Musterlösung Serie 15

ALGEBRAISCHE KÖRPERERWEITERUNGEN, IRREDUZIBLE POLYNOME

---

87. (a) Sei K ein Körper, sei $f = \sum_{i=0}^{n} a_i X^i \in K[X]$, und für $\alpha \in K$ sei

$$f(X+\alpha) := \sum_{i=0}^{n} a_i (X+\alpha)^i \in K[X]\,.$$

Zeige:

$$f \text{ ist irreduzibel über } K \iff f(X+\alpha) \text{ ist irreduzibel über } K \text{ für alle } \alpha \in K$$

(b) Zeige, dass für jede Primzahl p, $X^{p-1} + X^{p-2} + \cdots + X + 1$ irreduzibel über $\mathbb{Q}$ ist.

Hinweis: Ersetze X durch $X+1$ und verwende (a) und das Eisenstein-Schönemann Kriterium.

Lösung: (a) ($\Leftarrow$) Ist $f(X+\alpha)$ irreduzibel über K für alle $\alpha \in K$, dann erhalten wir, dass $f(X) = f(X + 0_K)$ auch irreduzibel über K ist.

($\Rightarrow$) Für die umgekehrte Implikation benutzen wir Kontraposition: Nehmen wir an, dass

$$f(X+\alpha) = \left(\sum_{i=0}^{k} b_i X^i\right)\left(\sum_{j=0}^{l} c_j X^j\right) =: p(X)\cdot q(X)$$

mit $k + l = n$ und $k, l \geqslant 1$ gilt. Dann ersetzen wir X durch

$$(\underbrace{X+\alpha}_{=:\tilde{X}}) - \alpha$$

und erhalten:

$$f(X+\alpha) = p(X)\cdot q(X) = \tilde{p}(\tilde{X})\cdot\tilde{q}(\tilde{X}) = \tilde{p}(X+\alpha)\cdot\tilde{q}(X+\alpha).$$

Schliesslich ersetzen wir wieder $X+\alpha$ durch X, und erhalten $f(X) = p(X)\cdot q(X)$, was zeigt, dass f reduzibel ist.

(b) Wir definieren $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ und zeigen, dass wir das Eisenstein-Schönemann Kriterium auf $f(X+1)$ anwenden können. Wir betrachten das Pascal'sche Dreieck und bemerken folgendes:

- Ist p eine Primzahl, so gibt es in der p-ten Zeile nur Zahlen k, so dass $p|k$ oder $k = 1$.
- Die Koeffizienten von $f(X+1) = \sum_{i=0}^{n} a'_i X^i$ sind genau $a'_{p-h} = \sum_{i=1}^{h} \binom{p-i}{h-i}$ für $1 \leqslant h \leqslant p$.

- Die Summen der Form $\sum_{i=1}^{h} \binom{p-i}{k-i}$ sind genau Summen von Elementen aus Diagonalen des Pascal'sche Dreieck (rote Elemente), und das Ergebnis davon ist immer das Element des Dreiecks links unten vom Ende der Diagonale (blaues Element).

$$
\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & \color{red}{1} & & 2 & & 1 & & & & & \\
 & & & & 1 & & \color{red}{3} & & 3 & & 1 & & & & \\
 & & & 1 & & 4 & & \color{red}{6} & & 4 & & 1 & & & \\
 & & 1 & & 5 & & 10 & & \color{red}{10} & & 5 & & 1 & & \\
 & 1 & & 6 & & 15 & & 20 & & \color{red}{15} & & 6 & & 1 & \\
1 & & 7 & & 21 & & 35 & & \color{blue}{35} & & 21 & & 7 & & 1
\end{array}
$$

Es folgt, dass wir das Eisenstein-Schönemann Kriterium auf $f(X+1)$ anwenden können. Jetzt verwenden wir (a). Da $f(X+1)$ irreduzibel über $\mathbb{Q}$ ist, ist $f(X+1+\alpha)$ für alle $\alpha \in \mathbb{Q}$ auch irreduzibel, und im Fall $\alpha = -1$ sind wir fertig.

