Musterlösung Serie 21

Algebraischer Abschluss, 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 Proposition 3.4.10 der Vorlesung 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. Betrachte eine algebraische Körpererweiterung L/K eine mit der Eigenschaft, dass jedes irreduzible Polynom in $K[X]$ über L in Linearfaktoren zerfällt. Zeige, dass L ein algebraischer Abschluss von K ist.

   (*Hinweis:* Später werden wir sehen, dass es sogar genügt, dass jedes irreduzible Polynom in $K[X]$ eine Nullstelle in L hat.)

   Lösung: Betrachte eine algebraische Erweiterung L'/L und ein Element $a \in L$. Sei $f \in K[X]$ das Minimalpolynom von a über K. Nach Voraussetzung zerfällt dieses in Linearfaktoren über L. Über L' haben wir aber $f(a) = 0$, folglich ist einer dieser Linearfaktoren gleich $X - a$. Da alle Linearfaktoren schon in $L[X]$ liegen, folgt daraus $a \in L$. Da a beliebig war, haben wir daher $L' = L$. Somit ist L algebraisch abgeschlossen und damit ein algebraischer Abschluss von K.

3. 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) Die Menge $\tilde{K}$ ist der eindeutige grösste Zwischenkörper von L/K, der über K algebraisch ist.

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

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

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

   Lösung: (a) Gemäss Bemerkung 3.4.7 der Vorlesung 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. Da alle Elemente von $\tilde{K}$ algebraisch über

K sind, ist $\tilde{K}/K$ algebraisch. Ausserdem 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) Nach (a) ist $\tilde{K}/K$ eine algebraische Körpererweiterung. Sodann sei $f \in \tilde{K}[X]$ ein nichtkonstantes Polynom. Da L algebraisch abgeschlossen ist, hat f eine Nullstelle a in L. Als Nullstelle von f ist a algebraisch über $\tilde{K}$. Somit ist $\tilde{K}(a)/\tilde{K}$ eine algebraische Körpererweiterung. Da schon $\tilde{K}/K$ algebraisch ist, folgt dasselbe für $\tilde{K}(a)/K$; also ist a algebraisch über K. Nach Konstruktion von $\tilde{K}$ bedeutet dies aber $a \in \tilde{K}$. Daher ist $\tilde{K}$ algebraisch abgeschlossen. Insgesamt zeigt dies, dass $\tilde{K}$ ein algebraischer Abschluss von K ist.

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

(*d) Nach Konstruktion ist $\overline{\mathbb{Q}}^+ = \overline{\mathbb{Q}} \cap \mathbb{R}$. 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 $[\overline{\mathbb{Q}}/\overline{\mathbb{Q}}^+] = 2$.

*4. 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 normiertes Polynom vom Grad $|\mathbb{F}| \geqslant 2$ über K. Nach Konstruktion gilt dann $f(a) = 1$ für alle $a \in \mathbb{F}$, also hat f keine Nullstelle in $\mathbb{F}$. Somit ist $\mathbb{F}$ nicht algebraisch abgeschlossen.

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.

*5. Sei $\overline{K}$ ein algebraischer Abschluss eines unendlichen Körpers K. Zeige $|\overline{K}| = |K|$.

Lösung: Ordnen wir jedem $a \in \overline{K}$ sein Minimalpolynom über K zu, so erhalten wir eine Abbildung $\chi\colon \overline{K} \to K[X]$ mit $|\chi^{-1}(f)| \leqslant \deg(f) < \infty$ für alle $f \in K[X]$. Daher gilt im Sinne unendlicher Kardinalzahlen

$$|\overline{K}| \;\leqslant\; \sum_{d\geqslant 1} d \cdot |K[X]_{\leqslant d}| \;=\; \sum_{d\geqslant 1} d \cdot |K|^{d+1}.$$

Da K unendlich ist, gilt nun aber $|K|^2 = |K|$ und nach Induktion über d folglich auch $|K|^{d+1} = |K|$. Andererseits haben wir $\sum_{d\geqslant 1} d = |\mathbb{N}|$. Weil K unendlich ist, folgt daraus insgesamt

$$|\overline{K}| \;\leqslant\; \sum_{d\geqslant 1} d \cdot |K| \;=\; |\mathbb{N}| \cdot |K| \;\leqslant\; |K|^2 \;=\; |K|.$$

Wegen $K \subset \bar{K}$ gilt sowieso die umgekehrte Ungleichung; also folgt $|\overline{K}| = |K|$.

*6. Zeige, dass eine endliche einfache Körpererweiterung $K(a)/K$ nur endlich viele Zwischenkörper K' besitzt.

(*Hinweis:* Untersuche das Minimalpolynom von a über K'.)

Lösung: Setze $L := K(a)$ und betrachte einen beliebigen Zwischenkörper K'. Sei $g \in K'[X]$ das Minimalpolynom von a über K'. Schreibe $g(X) = \sum_{i=0}^{m} b_i X^i$ mit $b_i \in K'$, und betrachte den Zwischenkörper $K'' := K(b_0, b_1, \ldots, b_m)$. Dann gilt $K \subset K'' \subset K'$, und da g irreduzibel über K' ist, ist es erst recht irreduzibel über K''. Nun gilt aber $L = K(a) = K''(a) = K'(a)$, und deshalb $[L/K''] = \deg(g) = [L/K']$. Wegen $[L/K''] = [L/K'] \cdot [K'/K'']$ folgt daraus $[K'/K''] = 1$ und daher $K'' = K'$. Somit ist der Zwischenkörper K' durch g eindeutig bestimmt.

Nun sei $f \in K[X]$ das Minimalpolynom von a über K. Sei $\overline{K}$ ein algebraischer Abschluss von L, und sei $f(X) = \prod_{i=1}^{n}(X - a_i)$ mit Elementen $a_i \in \overline{K}$. (Hier genügt auch ein Zerfällungskörper von f über L.) Wegen $f(a) = 0$ ist g dann ein normierter Teiler von f in $K'[X]$. Somit ist $g(X) = \prod_{i\in I}(X - a_i)$ für eine gewisse Teilmenge $I \subset \{1, \ldots, n\}$. Insbesondere gibt es nur endlich viele Möglichkeiten für g, und damit auch für K', wie zu zeigen war.

7. 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 $L[X]$.

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

   Lösung: In allen Fällen gilt $f'(X) = 3X^2 + 1$.

   Für $p = 2$ ist $f'(X) = X^2 + 1 = (X-1)^2$, wegen $f(1) = 5 = 1$ aber $(X-1) \nmid f(X)$. Somit sind f und f' teilerfremd und daher $f \in \mathbb{F}_2[X]$ 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:

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

   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.