Musterlösung 20

Algebraischer Abschluss und separable Polynome

1. Zeige: Sind L/K eine algebraische und M/L eine beliebige Körpererweiterung, so ist M ein algebraischer Abschluss von L genau dann, wenn M ein algebraischer Abschluss von K ist.

   Lösung: Die Körpererweiterung M/K ist gemäss Abschnitt 5.4 Proposition 7 genau dann algebraisch, wenn M/L und L/K algebraisch sind. Nach Voraussetzung ist L/K algebraisch, also ist die Bedingung „M algebraisch abgeschlossen und M/L algebraisch“ äquivalent zur Bedingung „M algebraisch abgeschlossen und M/K algebraisch“. Das bedeutet, dass M genau dann ein algebraischer Abschluss von L ist, wenn M ein algebraischer Abschluss von K ist.

2. Sei L/K eine beliebige Körpererweiterung. Die Menge $\tilde{K}$ aller über K algebraischen Elemente von L heisst *der (relative) algebraische Abschluss von K in L*. Zeige:

   (a) $\tilde{K}$ ist der eindeutige grösste Zwischenkörper von L/K, der algebraisch über K ist.

   (b) Ist L algebraisch abgeschlossen, so ist $\tilde{K}$ ein algebraischer Abschluss von K im Sinne der Vorlesung.

   (c) Gilt die Folgerung in (b) auch im Fall $\mathbb{R}/\mathbb{Q}$?

   (*d) Seien $\overline{\mathbb{Q}}$ der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{C}$, und $\overline{\mathbb{Q}}^+$ der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{R}$. Zeige $[\overline{\mathbb{Q}}/\overline{\mathbb{Q}}^+] = 2$.

   Lösung: (a) Gemäss der Bemerkung aus Kapitel 5.4 liegen Summe, Differenz, Produkt und (sofern definiert) Quotient zweier Elemente aus $\tilde{K}$ in $\tilde{K}$, also ist $\tilde{K}$ ein Zwischenkörper der Erweiterung L/K. Die Körpererweiterung $\tilde{K}/K$ ist nach Konstruktion algebraisch, denn jedes Element aus $\tilde{K}$ ist algebraisch über K. Weiters ist jedes Element aus $L \smallsetminus \tilde{K}$ transzendent über K, weshalb jeder echte Oberkörper von $\tilde{K}$ in L transzendente Elemente enthält. Somit ist $\tilde{K}$ der eindeutige grösste über K algebraische Zwischenkörper von L/K.

   (b) Sei $f \in K[X]$ ein nichtkonstantes Polynom. Da L algebraisch abgeschlossen ist, hat f eine Nullstelle a in L. Als Nullstelle von f ist a algebraisch über K und liegt deshalb in $\tilde{K}$. Somit hat jedes nichtkonstante Polynom in $K[X]$ eine Nullstelle in $\tilde{K}$. Weiters ist die Körpererweiterung $\tilde{K}/K$ gemäss (a) algebraisch. Also ist $\tilde{K}$ ein algebraischer Abschluss von K.

(c) Das Polynom $X^2 + 1 \in \mathbb{Q}[X]$ hat keine Nullstelle in $\mathbb{R}$, also ist $\tilde{\mathbb{Q}} \subset \mathbb{R}$ nicht algebraisch abgeschlossen und somit kein algebraischer Abschluss von $\mathbb{Q}$.

(*d) Nach Konstruktion ist

$$\overline{\mathbb{Q}}^+ = \{x \in \mathbb{R} : x \text{ algebraisch über } \mathbb{Q}\} = \overline{\mathbb{Q}} \cap \mathbb{R}.$$

Wegen (c) gilt $i \in \overline{\mathbb{Q}} \smallsetminus \overline{\mathbb{Q}}^+$, insbesondere ist $\overline{\mathbb{Q}}^+ \neq \overline{\mathbb{Q}}$. Betrachte nun ein beliebiges $z \in \overline{\mathbb{Q}}$. Dann ist $\bar{z}$ eine weitere Nullstelle des Minimalpolynoms von z über $\mathbb{Q}$ und liegt daher ebenfalls in $\overline{\mathbb{Q}}$. Somit liegen auch $\mathrm{Re}(z) = (z + \bar{z})/2$ und $\mathrm{Im}(z) = (z - \bar{z})/2i$ in $\overline{\mathbb{Q}}$. Da sie ausserdem reell sind, liegen sie folglich in $\overline{\mathbb{Q}}^+$. Wegen $z = \mathrm{Re}(z) + i\,\mathrm{Im}(z)$ ist die Menge $\{1, i\}$ also eine $\overline{\mathbb{Q}}^+$-Basis von $\overline{\mathbb{Q}}$. Es folgt $[\overline{\mathbb{Q}}/\overline{\mathbb{Q}}^+] = 2$.

3. Zeige, dass endliche Körper nicht algebraisch abgeschlossen sind.

   Lösung: Es gibt viele verschiedene Beweise dafür.

   Variante 1: Wir orientieren uns an Euklids Beweis für die Existenz unendlich vieler Primzahlen: Sei $\mathbb{F}$ ein endlicher Körper. Dann ist

   $$f(X) \;:=\; 1 + \prod_{a \in \mathbb{F}} (X - a) \;\in\; \mathbb{F}[X]$$

   ein wohldefiniertes normiertes Polynom über K. Nach Konstruktion gilt $f(a) = 1$ für alle $a \in \mathbb{F}$, also hat f keine Nullstelle in $\mathbb{F}$. Dies zeigt, dass $\mathbb{F}$ nicht algebraisch abgeschlossen ist.

