21. Körpererweiterungen

Lemma 192: Es seien K und L Körper und K sei ein Unterring von L. Dann ist L ein K-Vektorraum.

Beweis: Das folgt sofort aus den Rechenregeln für Körper. (Beachten Sie, dass $1_K = 1_L$ gilt, da K und L Integritätsbereiche sind.)

Definition: Es seien K und L Körper und K ein Unterring von L. Dann nennt man L einen Erweiterungskörper von K bzw. K einen Teilkörper von L und spricht von der Körpererweiterung L/K. Ein Teilkörper M von L heißt Zwischenkörper der Körpererweiterung L/K wenn K ein Teilkörper von M ist (d.h. $K \subseteq M \subseteq L$). Statt $\dim_K L$ (Dimension von L als K-Vektorraum) schreibt man $[L : K]$ und nennt es den Grad der Körpererweiterung L/K. Die Körpererweiterung L/K heißt endlich wenn $[L : K]$ endlich ist.

Beispiele: 1) Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist endlich und $[\mathbb{C} : \mathbb{R}] = 2$, denn $\{1, i\}$ ist eine Basis von $\mathbb{C}$ als reeller Vektorraum.
2) Es bezeichne $\mathbb{Q}(i)$ den Körper

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

(der auch als *Gaußscher Zahlkörper* bezeichnet wird). Das ist tatsächlich ein Körper. Für $a, b, c, d \in \mathbb{Q}$ gilt

$$(a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{Q}(i)$$

und

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Q}(i),$$

d.h. $\mathbb{Q}(i)$ ist ein Unterring von $\mathbb{C}$ und daher ein kommutativer Ring mit Eins. Wegen

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \in \mathbb{Q}(i)$$

(für $(a, b) \neq (0, 0)$) ist $\mathbb{Q}(i)$ tatsächlich ein Körper. Die Körpererweiterung $\mathbb{Q}(i)/\mathbb{Q}$ ist endlich und $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, da $\{1, i\}$ eine Basis von $\mathbb{Q}(i)$ also $\mathbb{Q}$-Vektorraum ist.
3) Wir haben in Kapitel 18 in Beispiel 5 zu Satz 138 bewiesen, dass

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

mit der üblichen Addition und Multiplikation reeller Zahlen einen Körper bildet. Die Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist endlich und $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, da $\{1, \sqrt{2}\}$ eine Basis von $\mathbb{Q}(\sqrt{2})$ als $\mathbb{Q}$-Vektorraum ist. (Es ist klar, dass $\{1, \sqrt{2}\}$ ein Erzeugendensystem von $\mathbb{Q}(\sqrt{2})$ ist. Da $\sqrt{2} \notin \mathbb{Q}$ ist diese Menge auch linear unabhängig über $\mathbb{Q}$.)

4) Die Körpererweiterung $\mathbb{R}/\mathbb{Q}$ ist unendlich, da $\mathbb{Q}$ abzählbar und $\mathbb{R}$ überabzählbar unendlich ist und es daher keine endliche Basis geben kann.

Satz 193: Es sei L/K eine Körpererweiterung und M ein Zwischenkörper dieser Körpererweiterung. Dann gelten:

(i) Ist $(x_i)_{i\in I}$ eine Basis von M als K-Vektorraum und $(y_j)_{j\in J}$ eine Basis von L als M-Vektorraum, so ist $(x_iy_j)_{(i,j)\in I\times J}$ eine Basis von L als K-Vektorraum,
(ii) $[L:K] = [L:M]\cdot[M:K]$.

