Algebra I

Musterlösung 16

Einheitswurzeln, algebraischer Abschluss

Sei p eine Primzahl.

95. Sei K ein Körper der Charakteristik 0 oder $p > 0$. Sei $n \in \mathbb{N}$. Falls $\mathrm{char}(K) = p$ nehmen wir an, dass $p \nmid n$ gilt.

(a) Zeige: Es gibt genau n paarweise verschiedene n-te Einheitswurzeln.

(b) Zeige: Die n-ten Einheitswurzeln bilden eine zyklische Untergruppe von $(K^*, \cdot)$.
Bemerkung: Die Erzeuger dieser Gruppe heissen *primitive n-te Einheitswurzeln*.

(c) Sei $\varphi(n) := |\{m \in \mathbb{N} : m \leq n, \, \mathrm{ggT}(m, n) = 1\}|$ die *Eulersche φ-Funktion*.
Zeige: Die Anzahl der primitiven n-ten Einheitswurzeln ist $\varphi(n)$.

Lösung: (a) Wir müssen zeigen, dass das Polynom $X^n - 1$ keine mehrfachen Nullstellen hat. Laut Vorlesung ist das äquivalent dazu, dass es teilerfremd zu seiner Ableitung nX^{n-1} ist. Da die Charakteristik von K kein Teiler von n ist, verschwindet die Ableitung nicht, sondern ihre einziger irreduzibler Teiler ist, bis auf Assoziiertheit, X. Allerdings teilt X das Polynom $X^n - 1$ nicht, somit sind wir fertig.

(b) Offensichtlich handelt es sich um eine zyklische Untergruppe von $(K^*, \cdot)$. Dass sie zyklisch ist, folgt verbatim nach der Lösung der Aufgabe 54, wobei $\mathbb{F}^*$ durch die Menge der n-ten Einheitswurzeln ersetzt wird.

(c) Gesucht ist also die Anzahl der Erzeuger der zyklischen Gruppe $\mathbb{Z}/n\mathbb{Z}$. Aus der Algebra I wissen wir, dass diese gleich $\varphi(n)$ ist. Siehe dazu auch Aufgabe 51.

96. Sei K ein Körper. Zeige: Die folgenden beiden Aussagen sind äquivalent.

i. Der Körper K ist algebraisch abgeschlossen.

ii. Es existiert ein Unterkörper $K_0 \subset K$, sodass die Erweiterung $K : K_0$ algebraisch ist und jedes Polynom in $K_0[X]$ über K zerfällt.

Lösung: Die Richtung i. $\Rightarrow$ ii. folgt mit $K_0 := K$.

Für die andere Richtung, sei $f \in K[X]$ irreduzibel. Sei α eine Nullstelle von f in einem Zerfällungskörper von f. Dann ist α algebraisch über K, also auch über K_0, und hat folglich ein Minimalpolynom g über K_0. Nach dem Euklidischen Algorithmus gibt es Polynome $q, r \in K[X]$ mit $g = qf + r$ und $\deg(r) < \deg(f)$ oder $r = 0$. An α ausgewertet sehen wir, dass r ein annullierendes Polynom für α sein muss. Da f aber minimalen Grad hat, impliziert das $r = 0$. Somit teilt f das Polynom g. Nach Voraussetzung zerfällt $g \in K_0[X]$ über K in Linearfaktoren. Dann muss aber auch f zerfallen. Somit ist K algebraisch abgeschlossen.

97. 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 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 $L : K$. Die Körpererweiterung $\tilde{K} : K$ ist nach Konstruktion algebraisch, denn jedes Element aus $\tilde{K}$ ist algebraisch über K. Weiters ist jedes Element aus $L \setminus \tilde{K}$ 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 $i \in \overline{\mathbb{Q}} \setminus \overline{\mathbb{Q}}^+$, 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 $[\overline{\mathbb{Q}} : \overline{\mathbb{Q}}^+] = 2$.

98. 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.

99. Sei $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss von $\mathbb{F}_p$. Sei $n \geq 1$ eine natürliche Zahl.

Wie viele Unterkörper der Kardinalität p^n enthält $\overline{\mathbb{F}_p}$?

Lösung: Seien $K, L \subset \overline{\mathbb{F}_p}$ zwei Körper der Kardinalität p^n. Beide Körper sind laut Vorlesung Zerfällungskörper von $X^{p^n} - X$, und jedes ihrer Elemente ist Nullstelle dieses Polynoms. Da dieses Polynom in $\overline{\mathbb{F}_p}[X]$ nur p^n Nullstellen hat, müssen K und L somit dieselben Elemente haben. Sie sind also gleich.