-\alpha) \cdot g(x)$, wo g irreduzibel ist:** Dann gibt es keinen quadratischen Zwischenkörper.
- **Fall $f(x) = (x-\alpha) \cdot (x-\beta) \cdot h(x)$, wo h irreduzibel ist:** Dann betrachten wir

  $$(x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta.$$

  Ein möglicher Zwischenkörper ist dann

  $$K(\alpha+\beta, \alpha\beta).$$

- **Fall $f(x) = (x-\alpha)(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$:** Wir betrachten

  $$(x-\alpha)(x-\alpha_i) = x^2 - (\alpha+\alpha_i)x + \alpha\alpha_i.$$

  Wir erhalten den Zwischenkörper

  $$K(\alpha+\alpha_i, \alpha\alpha_i).$$

  Insgesamt kann es also 3 Zwischenkörper geben.

Beispiele:

(1) Wir betrachten $\mathbb{Q}(\alpha)|\mathbb{Q}$, wo α eine Nullstelle des Polynoms $f = x^4 - x - 1$ ist. Als Zerlegung in irreduzible Faktoren über $\mathbb{Q}(\alpha)$ ergibt sich - ohne Beweis -

$$f = x^4 - x - 1 = (x-\alpha)(x^3 + \alpha x^2 + \alpha^2 x + (\alpha^3 - 1)).$$

f besitzt also kein quadratisches Polynom als Teiler. Daher gibt es auch keinen quadratischen Zwischenkörper.

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{array}$$

(2) Wir betrachten $\mathbb{Q}(\sqrt[4]{5})|\mathbb{Q}$. Wir schreiben $\alpha = \sqrt[4]{5}$. Das Minimalpolynom von α über $\mathbb{Q}$ ist

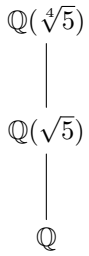
$$f = x^4 - 5 = (x-\alpha)(x+\alpha)(x^2+\alpha^2).$$

Daher gibt es nur eine Möglichkeit für g_E mit $\operatorname{grad}(g_E) = 2$:

$$g_E = (x-\alpha)(x+\alpha) = x - \alpha^2 = x - \sqrt{5}.$$

Wir erhalten als einzigen echten Zwischenkörper

$$E = \mathbb{Q}(\sqrt{5}).$$



(3) Wir betrachten $\mathbb{Q}(\sqrt{2}+\sqrt{3})|\mathbb{Q}$. Das Minimalpolynom von $\sqrt{2}+\sqrt{3}$ über $\mathbb{Q}$ ist

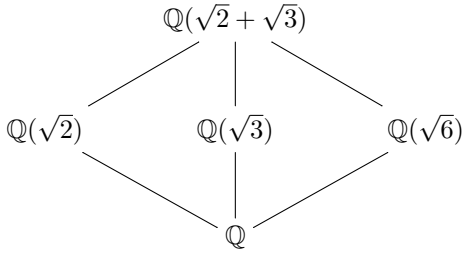
$$\begin{aligned} f &= x^4 - 10x^2 + 1 = \\ &= (x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3})). \end{aligned}$$

Es gibt drei Möglichkeiten für g_E:

$$\begin{aligned} g_{E_1}(x) &= (x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3})) = x^2 - 2\sqrt{2}x - 1, \\ g_{E_2}(x) &= (x-(\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3})) = x^2 - 2\sqrt{3}x + 1, \\ g_{E_3}(x) &= (x-(\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3})) = x^2 - (5 + \sqrt{2}\cdot\sqrt{3}). \end{aligned}$$

Wir erhalten drei Zwischenkörper:

$$E_1 = \mathbb{Q}(\sqrt{2}), \quad E_2 = \mathbb{Q}(\sqrt{3}), \quad E_3 = \mathbb{Q}(\sqrt{6}).$$



9. Der Satz vom primitiven Element I

Sei $L|K$ eine algebraische Erweiterung. Wie bereits erwähnt, heißt $\alpha \in L$ heißt ein **primitives Element** der Erweiterung $L|K$, wenn gilt $L = K(\alpha)$. In diesem Fall ist $L|K$ eine endliche Körpererweiterung. Wir wollen in diesem Abschnitt klären, wann eine endliche Körpererweiterung $L|K$ ein primitives Element besitzt.