88. Zeige, dass $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ nicht isomorph sind als Körper, aber als Vektorräume über $\mathbb{Q}$.

Lösung: $1, \sqrt{2}$ ist eine Basis des Vektorraums $\mathbb{Q}(\sqrt{2})$, und $1, \sqrt{3}$ ist eine Basis des Vektorraums $\mathbb{Q}(\sqrt{3})$. Die Abbildung $\kappa : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ zwischen den Vektorräumen $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$, welche definiert ist durch $\kappa\big(p + q\sqrt{2}\big) := p + \sqrt{3}$ ist ein Isomorphismus.

Wäre die Abbildung $\kappa : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ zwischen den Körpern $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ ein Isomorphismus, so müsste gelten $\kappa(p) = p$ für alle $p \in \mathbb{Q}$ und $\kappa(\sqrt{2}) = p + q\sqrt{3}$ für $p, q \in \mathbb{Q}$ und $q \neq 0$. Damit wäre:

$$2 = 1 + 1 = \kappa(1+1) = \kappa(2) = \kappa(\sqrt{2} \cdot \sqrt{2}) = (p + q\sqrt{3})^2 = p^2 + 3q^2 + 2pq\sqrt{3}$$

Aus $p^2 + 3q^2 + 2pq\sqrt{3} = 2$ und $q \neq 0$ folgt $p = 0$, und somit ist $3q^2 = 2$, was für $q \in \mathbb{Q}$ nicht möglich ist.

89. Zeige: $[\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}] = 8$.

Lösung: Weil $X^4 - 2$ irreduzibel ist über $\mathbb{Q}$, ist $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$, und weil $X^2 - 3$ irreduzibel ist über $\mathbb{Q}(\sqrt[4]{2})$, ist $[\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Somit ist mit dem Gradsatz für Körpererweiterungen 14.1,

$$[\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

90. Finde ein Beispiel für eine Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$ mit $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, sodass für alle $q \in \mathbb{Q}$ gilt: $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\sqrt[3]{q})$.

Lösung: Sei zum Beispiel α eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $f = X^3 + 3X + 3\mathbb{Q}[X]$ (dass f irreduzibel über $\mathbb{Q}$ ist, folgt aus dem Schönemann-Eisenstein Kriterium).

Für einen Widerspruch nehmen wir an, es gäbe ein $q \in \mathbb{Q}$, so dass gilt $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\sqrt[3]{q})$. Für $\beta := \sqrt[3]{q}$ hätten wir dann $\beta \in \mathbb{Q}(\alpha)$, $\beta^3 = q$, und $\beta \notin \mathbb{Q}$. Weil $\beta \in \mathbb{Q}(\alpha)$, ist

$$\beta = a_0 + a_1\alpha + a_2\alpha^2$$

mit $a_0, a_1, a_2 \in \mathbb{Q}$, und wir dürfen annehmen, dass $a_0 \in \{0, 1\}$ (andernfalls dividieren wir β durch a_0). Weil $\beta^3 \in \mathbb{Q}(\alpha)$, ist

$$\beta^3 = b_0 + b_1\alpha + b_2\alpha^2$$

und weil $\beta^3 \in \mathbb{Q}$ muss $b_1 = b_2 = 0$ sein. Das ist aber nur dann der Fall, wenn $a_0 = a_1 = a_2 = 0$ (also $\beta = 0$), oder $a_0 = 1$, $a_1 = a_2 = 0$ (also $\beta = 1$), oder $a_0 = 1$, $a_1 = -\frac{3\pm\sqrt{13}}{4}$, $a_2 = \frac{1}{2}$ (also $a_1 \notin \mathbb{Q}$, d.h. $\beta \notin \mathbb{Q}(\alpha)$). Alle Fälle führen somit zu einem Widerspruch.

91. (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.