Beweis: (i) Ist $a \in L$, so ist

$$a = \sum_{j\in J} \beta_j y_j$$

mit $\beta_j \in M\ \forall j \in J$ und $\beta_j = 0$ für alle bis auf endlich viele $j \in J$. Für alle $j \in J$ ist

$$\beta_j = \sum_{i\in I} \alpha_{ij} x_i$$

mit $\alpha_{ij} \in K\ \forall i \in I$ und $\alpha_{ij} = 0$ für alle bis auf endlich viele $i \in I$. (Ist $\beta_j = 0$, so ist $\alpha_{ij} = 0\ \forall i \in I$.) Daraus erhält man

$$a = \sum_{j\in J} \beta_j y_j = \sum_{j\in J}\Big(\sum_{i\in I} \alpha_{ij} x_i\Big) y_j = \sum_{(i,j)\in I\times J} \alpha_{ij} x_i y_j,$$

wobei $\alpha_{ij} = 0$ für alle bis auf endlich viele $(i,j) \in I\times J$. D.h. $\{x_iy_j \mid (i,j) \in I\times J\}$ ist ein Erzeugendensystem von L als K-Vektorraum.
Ist $i_1,\dots,i_n \in I$, $j_1,\dots,j_m \in J$ und

$$\sum_{\nu=1}^{n}\sum_{\mu=1}^{m} \alpha_{\nu\mu} x_{i_\nu} y_{j_\mu} = 0$$

(mit $\alpha_{\nu\mu} \in K$ für $1 \le \nu \le n$ und $1 \le \mu \le m$), so ist auch

$$\sum_{\mu=1}^{m}\Big(\sum_{\nu=1}^{n} \alpha_{\nu\mu} x_{i_\nu}\Big) y_{j_\mu} = 0 \quad \text{mit} \quad \sum_{\nu=1}^{n} \alpha_{\nu\mu} x_{i_\nu} \in M \quad \text{für } 1 \le \mu \le m.$$

Da die Basis $(y_j)_{j\in J}$ über M linear unabhängig ist, folgt

$$\sum_{\nu=1}^{n} \alpha_{\nu\mu} x_{i_\nu} = 0 \quad \text{für } 1 \le \mu \le m.$$

Da die Basis $(x_i)_{i\in I}$ über K linear unabhängig ist, folgt $\alpha_{\nu\mu} = 0$ für $1 \le \nu \le n$ und $1 \le \mu \le m$, d.h. die Menge $\{x_iy_j \mid (i,j) \in I\times J\}$ ist linear unabhängig über K.

(ii) Aus (i) folgt

$$[L : K] = |I \times J| = |I| \cdot |J| = [M : K] \cdot [L : M].$$

Definition: Es sei L/K eine Körpererweiterung und $a_1, \dots, a_n \in L$. Wir bezeichnen mit $K[a_1, \dots, a_n]$ den kleinsten Unterring von L, der K und $a_1, \dots, a_n$ enthält und mit $K(a_1, \dots, a_n)$ den kleinsten Zwischenkörper der Körpererweiterung L/K, der $a_1, \dots, a_n$ enthält.

Satz 194: Es sei L/K eine Körpererweiterung und $a_1, \dots, a_n \in L$. Dann gelten:

(i) $K[a_1, \dots, a_n] = \{p(a_1, \dots, a_n) \mid p \in K[X_1, \dots, X_n]\}$,

(ii) $K(a_1, \dots, a_n)$
$= \{p(a_1, \dots, a_n) \cdot q(a_1, \dots, a_n)^{-1} \mid p, q \in K[X_1, \dots, X_n], q(a_1, \dots, a_n) \neq 0\}$.

Beweis: (i) Es sei $R := \{p(a_1, \dots, a_n) \mid p \in K[X_1, \dots, X_n]\}$. Dann ist offenbar $K \subseteq R$ und $a_1, \dots, a_n \in R$. Wegen

$$p(a_1, \dots, a_n) - q(a_1, \dots, a_n) = (p - q)(a_1, \dots, a_n)$$

und

$$p(a_1, \dots, a_n) \cdot q(a_1, \dots, a_n) = (p \cdot q)(a_1, \dots, a_n)$$

für alle $p, q \in K[X_1, \dots, X_n]$ ist R ein Unterring von L. Ist S ein Unterring von L, der K und $a_1, \dots, a_n$ enthält, muss offenbar $p(a_1, \dots, a_n) \in S$ für alle $p \in K[X_1, \dots, X_n]$ gelten und daher $R \subseteq S$.