Wir behandeln zunächst endliche Körper.

Satz. *Sei $L|K$ eine Körpererweiterung endlicher Körper, d.h. $|L| < \infty$ und $|K| < \infty$. Dann gibt es ein $\alpha \in L$ mit*

$$L = K(\alpha).$$

(Ist α ein Erzeuger der zyklischen Gruppe L^*, so gilt $L = K(\alpha)$.)

Beweis: In der Algebra zeigt man: Jede endliche Untergruppe der multiplikativen Gruppe L^* eines Körpers L ist zyklisch. Da in unserem Fall L selbst endlich ist, ist L^* zyklisch, es gibt also ein $\alpha \in L$ mit

$$L \setminus \{0\} = L^* = \{\alpha, \alpha^2, \ldots, \alpha^{|L|-1} = 1\}.$$

Dann gilt natürlich

$$L = K(\alpha),$$

was wir zeigen wollten. ■

Beispiel: Das Polynom $f = x^4+x^3+x^2+x+1 \in \mathbb{F}_2[x]$ ist irreduzibel. Also ist $K = \mathbb{F}_2[x]/(f)$ ein Körper. Sei α das Bild von x in K. Dann ist (nach Definition) $K = \mathbb{F}_2(\alpha)$. Wegen $x^5-1 = (x-1)(x^4+x^3+x^2+x+1)$ gilt $\alpha^5 = 1$, also ist α kein Erzeuger der zyklischen Gruppe K^* (mit $|K^*| = 15$), obwohl α ein primitives Element der Körpererweiterung $L|K$ ist.

Satz (Satz vom primitiven Element). *Sei $L|K$ eine endliche Körpererweiterung. Dann sind äquivalent:*

(1) *Es gibt ein $\alpha \in L$ mit $L = K(\alpha)$.*
(2) *Es gibt nur endlich viele Körper E mit $K \subseteq E \subseteq L$.*

Beweis, Teil 1:

- **Fall $|K| < \infty$:** Da $L|K$ eine endliche Körpererweiterung ist, ist auch L ein endlicher Körper (mit $|L| = |K|^{[L:K]}$.) Nach dem vorangegangenen Satz gibt es dann ein primitives Element. Da L endlich ist, hat L nur endlich viele Teilmengen, insbesondere gibt es nur endlich viele Zwischenkörper. Die Aussagen (1) und (2) des Satzes gelten hier also immer.
- (1)$\Longrightarrow$(2) Dies haben wir bereits im letzten Abschnitt bewiesen. ■

Als Vorbereitung auf den 2. Teil des Beweises behandeln wir das folgende Lemma:

Lemma. *Sei K ein unendlicher Körper und $L|K$ eine endliche Körpererweiterung mit nur endlich vielen Zwischenkörpern. Zu $\alpha, \beta \in L$ gibt es dann ein $c \in K$ mit*

$$K(\alpha, \beta) = K(\alpha + c\beta).$$

Beweis: Wir betrachten für $c \in K$ die Zwischenkörper $K(\alpha+c\beta)$. Natürlich gilt $K \subseteq K(\alpha+c\beta) \subseteq K(\alpha, \beta)$. Da es nur endlich viele Zwischenkörper geben soll und K unendlich ist, gibt es $c_1, c_2 \in K$ mit $c_1 \neq c_2$ und $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. Sei $E = K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. Dann gilt

$$\alpha + c_1\beta, \alpha + c_2\beta \in E, \quad \text{also auch} \quad \beta = \frac{(\alpha + c_1\beta) - (\alpha + c_2\beta)}{c_1 - c_2} \in E.$$

