

Musterlösung Serie 20

ALGEBRAISCHER ABSCHLUSS

100. (a) Sei R ein kommutativer Ring. Beweisen Sie mit dem Teichmüllerprinzip, dass jedes echte Ideal in R zu einem maximalen Ideal erweitert werden kann.

Bemerkung: Es gilt auch die Umkehrung.

- (b) Beweisen Sie mit (a), dass jeder Körper einen algebraischen Abschluss besitzt.

Lösung:

- (a) Sei $I \subsetneq R$ ein echtes Ideal in R und sei $\mathcal{G}$ die Familie aller Mengen $X \subseteq R$, sodass $1 \notin (X \cup I)$, d.h. das von $X \cup I$ erzeugte Ideal ist ein echtes Ideal in R . Dann hat $\mathcal{G}$ endlichen Charakter und mit dem Teichmüllerprinzip existiert ein maximales Element $\mathfrak{m} \in \mathcal{G}$. Aus der Maximalität der Menge $\mathfrak{m} \in \mathcal{G}$ folgt, dass $\mathfrak{m}$ ein maximales Ideal ist welches I enthält.
- (b) Sei K ein Körper. Wir wenden die Konstruktion aus der Vorlesung an. Auf Seite 114e in Kapitel 17 wurden ein Ring $K[Z]$ und ein Ideal $I \subseteq K[Z]$ definiert. Aus Aufgabe (a) folgt nun, dass ein maximales Ideal $\mathfrak{m} \subseteq K[Z]$ existiert mit $I \subseteq \mathfrak{m}$. Wir definieren $L := K[Z]/\mathfrak{m}$. Dies ist ein Körper weil $\mathfrak{m}$ maximal ist. Sei $u \in K[X]$ ein Polynom. Dann gilt in $L[X]$ die Gleichung

$$u = \prod_{i=1}^{\deg u} (X - z_u^{(i)})$$

aufgrund der Vieta-Relationen (Serie 17, Aufgabe 87) und der Definition von I . Also zerfällt u in Linearfaktoren. Das Argument in Aufgabe 101 beweist, dass L/K algebraisch ist. Also ist L/K ein algebraischer Abschluss.

101. Beweisen Sie die Behauptung 3 im Beweis der Existenz eines algebraischen Abschlusses. Das heisst, beweisen Sie, dass die konstruierte Erweiterung algebraisch ist.

Lösung: Sei $\alpha \in \text{Quot}(K[Z]/\mathfrak{p})$. Dann existieren $f, g \in K[Z]/\mathfrak{p}$ mit

$$\alpha = \frac{f}{g}.$$

Da die Quotientenabbildung surjektiv ist, existieren Polynome $\tilde{f}, \tilde{g} \in K[Z]$, mit

$$\tilde{f} \equiv f \pmod{\mathfrak{p}}$$

und

$$\tilde{g} \equiv g \pmod{\mathfrak{p}}.$$

Nun haben die Polynome $\tilde{f}$ und $\tilde{g}$ nur endlich viele Monome, also existiert eine endliche Untermenge $Z_0 \subseteq Z$ mit $\tilde{f}, \tilde{g} \in K[Z_0]$. Die obige Gleichung impliziert $\alpha \in K(z : z \in Z_0)$. Also reicht es aus zu beweisen, dass jedes $z_u^{(m)}$ algebraisch über K ist, weil dann liegt α in einer endlichen Erweiterung von K .

Die Vieta-Relationen (siehe Serie 17, Aufgabe 87) implizieren

$$u(x) = \prod_i (x - z_u^{(i)})$$

in $(K[Z]/\mathfrak{p})[x]$. Insbesondere folgt nun

$$u(z_u^{(i)}) = 0$$

für alle i . Das Polynom u hat Koeffizienten in K , also ist $z_u^{(i)}$ algebraisch über K .

102. 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* . Zeigen Sie:

- (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.h. für $L = \mathbb{R}$ und $K = \mathbb{Q}$)?
- (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 $z \in \overline{\mathbb{Q}} \setminus \overline{\mathbb{Q}}^+$. Dann ist das konjugiert komplexe $\bar{z}$ eine weitere Nullstelle des Minimalpolynoms von z über $\mathbb{Q}$ und liegt daher ebenfalls in $\overline{\mathbb{Q}}$. Somit liegen auch $r_1 := \operatorname{Re}(z) = (z + \bar{z})/2$ und $r_2 := \operatorname{Im}(z) = (z - \bar{z})/2i$ in $\overline{\mathbb{Q}}$. Da nun r_1 und r_2 reell und algebraisch über $\mathbb{Q}$ sind, liegen r_1 und r_2 somit in $\overline{\mathbb{Q}}^+$. Wegen $z = r_1 + i \cdot r_2$, ist die Menge $\{1, i\}$ also eine $\overline{\mathbb{Q}}^+$ -Basis von $\overline{\mathbb{Q}}$. Somit ist $[\overline{\mathbb{Q}} : \overline{\mathbb{Q}}^+] = 2$.

