Musterlösung Serie 16

KÖRPERERWEITERUNGEN UND MINIMALPOLYNOME

---

82. Sei $L : K$ eine Körpererweiterung, $a \in L$ ein Element, und $p \in K[x]$ mit $p(a) = 0$.

(a) Beweisen Sie, dass das Minimalpolynom von a über K das Polynom p teilt.

(b) Beweisen Sie, dass der Grad des Minimalpolynoms von a den Grad $[L : K]$ teilt.

Lösung:

(a) Wir betrachten die Abbildung

$$K[x] \to L,\ x \mapsto a.$$

Dann liegt p im Kern dieser Abbildung. Sei f das Minimalpolynom von a über K, dann ist der Kern dieser Abbildung gegeben durch das Ideal (f). Also gilt $f|p$.

(b) Der Grad n des Minimalpolynoms ist $[K(a) : K]$, also erhalten wir

$$[L : K] = [L : K(a)][K(a) : K] = n[L : K(a)].$$

83. Sei $L = K(\alpha)$ mit $\alpha \neq 0$, wobei α beim irreduziblen Polynom $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ verschwindet. Bestimmen Sie eine Formel für α^{-1}, welche die Koeffizienten a_k und α verwendet.

Lösung: Das Polynom f ist irreduzibel und da $\alpha \neq 0$, folgt $a_0 \neq 0$. Es gilt

$$-a_0 = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha.$$

Wir dividieren diese Formel durch $-\alpha a_0$, dann erhalten wir

$$\alpha^{-1} = -a_0^{-1}(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1).$$

84. Seien $L : K$ und $M : K$ Körpererweiterungen und $a \in L$, $b \in M$ algebraisch über K. Beweisen Sie, a und b besitzen dasselbe Minimalpolynom, dann und nur dann falls ein Isomorphismus $\varphi\colon K(a) \to K(b)$ existiert mit $\varphi(a) = b$ und $\varphi|_K = \mathrm{id}$.

Lösung: Falls a und b dasselbe Minimalpolynom haben, dann folgt die Aussage aus Satz 14.4.

Wir nehmen an es existiert ein Isomorphismus $\varphi\colon K(a) \to K(b)$ mit $\varphi(a) = b$ und $\varphi|_K = \mathrm{id}$. Sei $f \in K[x]$ das Minimalpolynom von a. Wir schreiben $f = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Dann gilt

$$a^n + a_{n-1}a^{n-1} + \ldots + a_0 = 0.$$

Also erhalten wir

$$0 = \varphi(a^n + a_{n-1}a^{n-1} + \ldots + a_0) = b^n + a_{n-1}b^{n-1} + \ldots + a_0.$$

Also gilt $f(b) = 0$. Somit folgt aus Aufgabe 82 (a), dass das Minimalpolynom von b das Polynom f teilt. Das Polynom f und das Minimalpolynom von b sind irreduzibel und monisch, also folgt aus dieser Teilbarkeit, dass sie gleich sein müssen.

Hier ist eine zweite Lösung. Wir nehmen an es existiert ein Isomorphismus $\varphi\colon K(a) \to K(b)$ mit $\varphi(a) = b$ und $\varphi|_K = \mathrm{id}$. Wir betrachten die Abbildung

$$\psi\colon K[x] \to K(a), x \mapsto a.$$

Der Kern von ψ wird durch das Minimalpolynom von a über K generiert. Aus $\varphi|_K = \mathrm{id}$ folgt, dass die Komposition $\varphi \circ \psi$ gleich der Abbildung

$$K[x] \to K(b), x \mapsto b$$

ist. Der Kern von $\varphi \circ \psi$ wird somit durch das Minimalpolynom von b generiert. Die Abbildung φ ist ein Isomorphismus, also ist der Kern von $\varphi \circ \psi$ gleich dem Kern von ψ. Also sind die beiden Minimalpolynome gleich.

85. (a) Zeige: Ist eine Körpererweiterung $L : K$ endlich, so ist sie algebraisch und wird von endlich vielen Elementen erzeugt.

Bemerkung: Die andere Richtung wird in der Vorlesung gezeigt (siehe Satz 14.7.(b)).