Dies impliziert

$$\alpha = (\alpha + c_1\beta) - c_1\beta \in E.$$

Aus $\alpha, \beta \in E$ folgt $K(\alpha, \beta) \subseteq E$, und zusammen mit $E \subseteq K(\alpha, \beta)$ dann

$$K(\alpha, \beta) = E = K(\alpha + c_1\beta).$$

Die beweist die Behauptung. ■

Beweis des Satzes vom primitiven Element, 2. Teil

- (2)$\Longrightarrow$(1) Da $L|K$ endlich ist, gibt es $\alpha_1, \ldots, \alpha_n \in L$ mit

  $$L = K(\alpha_1, \ldots, \alpha_n).$$

  Wir zeigen, dass es $c_2, \ldots, c_n \in K$ gibt mit

  $$L = K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n).$$

  Das Element

  $$\alpha = \alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$$

  ist also ein primitives Element der Erweiterung.
  Wir zeigen durch Induktion, dass es $c_2, \ldots, c_i$ gibt mit

  $$K(\alpha_1, \alpha_2, \ldots, \alpha_i) = K(\alpha_1 + c_2\alpha_2 + \cdots + c_i\alpha_i).$$

Für $i = 1$ ist die Aussage trivial, für $i = 2$ folgt sie direkt aus dem vorangegangenen Lemma. Gilt nun bereits

$$K(\alpha_1, \alpha_2, \ldots, \alpha_i) = K(\alpha_1 + c_2\alpha_2 + \cdots + c_i\alpha_i),$$

so erhalten wir mit dem vorangegangenen Lemma ein $c_{i+1} \in K$ mit

$$\begin{aligned} K(\alpha_1, \alpha_2, \ldots, \alpha_i, \alpha_{i+1}) &= K(\alpha_1, \ldots, \alpha_i)(\alpha_{i+1}) = \\ &= K(\alpha_1 + c_2\alpha_2 + \cdots + c_i\alpha_i)(\alpha_{i+1}) = \\ &= K(\alpha_1 + c_2\alpha_2 + \cdots + c_i\alpha_i, \alpha_{i+1}) = \\ &= K(\alpha_1 + c_2\alpha_2 + \cdots + c_i\alpha_i + c_{i+1}\alpha_{i+1}). \end{aligned}$$

Damit ist die Behauptung durch Induktion bewiesen. ■

Wir formulieren das Ergebnis des Beweises nochmals explizit:

FOLGERUNG. *Sei $L|K$ eine endliche Körpererweiterung der Gestalt*

$$L = K(\alpha_1, \ldots, \alpha_n),$$

sodass es nur endlich viele Körper E mit $K \subseteq K \subseteq L$ gibt. Dann existieren $c_2, \ldots, c_n \in K$ mit

$$L = K(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n).$$

Beispiel: Wir haben bereits gesehen, dass

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

gilt, d.h. $\sqrt{2} + \sqrt{3}$ ist ein primitives Element der Erweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$.

Bemerkung: Es gibt endliche Körpererweiterungen $L|K$, die kein primitives Element besitzen, daher unendlich viele Zwischenkörper haben. Hier ist ein Beispiel: Sei p eine Primzahl, seien x, y Unbestimmte über $\mathbb{F}_p$ und

$$L = \mathbb{F}_p(x, y) \quad \text{und} \quad K = \mathbb{F}_p(x^p, y^p).$$

10. Spur und Norm bei endlichen Körpererweiterungen

Sei $L|K$ eine endliche Körpererweiterung. Für $\alpha \in L$ erhält man durch Multiplikation eine K-lineare Abbildung

$$\phi_\alpha : L \to L \text{ mit } \phi_\alpha(\beta) = \alpha\beta$$

eine K-lineare Abbildung von L. Wir definieren **Spur**, **Norm** und **charakteristisches Polynom** von α durch

$$\mathrm{Sp}_{L|K}(\alpha) = \mathrm{sp}(\phi_\alpha), \quad \mathrm{N}_{L|K}(\alpha) = \det(\phi_\alpha), \quad \chi_{\alpha,L|K}(x) = \chi_{\phi_\alpha}(x).$$

Wir können ϕ_α durch Matrizen beschreiben. Sei $\omega_1, \ldots, \omega_n$ eine K-Basis von L. Dann gibt es Zahlen $a_{ij} \in K$ mit

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j.$$

Wir können diese n Gleichungen auch durch Matrizengleichung beschreiben:

$$\alpha \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Wir nennen

$$A(\alpha) = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$$

die α darstellende Matrix bezüglich der Basis $\omega_1, \ldots, \omega_n$. Dann ist also

$$\alpha \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A(\alpha) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Damit erhält man

$$\mathrm{Sp}_{L|K}(\alpha) = \mathrm{sp}(A(\alpha)), \quad \mathrm{N}_{L|K}(\alpha) = \det(A(\alpha)), \quad \chi_{\alpha,L|K}(x) = \det(x \cdot \mathbf{1}_n - A(\alpha)).$$