(ii) Es sei

$$M := \{p(a_1, \dots, a_n) \cdot q(a_1, \dots, a_n)^{-1} \mid p, q \in K[X_1, \dots, X_n], q(a_1, \dots, a_n) \neq 0\}.$$

Dann gelten wieder $K \subseteq M$ und $a_1, \dots, a_n \in M$ und wie in (i) überlegt man sich leicht, dass M ein Unterring von L ist. Offenbar ist M ein kommutativer Ring mit Eins. Ist $p(a_1, \dots, a_n) \cdot q(a_1, \dots, a_n)^{-1} \in M \setminus \{0\}$, so ist $p(a_1, \dots, a_n) \neq 0$ und

$$\big(p(a_1, \dots, a_n) \cdot q(a_1, \dots, a_n)^{-1}\big)^{-1} = q(a_1, \dots, a_n) \cdot p(a_1, \dots, a_n)^{-1} \in M,$$

d.h. M ist ein Körper. Ist N ein Zwischenkörper der Körpererweiterung L/K und erfüllt $a_1, \dots, a_n \in N$, so muss offenbar $M \subseteq N$ gelten.

Bemerkungen: 1) Der Ring $K[a_1, \dots, a_n]$ ist das Bild des Einsetzhomomorphismus

$$K[X_1, \dots, X_n] \to L,\ p \mapsto p(a_1, \dots, a_n).$$

Die Notation entspricht also der nach Korollar 164 eingeführten.

2) Oft schreibt man

$$K(a_1, \dots, a_n) = \left\{ \frac{p(a_1, \dots, a_n)}{q(a_1, \dots, a_n)} \,\middle|\, p, q \in K[X_1, \dots, X_n], q(a_1, \dots, a_n) \neq 0 \right\},$$

d.h. man indentifiziert den Quotientenkörper von $K[a_1, \dots, a_n]$ mit seiner Einbettung in $K(a_1, \dots, a_n)$ (vergleiche auch Satz 91).
3) Ein wichtiger Spezialfall ist $n = 1$, d.h. ist L/K eine Körpererweiterung und $a \in L$, so ist

$$K[a] = \{p(a) \mid p \in K[X]\} \quad \text{und} \quad K(a) = \{p(a)q(a)^{-1} \mid p, q \in K[X], q(a) \neq 0\}.$$

Definition: Ist L/K eine Körpererweiterung und $a_1, \dots, a_n \in L$, so sagt man in der Situation von Satz 194 (ii) $a_1, \dots, a_n$ werden zu K adjungiert und nennt $K(a_1, \dots, a_n)$ den durch Adjunktion von $a_1, \dots, a_n$ zu K entstandenen Körper. Ist $a \in L$, so nennt man a primitives Element des Körpers $K(a)$. Eine Körpererweiterung L/K heißt einfach, wenn $\exists a \in L : L = K(a)$, d.h. wenn ein primitives Element existiert.

Beispiele: 1) $\mathbb{Q}(i)/\mathbb{Q}$ ist eine einfache Körpererweiterung.
2) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist eine einfache Körpererweiterung.
3) $\mathbb{C}/\mathbb{R}$ ist eine einfache Körpererweiterung, da $\mathbb{C} = \mathbb{R}(i)$.

Definition: Es sei L/K eine Körpererweiterung. Ein $a \in L$ heißt algebraisch über K, wenn es Nullstelle eines Polynoms $p \in K[X] \setminus \{0\}$ ist. (D.h. es gibt ein Polynom $p \in K[X]$, $p \neq 0$ mit der Eigenschaft $p(a) = 0$.) Ist $a \in L$ nicht algebraisch über K (d.h. $p(a) \neq 0$ für alle $p \in K[X] \setminus \{0\}$), so wird a transzendent über K genannt.