(b) Seien $M : L$ und $L : K$ Körpererweiterungen.

Zeige: $M : K$ ist genau dann algebraisch, wenn $M : L$ und $L : K$ algebraisch sind.

Lösung: (a) Sei $L : K$ endlich. Dann ist L ein endlich-dimensionaler K-Vektorraum. Offensichtlich ist L über K von einer Vektorraumbasis erzeugt. Daher ist $L : K$ von endlich vielen Elementen erzeugt.

Sei nun $a \in L$. Wir müssen zeigen, dass a algebraisch über K ist. Dann sind die $[L : K] + 1$ Vektoren $1, a^1, a^2, \ldots, a^{[L:K]}$ linear abhängig. Somit existieren $\alpha_i \in K$, nicht alle gleich Null, mit $\sum_{i=0}^{[L:K]} \alpha_i a^k = 0$. Offensichtlich ist nun für $p = \sum_{i=0}^{[L:K]} \alpha_i X^k$, $p(a) = 0$, d.h. p ist ein nichtverschwindendes annulierendes Polynom von a mit Koeffizienten in K. Somit ist a algebraisch über K und die Körpererweiterung $L : K$ ist algebraisch.

(b) Sei $M : K$ algebraisch. Dann ist jedes Element von M algebraisch über K. Da wegen $K \subseteq L$ ein annulierendes Polynom mit Koeffizienten in K, alle seine Koeffizienten in L hat, ist jedes Element von M auch algebraisch über L, d.h. $M : L$ ist algebraisch.

Andererseits ist liegt wegen $L \subseteq M$ jedes Element aus L auch in M. Weil nun $M : K$ algebraisch ist, ist jedes Element von L algebraisch über K und somit ist $L : K$ algebraisch.

Seien nun $M : L$ und $L : K$ algebraisch. Sei $a \in M$. Sei $\sum_{i=0}^{n} \alpha_i X^i$ das Minimalpolynom von a über L. Wegen Aufgabe (a) gilt $[K(\alpha_0, \ldots, \alpha_n) : K] < \infty$. Ausserdem ist a algebraisch über $K(\alpha_0, \ldots, \alpha_n)$. Folglich gilt auch $[K(a, \alpha_0, \ldots, \alpha_n) : K(\alpha_0, \ldots, \alpha_n)] < \infty$.

Insgesamt folgern wir mit der Multiplikativität des Körpergrades

$$\begin{aligned}
[K(a):K] &= \frac{[K(a,\alpha_0,\ldots,\alpha_n):K]}{[K(a,\alpha_0,\ldots,\alpha_n):K(a)]} \\
&\leqslant [K(a,\alpha_0,\ldots,\alpha_n):K] \\
&= [K(a,\alpha_0,\ldots,\alpha_n):K(\alpha_0,\ldots,\alpha_n)]\cdot[K(\alpha_0,\ldots,\alpha_n):K] \\
&< \infty.
\end{aligned}$$

Somit ist a algebraisch über K, und weil $a \in M$ beliebig war, ist die Körpererweiterung $M : K$ algebraisch.

86. Berechnen Sie das Minimalpolynom von $\sqrt{3}+\sqrt{5}$ über jedem der folgenden Körper.

a) $\mathbb{Q}$ b) $\mathbb{Q}(\sqrt{5})$

c) $\mathbb{Q}(\sqrt{10})$ d) $\mathbb{Q}(\sqrt{15})$

Lösung: Wir beweisen dass eine Erweiterung $K(\sqrt{a}) : K$ Grad 2 oder Grad 1 hat. In der Tat, der Kern der Abbildung $K[x] \to K(a), x \mapsto a$ enthält $x^2 - a$. Somit teilt das Minimalpolynom von $\sqrt{a}$ über K das Polynom $x^2 - a$. Also ist das Minimalpolynom entweder linear oder quadratisch und dann hat die Erweiterung jeweils Grad 1 oder Grad 2.