   Variante 2: Sei $\mathbb{F}$ ein endlicher Körper der Ordnung q. Wähle eine zu q teilerfremde natürliche Zahl $n > q$, zum Beispiel $n = q + 1$. Betrachte das Polynom $f(X) := X^n - 1$. Dann ist $f'(X) = nX^{n-1}$ ungleich 0 und teilerfremd zu $f(X)$. Folglich ist f separabel, also haben alle seine Nullstellen die Multiplizität 1. Aber f hat Grad n und höchstens q Nullstellen in $\mathbb{F}$; deshalb kann es nicht über $\mathbb{F}$ in Linearfaktoren zerfallen. Folglich ist $\mathbb{F}$ nicht algebraisch abgeschlossen.

4. Sei $h \in K[X]$ ein grösster gemeinsamer Teiler zweier Polynome $f, g \in K[X] \smallsetminus \{0\}$. Zeige: Für jeden Oberkörper L/K ist h auch ein grösster gemeinsamer Teiler von f und g in $L[X]$.

   Lösung: Nach Voraussetzung gilt $h|f$ und $h|g$ in $K[X]$, also existieren Polynome $p, q \in K[X]$ mit $f = ph$ und $g = qh$. Dies sind Gleichungen in $K[X]$, sie gelten aber genauso in $L[X]$. Folglich gilt auch $h|f$ und $h|g$ in $L[X]$. Ist $\tilde{h}$ ein grösster gemeinsamer Teiler von f und g in $L[X]$, so gilt folglich auch $h|\tilde{h}$ in $L[X]$.

   Andererseits existieren nach dem chinesischen Restsatz Polynome $u, v \in K[X]$ mit $h = uf + vg$. Dies ist wieder eine Gleichung in $K[X]$, sie gilt aber genauso in $L[X]$. Wegen $\tilde{h}|f$ und $\tilde{h}|g$ in $L[X]$ folgt daraus auch $\tilde{h}|h$ in $L[X]$.

   Aus $h|\tilde{h}|h$ in $L[X]$ folgt nun $\tilde{h} \sim h$ in $L[X]$. Mit $\tilde{h}$ ist somit auch h ein grösster gemeinsamer Teiler von f und g in $L[X]$.

5. Für welche Primzahlen p ist das Polynom $f(X) := X^3 + X + 3 \in \mathbb{F}_p[X]$ separabel?

   Lösung: Für $p = 2$ sind $f(X) = X^3 + X + 1$ und $f'(X) = X^2 + 1 = (X + 1)^2$ teilerfremd, da f keine Nullstellen in $\mathbb{F}_2$ hat, jedoch f' vollständig in Linearfaktoren zerfällt. Also ist $f \in \mathbb{F}_2[X]$ separabel.

   Für $p = 3$ ist $f'(X) = 1$, also sind f und f' teilerfremd und $f \in \mathbb{F}_3[X]$ ist separabel.

   Sei nun $p > 3$. Wir untersuchen die Teilerfremdheit von f und f' mit dem Euklidischen Algorithmus:

$$\begin{aligned}
\mathrm{ggT}(f(X), f'(X)) &\sim \mathrm{ggT}(X^3 + X + 3, 3X^2 + 1) \\
&\overset{3\neq 0}{\sim} \mathrm{ggT}(3X^3 + 3X + 9, 3X^2 + 1) \\
&\sim \mathrm{ggT}(3X^2 + 1, 2X + 9) \\
&\overset{2,3\neq 0}{\sim} \mathrm{ggT}(6X^2 + 2, 6X + 27) \\
&\sim \mathrm{ggT}(2X + 9, -27X + 2) \\
&\overset{2,3\neq 0}{\sim} \mathrm{ggT}(54X + 243, 54X - 4) \\
&\sim \mathrm{ggT}(247, 54X - 4) \\
&\overset{2,3\neq 0}{\sim} \begin{cases} X - 2/27 & \text{falls } p|247, \\ 1 & \text{sonst.} \end{cases}
\end{aligned}$$

   Wegen $247 = 13 \cdot 19$ sind also f und f' genau dann teilerfremd, wenn $p \neq 13, 19$ ist. Somit ist f inseparabel in $\mathbb{F}_{13}[X]$ und $\mathbb{F}_{19}[X]$, und in allen anderen $\mathbb{F}_p[X]$ ist es separabel.

*6. Sei K ein Körper, und betrachte den Ring $R := K[T]/(T^n)$ für ein $n \geqslant 2$. Konstruiere ein normiertes Polynom in $R[X]$, welches verschiedene Zerlegungen in normierte Linearfaktoren besitzt, die nicht durch Vertauschung ineinander übergehen.

   Lösung: Sei $\varepsilon \in R$ die Restklasse des Elements T^{n-1}. Dann gilt $\varepsilon \neq 0$ und $\varepsilon^2 = 0$. Folglich ist $(X + \varepsilon)(X - \varepsilon) = X^2 - \varepsilon^2 = (X - 0)^2$.