Beispiele: 1) Jedes $a \in K$ ist algebraisch über dem Körper K, da es Nullstelle des Polynoms $X - a \in K[X]$ ist.
2) i ist algebraisch über $\mathbb{Q}$, da es Nullstelle des Polynoms $X^2 + 1 \in \mathbb{Q}[X]$ ist.
3) Für jedes $d \in \mathbb{Z}$ ist $\sqrt{d}$ algebraisch über $\mathbb{Q}$, da es Nullstelle von $X^2 - d \in \mathbb{Q}[X]$ ist.
4) $\sqrt[3]{2}$ ist algebraisch über $\mathbb{Q}$, da es Nullstelle des Polynoms $X^3 - 2 \in \mathbb{Q}[X]$ ist.
5) Ist $m \in \mathbb{N} \setminus \{0, 1\}$ und $\zeta \in \mathbb{C}$ eine m-te Einheitswurzel, so ist ζ algebraisch über $\mathbb{Q}$, da es Nullstelle des Polynoms $X^m - 1 \in \mathbb{Q}[X]$ ist.
6) e und π sind transzendent über $\mathbb{Q}$ (ohne Beweis), aber e und π sind algebraisch über $\mathbb{R}$, da sie Nullstellen der Polynome $X - e \in \mathbb{R}[X]$ und $X - \pi \in \mathbb{R}[X]$ sind.

Satz 195: Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K.

(i) Es gibt ein eindeutig bestimmtes normiertes Polynom $m_{a,K} \in K[X]$ minimalen Grades mit der Eigenschaft $m_{a,K}(a) = 0$,
(ii) Das Polynom $m_{a,K}$ ist irreduzibles Element des Rings $K[X]$,
(iii) Für Polynome $f \in K[X]$ gilt: $f(a) = 0 \Leftrightarrow m_{a,K} \mid f$ (Teilbarkeit in $K[X]$),
(iv) $\{f \in K[X] \mid f(a) = 0\} = (m_{a,K})$, d.h. die Menge aller Polynome in $K[X]$, deren Nullstelle a ist, ist das von $m_{a,K}$ in $K[X]$ erzeugte Hauptideal.

Beweis: (i) Da a algebraisch über K ist, gibt es ein Polynom $p \in K[X] \setminus \{0\}$ mit der Eigenschaft $p(a) = 0$ (wobei offenbar $\operatorname{grad} p \geq 1$ gelten muss). Klarerweise muss es dann auch ein derartiges Polynom mit minimalem Grad geben und wir können ab jetzt voraussetzen, dass p diese Eigenschaft besitzt. Ist $\alpha \in K \setminus \{0\}$ Leitkoeffizient von p, so ist $\alpha^{-1}p$ normiert und $\alpha^{-1}p(a) = 0$. Wir können darum ab jetzt voraussetzen, dass p außerdem normiert ist. Ist $q \in K[X]$ irgendein normiertes Polynom minimalen Grades mit $q(a) = 0$, so gilt auch $(p-q)(a) = p(a) - q(a) = 0$ und $\operatorname{grad}(p-q) < \operatorname{grad} p$. Daher ist $p - q = 0$ und daher $p = q$, d.h. das Polynom p ist eindeutig bestimmt.
(ii) Wäre $m_{a,K}$ reduzibel als Element von $K[X]$, so würde es $f, g \in K[X]$ mit den Eigenschaften $m_{a,K} = f \cdot g$, $\operatorname{grad} f \geq 1$ und $\operatorname{grad} g \geq 1$ geben. Aus $0 = m_{a,K}(a) = f(a) \cdot g(a)$ würde aber folgen, dass $f(a) = 0$ oder $g(a) = 0$. Da $\operatorname{grad} m_{a,K} = \operatorname{grad} f + \operatorname{grad} g$, wären $\operatorname{grad} f < \operatorname{grad} m_{a,K}$ und $\operatorname{grad} g < \operatorname{grad} m_{a,K}$, was der Minimalität des Grads von $m_{a,K}$ widersprechen würde.
(iii) Es sei $f \in K[X]$ und besitze die Eigenschaft $f(a) = 0$. Nach Satz 157 gibt es $q, r \in K[X]$ mit den Eigenschaften $f = q \cdot m_{a,K} + r$ und $\operatorname{grad} r < \operatorname{grad} m_{a,K}$. Aus $0 = f(a) = q(a) \cdot m_{a,K}(a) + r(a) = r(a)$ folgt $r = 0$, da sonst $\operatorname{grad} r < \operatorname{grad} m_{a,K}$ der Minimalität des Grads von $m_{a,K}$ widersprechen würde. Also gilt $m_{a,K} \mid f$. Die Umkehrung ist trivial.
(iv) Folgt sofort aus (iii).