Bemerkungen:

(1) Wir erinnern daran, dass Spur, Determinante und charakteristisches Polynom nicht von der gewählten Basis abhängen.
(2) In der Linearen Algebra beschreibt man die obige Abbildung ϕ_α in der Regel durch die transponierte Matrix $A(\alpha)^t$. Wir verwenden obige Konvention, weil dies manchmal komfortabler ist. Spur, Norm und charakteristisches Polynom sind unabhängig davon, ob man die Matrix $A(\alpha)$ oder $A(\alpha)^t$ nimmt.

Beispiel: Sei $L|K$ eine Körpererweiterung vom Grad 2. Sei $\omega \in L \setminus K$. Dann ist $1, \omega$ eine K-Basis von L. Wir nehmen an, es gibt ein $d \in K$ mit $\omega^2 = d$. Dann ist $1, \omega$ eine K-Basis von L. Sei $\alpha = x + y\omega$ in L (mit $x, y \in K$). Es ist

$$(x + y\omega) \begin{pmatrix} 1 \\ \omega \end{pmatrix} = \begin{pmatrix} x + y\omega \\ x\omega + y\omega^2 \end{pmatrix} = \begin{pmatrix} x + y\omega \\ dy + x\omega \end{pmatrix} = \begin{pmatrix} x & y \\ dy & x \end{pmatrix} \begin{pmatrix} 1 \\ \omega \end{pmatrix},$$

also gilt

$$A(x + y\omega) = \begin{pmatrix} x & y \\ dy & x \end{pmatrix}.$$

Dann ist

$$\mathrm{Sp}_{L|K}(\alpha) = 2x, \quad \mathrm{N}_{L|K}(\alpha) = x^2 - dy^2.$$

Für das charakteristische Polynom erhält man

$$\chi_{\alpha,L|K}(X) = X^2 - \mathrm{Sp}_{L|K}(\alpha)X + \mathrm{N}_{L|K}(\alpha) = X^2 - 2x\,X + (x^2 - dy^2).$$

LEMMA. *Sei $L|K$ eine endliche Körpererweiterung, $\omega_1, \ldots \omega_n$ eine K-Basis von L. Für $\alpha \in L$ wird durch*

$$\omega \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A(\alpha) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}$$

eine Matrix $A(\alpha) \in \mathrm{M}_n(K)$ definiert. Dann definiert

$$A : L \to \mathrm{M}_n(K), \quad \alpha \mapsto A(\alpha)$$

einen K-linearen Ringhomomorphismus.

Beweis: Wir betrachten den Spaltenvektor

$$w = \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \in L^n.$$

Dann gilt also

$$\alpha w = A(\alpha)w.$$

Jeder Vektor aus L^n hat eine eindeutige Darstellung Mw mit $M \in \mathrm{M}_n(K)$. Für $\alpha, \beta \in L$ und $c \in K$ gilt

$$\begin{aligned} A(\alpha + \beta)w &= (\alpha + \beta)w = \alpha w + \beta w = A(\alpha)w + A(\beta)w = (A(\alpha) + A(\beta))w, \\ A(\alpha\beta)w &= \alpha\beta w = \beta\alpha w = \beta A(\alpha)w = A(\alpha)\beta w = A(\alpha)A(\beta)w, \\ A(c\alpha)w &= c\alpha w = cA(\alpha)w, \\ A(1)w &= 1w = w = \mathbf{1}_n w, \end{aligned}$$

woraus dann

$$A(\alpha+\beta)=A(\alpha)+A(\beta),\quad A(\alpha)A(\beta),\quad A(c\alpha)=cA(\alpha),\quad A(1)=\mathbf{1}_n$$

folgt. Daraus folgt die Behauptung. ■

SATZ. *Sei $L|K$ eine endliche Körpererweiterung.*

(1) $\mathrm{Sp}_{L|K}: L\to K$ *ist eine K-lineare Abbildung mit* $\mathrm{Sp}_{L|K}(1)=[L:K]$.
(2) $\mathrm{N}_{L|K}: L\to K$ *ist eine multiplikative Abbildung, d.h.*