Seien $a, b \in \mathbb{Q}$, so dass b kein Quadrat in $\mathbb{Q}$ ist. Wir nehmen an, die Erweiterung $\mathbb{Q}(\sqrt{a},\sqrt{b}) : \mathbb{Q}(\sqrt{b})$ hat Grad 1. Dies ist äquivalent zur Bedingung $\sqrt{a} \in \mathbb{Q}(\sqrt{b})$. Also existieren $s, t \in \mathbb{Q}$, so dass $(s + t\sqrt{b})^2 = a$. Diese Gleichung klammert aus zu

$$(s^2 + at^2) + 2st\sqrt{b} = a.$$

Die Elemente 1 und $\sqrt{b}$ sind linear unabhängig über $\mathbb{Q}$, also gilt $2st = 0$. Wir nehmen an, $t = 0$. Dann folgt $b = s^2$, also ist b ein Quadrat in $\mathbb{Q}$. Falls $t \neq 0$, dann folgt $s = 0$. Also folgt $at^2 = b$. Zusammenfassend haben wir beweisen, dass $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$ dann und nur dann falls $b = t^2$ oder $b = at^2$ für ein $t \in \mathbb{Q}$. Falls keiner dieser beider Fälle eintritt und a ist kein Quadrat in $\mathbb{Q}$, so gilt

$$[\mathbb{Q}(\sqrt{a},\sqrt{b}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a},\sqrt{b}) : \mathbb{Q}(\sqrt{a})][\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Wir definieren die Polynome

$$P_1 := x - (\sqrt{3}+\sqrt{5}) \qquad P_2 := x - (-\sqrt{3}+\sqrt{5})$$
$$P_3 := x - (\sqrt{3}-\sqrt{5}) \qquad P_4 := x - (-\sqrt{3}-\sqrt{5}).$$

Wir definieren

$$Q_0 := P_1P_2P_3P_4 = x^4 - 16x^2 + 4.$$

Also teilt jedes der Minimalpolynome, welche wir berechnen müssen, das obige Polynom. Weiters berechnen wir die Polynome

$$
\begin{aligned}
Q_1 &:= P_1 P_2 = x^2 - 2\sqrt{3}x - 2 \\
Q_2 &:= P_1 P_3 = x^2 - 2\sqrt{5}x + 2 \\
Q_3 &:= P_1 P_4 = x^2 - 2\sqrt{15} - 8.
\end{aligned}
$$

Wir bemerken, dass nach Aufgabe 82, (b) das Minimalpolynom von $\sqrt{3}+\sqrt{5}$ über jeden der Körper K aus der Aufgabe den Grad der Erweiterung $K(\sqrt{3}+\sqrt{5}) : \mathbb{Q}$ teilen muss. Dieser ist immer eine Potenz von 2, weil er in $K(\sqrt{3}, \sqrt{5})$ enthalten ist, also hat das Minmalpolynom in jeder der Aufgaben entweder Grad 1, Grad 2 oder Grad 4. Somit ist in jedem der 4 Fälle das Minmalpolynom entweder P_1, Q_0, Q_1, Q_2 oder Q_3.

Sei $K = \mathbb{Q}$. Das einzige der Polynome, welches in $\mathbb{Q}$ liegt, ist Q_0. Also ist Q_0 das Minimalpolynom.

Dies impliziert $\sqrt{3} + \sqrt{5} \notin K$ in den drei anderen Fällen, weil nun $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Die Inklusion $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq K$ ist in keinem der drei Fälle möglich, weil der $\mathbb{Q}$-Vektorraum $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ Dimension 4 und der $\mathbb{Q}$-Vektorraum K Dimension 2 hat.

Sei $K = \mathbb{Q}(\sqrt{5})$. Dann hat Q_2 Koeffizienten in K. Es gilt $\sqrt{5} + \sqrt{3} \notin K$, also ist Q_2 das Minimalpolynom.

Sei $K = \mathbb{Q}(\sqrt{10})$. Wir sehen aus den Bemerkung bei Beginn der Lösung, dass keines der Polynome $Q_1, Q_2, Q_3 \notin K[x]$. Also ist das Minimalpolynom Q_0.

Sei $K = \mathbb{Q}(\sqrt{15})$. Hier ist das Minimalpolynom nun Q_3.