Definition: Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Das eindeutig bestimmte Polynom $m_{a,K}$, dessen Eigenschaften in Satz 195 beschrieben wurden, wird das Minimalpolynom von a über K genannt. Man bezeichnet $\operatorname{grad} m_{a,K}$ auch als den Grad von a über K.

Korollar 196: Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Ist $p \in K[X]$ irreduzibel (als Element von $K[X]$) und normiert und $p(a) = 0$, so ist $p = m_{a,K}$.

Beweis: Wegen Satz 195 (iii) muss $m_{a,K} \mid p$ gelten, d.h. es gibt ein $q \in K[X]$ mit der Eigenschaft $p = m_{a,K} \cdot q$. Da p irreduzibel ist, muss entweder $m_{a,K} \in K \setminus \{0\}$ sein (was unmöglich ist) oder $q \in K \setminus \{0\}$ (was daher gelten muss). Da p und $m_{a,K}$ beide normiert sind, ist $q = 1$ und $p = m_{a,K}$.

Satz 197: Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Dann gelten:
(i) $K(a) = K[a]$, d.h.

$$K(a) = \{p(a) \mid p \in K[X]\} = \{b_n a^n + b_{n-1}a^{n-1} + \cdots + b_1 a + b_0 \mid b_i \in K \text{ für } 0 \leq i \leq n\},$$

(ii) $K(a) \cong K[X]/(m_{a,K})$,

(iii) $[K(a) : K] = \operatorname{grad} m_{a,K}$,
(iv) $1_K, a, a^2, \dots, a^{n-1}$ ist eine Basis von $K(a)$ als K-Vektorraum (wobei $n = \operatorname{grad} m_{a,K}$),
(v) Jedes $c \in K(a)$ besitzt eine eindeutige Darstellung $c = b_{n-1}a^{n-1} + \cdots + b_1 a + b_0$ (mit $n = \operatorname{grad} m_{K,a}$ und $b_i \in K$ für $0 \leq i \leq n-1$).

Beweis: (i) und (ii) Wir betrachten den Einsetzhomomorphismus

$$\varphi : K[X] \to K[a],\ p \mapsto p(a).$$

Nach Satz 195 (iv) ist $\ker \varphi = (m_{a,K})$. Aus dem Homomorphiesatz (Korollar 70) folgt

$$K[X]/(m_{a,K}) = K[X]/\ker \varphi \cong \operatorname{Im} \varphi = K[a].$$

Nach Satz 195 (ii) ist $m_{a,K}$ ein irreduzibles Element von $K[X]$ und nach Korollar 167 ist $K[X]$ ein Hauptidealbereich. Wegen Satz 132 (ii) ist $(m_{a,K})$ daher ein maximales Ideal des Rings $K[X]$. Daher ist $K[X]/(m_{a,K}) \cong K[a]$ (nach Satz 77) ein Körper. Da $K(a)$ der kleinste Körper ist, der K und a enthält und $K[a] (\subseteq K(a))$ bereits ein Körper ist, muss $K[a] = K(a)$ gelten.
(iii), (iv) und (v) Es sei $f(a) \in K[a] = K(a)$. Nach Satz 157 gibt es $q, r \in K[X]$ mit den Eigenschaften $f = q \cdot m_{a,K} + r$ und $\operatorname{grad} r < \operatorname{grad} m_{a,K}$. Ist

$$r(X) = \sum_{i=0}^{n-1} b_i X^i \in K[X],$$

so ist

$$f(a) = q(a) \cdot m_{a,K}(a) + r(a) = r(a) = \sum_{i=0}^{n-1} b_i a^i,$$

d.h. $1_K, a, a^2, \dots, a^{n-1}$ ist ein Erzeugendensystem von $K[a]$ als K-Vektorraum. Diese Körperelemente sind auch linear unabhängig über K. Angenommen,