$$\mathrm{N}_{L|L}(\alpha\beta)=\mathrm{N}_{L|K}(\alpha)\mathrm{N}_{L|K}(\beta),$$

die Einschränkung auf L^* liefert einen Gruppenhomomorphismus

$$L^*\to K^*.$$

(3) $\alpha\in L$ *ist Nullstelle des charakteristischen Polynoms $\chi_{\alpha,L|K}(x)$, d.h.* $\chi_{\alpha,L|K}(\alpha)=0$.
(4) *Charakteristisches Polynom und Minimalpolynom eines Element $\alpha\in L$ hängen so zusammen:*

$$\chi_{\alpha,L|K}(x)=m_{\alpha,K}(x)^{[L:K(\alpha)]}.$$

Beweis: Wir wählen eine K-Basis $\omega_1,\dots,\omega_n$ von L und betrachten die zugehörigen darstellenden Matrizen $A(\alpha)$. Wir verwenden die Eigenschaften des vorangegangenen Lemmas.

(1) Für $\alpha,\beta\in L$ und $c\in K$ gilt

$$\begin{aligned}\mathrm{Sp}_{L|K}(\alpha+\beta) &= \mathrm{Sp}(A(\alpha+\beta))=\mathrm{Sp}(A(\alpha)+A(\beta))=\mathrm{Sp}(A(\alpha))+\mathrm{Sp}(A(\beta)=\\ &= \mathrm{Sp}_{L|K}(\alpha)+\mathrm{Sp}_{L|K}(\beta),\\ \mathrm{Sp}_{L|K}(c\alpha) &= \mathrm{Sp}(A(c\alpha))=\mathrm{Sp}(cA(\alpha))=c\mathrm{Sp}(A(\alpha))=c\mathrm{Sp}_{L|K}(\alpha),\\ \mathrm{Sp}_{L|K}(1) &= \mathrm{Sp}(A(1))=\mathrm{Sp}(\mathbf{1}_n)=n=[L:K].\end{aligned}$$

(2) Für $\alpha,\beta\in L$ gilt

$$\begin{aligned}\mathrm{N}_{L|K}(\alpha\beta) &= \det A(\alpha\beta)=\det(A(\alpha)A(\beta))=\det(A(\alpha))\det(A(\beta))=\\ &= \mathrm{N}_{L|K}(\alpha)\cdot\mathrm{N}_{L|K}(\beta),\\ \mathrm{N}_{L|K}(1) &= \det A(1)=\det\mathbf{1}_n=1.\end{aligned}$$

(3) $\chi_{\alpha,L|K}(x)$ ist nach Definition das charakteristische Polynom der Matrix $A(\alpha)$. Nach Cayley-Hamilton gilt

$$\chi_{\alpha,L|K}(A(\alpha))=0.$$

Schreiben wir $\chi_{\alpha,L|K}(x)=\sum_i c_ix^i$ mit $c_i\in K$, so gilt

$$0=\chi_{\alpha,L|K}(A(\alpha))=\sum_i c_iA(\alpha)^i=\sum_i c_iA(\alpha^i)=A(\sum_i c_i\alpha^i)=A(\chi_{\alpha,L|K}(\alpha)).$$

Da $A: K\to \mathrm{M}_n(K)$ injektiv ist, folgt

$$\chi_{\alpha,L|K}(\alpha)=0,$$

wie behauptet.

(4) Sei $\xi_1,\dots,\xi_m$ eine K-Basis von $K(\alpha)$ und $\eta_1,\dots,\eta_n$ eine $K(\alpha)$-Basis von L. Wir wissen, dass dann $(\xi_i\eta_j)_{1\le i\le m,1\le j\le n}$ eine K-Basis von L über K ist. Es gibt Zahlen $a_{ij}\in K$ mit

$$\alpha\xi_i=\sum_{j=1}^m a_{ij}\xi_j.$$

Es folgt

$$\alpha\xi_i\eta_k=\sum_{j=1}^m a_{ij}\xi_j\eta_k.$$

Als darstellende Matrix ergibt sich eine Blockmatrix mit n Matrizen (a_{ij}) längs der Diagonalen:

$$A(\alpha) = \begin{pmatrix} (a_{ij}) & & & \\ & (a_{ij}) & & \\ & & \ddots & \\ & & & (a_{ij}) \end{pmatrix}.$$