$$\sum_{i=0}^{n-1} c_i a^i = 0$$

für gewisse $c_0, c_1, \dots, c_{n-1} \in K$. Setzt man

$$g(X) = \sum_{i=0}^{n-1} c_i X^i \in K[X],$$

so ist a Nullstelle von g und aus Satz 195 (iii) folgt $m_{a,K} \mid g$. Da

$$\operatorname{grad} g \leq n - 1 < n = \operatorname{grad} m_{a,K},$$

muss $g = 0$ gelten, d.h. $c_0 = c_1 = \cdots = c_{n-1} = 0$. Also ist $1_K, a, a^2, \dots, a^{n-1}$ eine Basis von $K[a]$ als K-Vektorraum. Daraus folgen $[K(a) : K] = n$ und (v).

Beispiele: 1) $m_{\sqrt{2},\mathbb{Q}}(X) = X^2 - 2$, denn $X^2 - 2$ ist irreduzibles Element von $\mathbb{Q}[X]$ nach Satz 185 und daher Minimalpolynom von $\sqrt{2}$ nach Korollar 196. Wegen Satz 197 ist

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

(wie bisher definiert), $1, \sqrt{2}$ eine Basis von $\mathbb{Q}(\sqrt{2})$ als $\mathbb{Q}$-Vektorraum und $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.
2) $m_{i,\mathbb{Q}}(X) = X^2 + 1$, denn $(X+1)^2 + 1 = X^2 + 2X + 2$ ist irreduzibles Element von $\mathbb{Q}[X]$ nach Satz 185 und daher ist (wegen Lemma 186) auch $X^2 + 1$ irreduzibles Element von $\mathbb{Q}[X]$. Wegen Satz 197 ist

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

(wie bisher definiert), $1, i$ eine Basis von $\mathbb{Q}(i)$ als $\mathbb{Q}$-Vektorraum und $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.
3) $m_{i,\mathbb{R}}(X) = X^2 + 1$, denn $X^2 + 1$ ist irreduzibles Element von $\mathbb{R}[X]$, da es keine reelle Nullstelle besitzt. Wegen Satz 197 ist

$$\mathbb{C} = \mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$$

(wie bisher definiert), $1, i$ eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum und $[\mathbb{C} : \mathbb{R}] = 2$. (All das ist natürlich längst bekannt, z.B. aus der Linearen Algebra.)
4) $m_{\sqrt[3]{2},\mathbb{Q}}(X) = X^3 - 2$, denn $X^3 - 2$ ist irreduzibles Element von $\mathbb{Q}[X]$ nach Satz 185 und daher Minimalpolynom von $\sqrt[3]{2}$ nach Korollar 196. Wegen Satz 197 ist

$$\mathbb{Q}(\sqrt[3]{2}) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \,\middle|\, a, b, c \in \mathbb{Q}\right\},$$

$1, \sqrt[3]{2}, \sqrt[3]{4}$ ist eine Basis von $\mathbb{Q}(\sqrt[3]{2})$ als $\mathbb{Q}$-Vektorraum und $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$.
5) Die komplexe Zahl $\zeta = e^{2\pi i/3}$ ist eine dritte Einheitswurzel und es gilt

$$e^{2\pi i/3} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \frac{-1 + i\sqrt{3}}{2}.$$

Offenbar gilt $p(\zeta) = 0$ für $p(X) = X^3 - 1$, allerdings ist p reduzibel, da

$$p(X) = X^3 - 1 = (X - 1)(X^2 + X + 1).$$

Da $\zeta \neq 1$, ist ζ Nullstelle von $\Phi(X) = X^2 + X + 1$. Tatsächlich ist $m_{\zeta,\mathbb{Q}}(X) = X^2 + X + 1$. Das Polynom Φ ist irreduzibles Element von $\mathbb{Q}[X]$, da

$$\Phi(X + 1) = (X + 1)^2 + (X + 1) + 1 = X^2 + 3X + 3$$

nach Satz 185 irreduzibel ist und daher (wegen Lemma 186) auch Φ irreduzibel ist. Wegen Satz 197 ist

$$\mathbb{Q}(\zeta) = \{a + b\zeta \mid a, b \in \mathbb{Q}\},$$

$1, \zeta$ ist eine Basis von $\mathbb{Q}(\zeta)$ als $\mathbb{Q}$-Vektorraum und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$.
6) Allerdings gilt $\mathbb{Q}(\zeta) = \mathbb{Q}(i\sqrt{3})$. Es ist $m_{i\sqrt{3},\mathbb{Q}} = X^2 + 3$, denn $X^2 + 3$ ist irreduzibles Element von $\mathbb{Q}[X]$ nach Satz 185 und daher Minimalpolynom von $i\sqrt{3}$ nach Korollar 196.