Daraus ergibt sich

$$\begin{aligned} \chi_{\alpha,L|K}(x) &= \det(x \cdot \mathbf{1}_{mn} - A(\alpha)) = (\det(x \cdot \mathbf{1}_m - (a_{ij})))^n = \\ &= \chi_{\alpha,K(\alpha)|K}(x)^n = \chi_{\alpha,K(\alpha)|K}(x)^{[L:K(\alpha)]}. \end{aligned}$$

Aus $\chi_{\alpha,K(\alpha)|K}(\alpha) = 0$ folgt $m_{\alpha,K} \mid \chi_{\alpha,K(\alpha)|K}$. Da die Polynome gleichen Grad haben und normiert sind, folgt $m_{\alpha,K} = \chi_{\alpha,K(\alpha)|K}$. Durch Einsetzen erhält man die Behauptung. ■

Beispiel: Wir betrachten $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Wir wissen, dass gilt $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$. Man überlegt sich, dass

$$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$$

eine Basis von $\mathbb{Q}(\sqrt{2},\sqrt{3})$ über $\mathbb{Q}$ ist. Bezüglich dieser Basis berechnen wir darstellende Matrizen:

- Wir beginnen mit $\sqrt{2}+\sqrt{3}$

$$(\sqrt{2}+\sqrt{3}) \begin{pmatrix} 1 \\ \sqrt{2} \\ \sqrt{3} \\ \sqrt{6} \end{pmatrix} = \begin{pmatrix} \sqrt{2}+\sqrt{3} \\ 2+\sqrt{6} \\ 3+\sqrt{6} \\ 3\sqrt{2}+2\sqrt{3} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 1 \\ 0 & 3 & 2 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{2} \\ \sqrt{3} \\ \sqrt{6} \end{pmatrix},$$

also

$$A(\sqrt{2}+\sqrt{3}) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 1 \\ 0 & 3 & 2 & 0 \end{pmatrix}.$$

Es folgt

$$\mathrm{Sp}_{K|\mathbb{Q}}(\sqrt{2}+\sqrt{3}) = 0, \quad \mathrm{N}_{K|\mathbb{Q}}(\sqrt{2}+\sqrt{3}) = 1, \quad \chi_{\sqrt{2}+\sqrt{3},K|\mathbb{Q}}(x) = x^4 - 10x^2 + 1.$$

- Wir betrachten nun $\sqrt{6}$ als Element von $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Es ist

$$\sqrt{6} \begin{pmatrix} 1 \\ \sqrt{2} \\ \sqrt{3} \\ \sqrt{6} \end{pmatrix} = \begin{pmatrix} \sqrt{6} \\ 2\sqrt{3} \\ 3\sqrt{2} \\ 6 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 3 & 0 & 0 \\ 6 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{2} \\ \sqrt{3} \\ \sqrt{6} \end{pmatrix},$$

also

$$A(\sqrt{6}) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 3 & 0 & 0 \\ 6 & 0 & 0 & 0 \end{pmatrix}.$$

Es folgt

$$\mathrm{Sp}_{K|\mathbb{Q}}(\sqrt{6}) = 0, \quad \mathrm{N}_{K|\mathbb{Q}}(\sqrt{6}) = 36, \quad \chi_{\sqrt{6},K|\mathbb{Q}}(x) = x^4 - 12x^2 + 36 = (x^2-6)^2.$$

11. Die Transitivität der Spur-Abbildung

Satz. *Seien $L|K$ und $M|L$ endliche Körpererweiterungen. Dann ist auch $M|K$ eine endliche Körpererweiterung. Es gilt:*

$$\mathrm{Sp}_{M|K} = \mathrm{Sp}_{L|K} \circ \mathrm{Sp}_{M|L}.$$

$$\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}$$

Beweis:

- Sei $\alpha_1, \ldots, \alpha_m \in L$ eine K-Basis von L und $\beta_1, \ldots, \beta_n \in M$ eine L-Basis von M. Dann ist nach einem früheren Satz $(\alpha_i \beta_j)_{1 \le i \le m, 1 \le j \le n}$ eine K-Basis von M.
- Sei $\xi \in M$. Dann gibt es $\lambda_{jk} \in L$ mit
$$\xi \beta_j = \sum_{k=1}^{n} \lambda_{jk} \beta_k.$$
Es ist
$$\mathrm{Sp}_{M|L}(\xi) = \sum_{j=1}^{n} \lambda_{jj}.$$
- Zu $\lambda_{jk} \in L$ gibt es $\mu_{jk,il} \in K$ mit
$$\lambda_{jk} \alpha_i = \sum_{l=1}^{m} \mu_{jk,il} \alpha_l.$$
Es folgt
$$\mathrm{Sp}_{L|K}(\lambda_{jk}) = \sum_{i=1}^{m} \mu_{jk,ii},$$
und damit
$$\mathrm{Sp}_{L|K}(\mathrm{Sp}_{M|L}(\xi)) = \mathrm{Sp}_{L|K}(\sum_{j=1}^{n} \lambda_{jj}) = \sum_{j=1}^{n} \mathrm{Sp}_{L|K}(\lambda_{jj}) = \sum_{j=1}^{n} \sum_{i=1}^{m} \mu_{jj,ii}.$$
- Weiter gilt
$$\xi \alpha_i \beta_j = \alpha_i \sum_{k=1}^{n} \lambda_{jk} \beta_k = \sum_{k=1}^{n} (\lambda_{jk} \alpha_i) \beta_k = \sum_{k=1}^{n} \left(\sum_{l=1}^{m} \mu_{jk,il} \alpha_l \right) \beta_k = \sum_{k=1}^{n} \sum_{l=1}^{m} \mu_{jk,il} \alpha_l \beta_k.$$
Der Koeffizient bei $\alpha_i \beta_j$ ist dann $\mu_{jj,ii}$, woraus
$$\mathrm{Sp}_{F|K}(\xi) = \sum_{i=1}^{m} \sum_{j=1}^{n} \mu_{jj,ii}$$
folgt.
- Aus den Formeln ersieht man die Gleichheit
$$\mathrm{Sp}_{F|E}(\mathrm{Sp}_{E|K}(\xi)) = \mathrm{Sp}_{F|K}(\xi),$$
was gezeigt werden sollte. ■

Bemerkung: Für $a \in \mathbb{R}_{\ge 0}$ ist $\sqrt{a}$ durch die Bedingungen
$$\left(\sqrt{a}\right)^2 = a \quad \text{und} \quad \sqrt{a} \ge 0$$
eindeutig bestimmt. Weiter sei
$$\sqrt{a} = i\sqrt{|a|} \quad \text{für} \quad a \in \mathbb{R}_{<0}.$$

LEMMA. *Sei $d \in \mathbb{Q}^* \setminus \mathbb{Q}^{*2}$, d.h. d ist ein Nichtquadrat in $\mathbb{Q}$.*

(1) *$\mathbb{Q}(\sqrt{d})$ ist eine quadratische Erweiterung von $\mathbb{Q}$ und*
$$\mathrm{Sp}_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}(\sqrt{d}) = 0.$$

(2) *Ist K eine endliche Körpererweiterung von $\mathbb{Q}$ mit $\sqrt{d} \in K$, so gilt*

$$\mathrm{Sp}_{K|\mathbb{Q}}(\sqrt{d}) = 0.$$

Beweis:

(1) Dies wissen wir bereits. Die Spuraussage folgt auch nochmals aus

$$\sqrt{d}\begin{pmatrix} 1 \\ \sqrt{d} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix}\begin{pmatrix} 1 \\ \sqrt{d} \end{pmatrix},$$

da $1, \sqrt{d}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{d})$ ist.