Wegen Satz 197 ist

$$\mathbb{Q}(i\sqrt{3}) = \{a + i\sqrt{3}b \mid a, b \in \mathbb{Q}\},$$

$1, i\sqrt{3}$ eine Basis von $\mathbb{Q}(i\sqrt{3})$ als $\mathbb{Q}$-Vektorraum und $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$. Nach Definition ist $\mathbb{Q} \subseteq \mathbb{Q}(i\sqrt{3})$ und offenbar ist

$$\zeta = -\frac{1}{2} + \frac{1}{2} \cdot i\sqrt{3} \in \mathbb{Q}(i\sqrt{3}).$$

Daher ist $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(i\sqrt{3})$. Umgekehrt gelten $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ und $i\sqrt{3} = 1 + 2 \cdot \zeta \in \mathbb{Q}(\zeta)$ und daher auch $\mathbb{Q}(i\sqrt{3}) \subseteq \mathbb{Q}(\zeta)$.

Definition: Eine Körpererweiterung L/K heißt algebraisch, wenn jedes $a \in L$ algebraisch über K ist.

Satz 198: (i) Ist die Körpererweiterung L/K endlich, so ist sie auch algebraisch.
(ii) Ist die Körpererweiterung L/K endlich und $[L : K] = m$, so gibt es algebraische $a_1, \dots, a_m \in L$, derart dass $L = K(a_1, \dots, a_m)$.
(iii) Ist die Körpererweiterung L/K algebraisch und $\exists a_1, \dots, a_m \in L : L = K(a_1, \dots, a_m)$, so ist sie endlich.

Beweis: (i) Ist $[L : K] = m$ (mit $m \in \mathbb{N} \setminus \{0\}$) und $a \in L$, so sind $1, a, a^2, \dots, a^m$ linear abhängig über K, d.h. es gibt $b_0, b_1, \dots, b_m \in K$ (die nicht alle $= 0$ sind) mit der Eigenschaft

$$b_m a^m + \cdots + b_1 a + b_0 = 0.$$

Setzt man

$$p(X) = b_m X^m + \cdots + b_1 X + b_0 \in K[X] \setminus \{0\},$$

so ist $p(a) = 0$ und a daher algebraisch über K.
(ii) Bilden $a_1, \dots, a_m$ eine K-Basis von L, so ist

$$L = Ka_1 + \cdots + Ka_m \subseteq K(a_1, \dots, a_m) \subseteq L$$

und daher $L = K(a_1, \dots, a_m)$. Nach (i) sind $a_1, \dots, a_m \in L$ algebraisch über K.
(iii) Betrachte den folgenden Turm von Körpererweiterungen:

$$K \subseteq K(a_1) \subseteq K(a_1, a_2) \subseteq \cdots \subseteq K(a_1, \dots, a_{m-1}) \subseteq K(a_1, \dots, a_m) = L$$

Für $1 \leq i \leq m$ ist a_i algebraisch über K und daher auch algebraisch über $K(a_1, \dots, a_{i-1})$. Wegen $K(a_1, \dots, a_i) = K(a_1, \dots, a_{i-1})(a_i)$ gilt

$$[K(a_1, \dots, a_i) : K(a_1, \dots, a_{i-1})] < \infty$$

nach Satz 197. Aus Satz 193 (ii) folgt nun

$$[L : K] = [K(a_1, \dots, a_m) : K] = \prod_{i=1}^{m} [K(a_1, \dots, a_i) : K(a_1, \dots, a_{i-1})] < \infty.$$

Beispiel: Wegen Satz 194 (ii) ist

$$\mathbb{Q}(\pi) = \left\{ \frac{a_n\pi^n + \cdots + a_1\pi + a_0}{b_m\pi^m + \cdots + b_1\pi + b_0} \,\middle|\, a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathbb{Q}, b_0, \ldots, b_m \text{ nicht alle } = 0 \right\}.$$

Da π transzendent ist (über $\mathbb{Q}$), ist $\mathbb{Q}(\pi)/\mathbb{Q}$ (wegen Satz 198 (i)) eine unendliche Köpererweiterung.

Satz 199: Es sei L/K eine Körpererweiterung und M ein Zwischenkörper. Dann sind äquivalent:

(i) L/K ist eine algebraische Körpererweiterung,
(ii) L/M und M/K sind beides algebraische Körpererweiterungen.

Beweis: (i) $\Rightarrow$ (ii) Ist $a \in L$, so ist a algebraisch über K und daher auch über M. Ist $a \in M$, so ist auch $a \in L$ und a daher algebraisch über K.
(ii) $\Rightarrow$ (i) Es sei $a \in L$. Da a algebraisch über M ist, $\exists p \in M[X] \setminus \{0\} : p(a) = 0$. Es sei $p(X) = b_mX^m + \cdots + b_1X + b_0$ (mit $b_0, b_1, \ldots, b_m \in M$). Dann ist a auch algebraisch über $K(b_0, \ldots, b_m)$. Wir betrachten nun den folgenden Turm von Körpererweiterungen:

$$K \subseteq K(b_0, \ldots, b_m) \subseteq K(b_0 \ldots, b_m)(a)$$

Da a algebraisch ist über $K(b_0, \ldots, b_m)$, ist

$$[K(b_0, \ldots, b_m)(a) : K(b_0, \ldots, b_m)] < \infty$$

nach Satz 197. Aus $K(b_0, \ldots, b_m) \subseteq M$ folgt, dass $K(b_0, \ldots, b_m)/K$ eine algebraische Körpererweiterung ist. Wegen Satz 198 (iii) ist $[K(b_0, \ldots, b_m) : K] < \infty$. Aus Satz 193 (ii) folgt

$$[K(b_0, \ldots, b_m)(a) : K] = [K(b_0, \ldots, b_m)(a) : K(b_0, \ldots, b_m)] \cdot [K(b_0, \ldots, b_m) : K] < \infty$$

und a ist algebraisch über K nach Satz 198 (i).

Korollar 200: Es sei L/K eine Körpererweiterung und

$$A := \{a \in L \mid a \text{ ist algebraisch über } K\}.$$

Dann ist A ein Zwischenkörper der Körpererweiterung L/K und die Körpererweiterung A/K ist algebraisch.

Beweis: Sind $a, b \in A$, so ist $K(a, b)/K$ eine endliche Körpererweiterung. (Da a algebraisch über K ist, ist $[K(a) : K] < \infty$. Da b auch über $K(a)$ algebraisch ist, ist $[K(a, b) : K(a)] = [K(a)(b) : K(a)] < \infty$.) Wegen Satz 198 (i) ist $K(a, b)/K$ eine algebraische Körpererweiterung. Daher sind $a - b, a \cdot b \in A$ algebraisch über K und A ist ein Unterring von L. Ist $a \in A \setminus \{0\}$, so ist $a^{-1} \in K(a)$ algebraisch über K und A daher ein Körper.

Definition: Es sei L/K eine Körpererweiterung. Der in Korollar 200 beschriebene Zwischenkörper $A = \{a \in L \mid a \text{ ist algebraisch über } K\}$ wird der algebraische Abschluss von K in L genannt.

Beispiele: 1) $\{a \in \mathbb{R} \mid a \text{ ist algebraisch über } \mathbb{Q}\}$ ist ein Körper. Das zeigt auch, dass Zahlen wie $\sqrt[3]{2} + \sqrt{3}$ algebraisch (über $\mathbb{Q}$) sind.
2) Ebenso ist $\{a \in \mathbb{C} \mid a \text{ ist algebraisch über } \mathbb{Q}\}$ ein Körper.