(2) Wir wenden die Spurformel auf den Körperturm $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d}) \subseteq K$ an:

$$\begin{aligned} \mathrm{Sp}_{K|\mathbb{Q}}(\sqrt{d}) &= \mathrm{Sp}_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}\left(\mathrm{Sp}_{K|\mathbb{Q}(\sqrt{d})}(\sqrt{d})\right) = \mathrm{Sp}_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}\left(\sqrt{d}\cdot \mathrm{Sp}_{K|\mathbb{Q}(\sqrt{d})}(1)\right) = \\ &= \mathrm{Sp}_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}\left(\sqrt{d}\cdot [K:\mathbb{Q}(\sqrt{d})]\right) = [K:\mathbb{Q}(\sqrt{d})]\cdot \mathrm{Sp}_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}(\sqrt{d}) = \\ &= [K:\mathbb{Q}(\sqrt{d})]\cdot 0 = 0. \end{aligned}$$

Dies war zu zeigen. ■

Satz. *Sei $D \subseteq \mathbb{Z} \setminus \{0\}$ die Menge der quadratfreien ganzen Zahlen, d.h. die Menge der ganzen Zahlen, die nicht durch das Quadrat einer Primzahl teilbar sind, also*

$$D = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7, \pm 10, \pm 11, \pm 13, \pm 14, \pm 15, \pm 17, \pm 19, \dots\}.$$

Dann ist die Menge von komplexen Zahlen

$$\{\sqrt{d} : d \in D\}$$

linear unabhängig über $\mathbb{Q}$, d.h. sind $d_1, \dots, d_n$ paarweise verschiedene Elemente aus D, so gilt

$$\dim_Q\left(\mathbb{Q}\sqrt{d_1} + \cdots + \mathbb{Q}\sqrt{d_n}\right) = n.$$

Beweis:

- Wir nehmen an, wir haben eine Relation

$$\sum_{d\in D} c_d\sqrt{d} = 0 \quad \text{mit} \quad c_d \in \mathbb{Q},$$

wobei natürlich nur endlich viele c_d von 0 verschieden sein können, damit die Summe definiert ist. Sei

$$C = \{d \in D : c_d \neq 0\}.$$

Wir nehmen an, es ist $C \neq \emptyset$. Sei

$$K = \mathbb{Q}(\{\sqrt{d} : d \in C\}).$$

- Sind $d_1, d_2 \in C$ mit $d_1 \neq d_2$, so ist $d_1 d_2$ kein Quadrat in $\mathbb{Q}$, also wegen

$$(\sqrt{d_1}\cdot\sqrt{d_2})^2 = d_1 d_2 \in \mathbb{Q}^* \setminus \mathbb{Q}^{*2}$$

$$\sqrt{d_1}\cdot\sqrt{d_2} = \pm\sqrt{d_1 d_2},$$

und damit

$$\mathrm{Sp}_{K|\mathbb{Q}}(\sqrt{d_1}\cdot\sqrt{d_2}) = 0.$$

Andererseits gilt natürlich für $d \in C$

$$\mathrm{Sp}_{K|\mathbb{Q}}(\sqrt{d}\cdot\sqrt{d}) = \mathrm{Sp}_{K|\mathbb{Q}}(d) = d\cdot[K:\mathbb{Q}] \neq 0.$$

- Sei nun $d' \in C$. Multiplizieren wir $\sum_{d\in D} c_d\sqrt{d} = 0$ mit $\sqrt{d'}$, so erhalten wir

$$\sum_{d\in C} c_d\sqrt{d}\cdot\sqrt{d'} = 0.$$

Spurbildung liefert

$$\begin{aligned} 0 &= \mathrm{Sp}_{K|\mathbb{Q}}(\sum_{d\in C} c_d\sqrt{d}\cdot\sqrt{d'}) = \sum_{d\in C} c_d\cdot\mathrm{Sp}_{K|\mathbb{Q}}(\sqrt{d}\cdot\sqrt{d'}) = \\ &= c_{d'}\cdot\mathrm{Sp}_{K|\mathbb{Q}}(\sqrt{d'}\cdot\sqrt{d'}) = c_{d'}\cdot d'\cdot[K:\mathbb{Q}] \neq 0, \end{aligned}$$

und damit $c_{d'} = 0$. Dieser widerspricht aber der Wahl von C. Daher war die Annahme $C \neq \emptyset$ falsch. Damit ist bewiesen, dass $\{\sqrt{d} : d \in D\}$ linear unabhängig über $\mathbb{Q}$ ist. ■