103. Sei p eine Primzahl. In dieser Aufgabe konstruieren wir einen algebraischen Abschluss von $\mathbb{F}_p$ ohne das Primidealtheorem zu verwenden.

(a) Konstruieren Sie für jedes $n \geq 1$ einen Körperhomomorphismus

$$\varphi_n: \mathbb{F}_{p^{n!}} \rightarrow \mathbb{F}_{p^{(n+1)!}}.$$

(b) Für $n \geq m$ definieren wir nun die Abbildung

$$\varphi_{mn}: \mathbb{F}_{p^{m!}} \rightarrow \mathbb{F}_{p^{n!}}$$

als die Verknüpfung $\varphi_{n-1}\varphi_{n-2}\cdots\varphi_m$ wobei $\varphi_{nn} = \text{id}$. Wir definieren die Quotientenmenge

$$\overline{\mathbb{F}}_p := \left(\bigsqcup_{i=1}^{\infty} \mathbb{F}_{p^{i!}} \right) / \sim$$

wobei $\sim$ folgende Äquivalenzrelation ist: Sei $x \in \mathbb{F}_{p^{n!}}$ und $y \in \mathbb{F}_{p^{m!}}$. Dann gilt $x \sim y$ dann und nur dann falls für alle $N \geq \max(n, m)$ die Gleichung $\varphi_{nN}(x) = \varphi_{mN}(y)$ gilt. Konstruieren Sie eine Addition und eine Multiplikation auf $\overline{\mathbb{F}}_p$.

(c) Nehmen Sie an, dass die Menge $\overline{\mathbb{F}}_p$ mit Ihrer Addition und Multiplikation ein kommutativer Ring ist. Beweisen Sie, dass $\overline{\mathbb{F}}_p$ ein Körper ist.

(d) Beweisen Sie, dass $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$ ist.

Lösung:

(a) Sei $n \geq 1$. Wir betrachten den Unterkörper

$$k := \{x \in \mathbb{F}_{p^{(n+1)!}} : x^{p^{n!}} = x\}.$$

Dies ist ein Unterkörper weil die Frobeniusabbildung ein Körperhomomorphismus ist. Die Elemente dieses Körpers sind genau die Nullstellen von $X^{p^{n!}} - X$. Dieses Polynom teilt $X^{p^{(n+1)!}} - X$, also hat der Körper k genau $p^{n!}$ Elemente. Nun erhalten wir aus Aufgabe 91 (b), Serie 18 einen Isomorphismus

$$\mathbb{F}_{p^{n!}} \rightarrow k.$$

Wir verknüpfen diesen Isomorphismus mit der natürlichen Inklusion $k \rightarrow \mathbb{F}_{p^{(n+1)!}}$ und erhalten so den gewünschten Körperhomomorphismus

$$\varphi_n: \mathbb{F}_{p^{n!}} \rightarrow \mathbb{F}_{p^{(n+1)!}}.$$

(b) Sei $0 \in \mathbb{F}_p$ und $1 \in \mathbb{F}_p$ das Null- und Einselement. Die Äquivalenzklassen dieser Elemente in $\overline{\mathbb{F}}_p$ bezeichnen wir mit $[0]$ und $[1]$.

Sei $x_0 \in \overline{\mathbb{F}}_p$ und $y_0 \in \overline{\mathbb{F}}_p$. Dann existieren $n, m \geq 1$, $x \in \mathbb{F}_{p^{n!}}$, $y \in \mathbb{F}_{p^{m!}}$, so dass $x_0 = [x]$ und $y_0 = [y]$. Dann existiert $N \geq 1$, so dass $N \geq n$ und $N \geq m$. Wir definieren

$$x_0 + y_0 := [\varphi_{nN}(x) + \varphi_{mN}(y)]$$

und

$$x_0 \cdot y_0 := [\varphi_{nN}(x) \cdot \varphi_{mN}(y)].$$

Wir beweisen nun, dass die Addition wohldefiniert ist. Für die Multiplikation kann man ähnlich argumentieren. Zuerst beweisen wir, dass die obige Definition nicht von der Wahl von N abhängig ist. Sei $N' \geq N$, dann gilt

$$[\varphi_{nN}(x) + \varphi_{mN}(y)] = [\varphi_{nN'}(\varphi_{nN}(x) + \varphi_{mN}(y))] = [\varphi_{nN'}(x) + \varphi_{mN'}(y)].$$

Also können wir bei fixierten Repräsentanten x und y die Zahl N beliebig gross wählen. Seien $\tilde{x} \in \mathbb{F}_{p^{\tilde{n}}!}$, $\tilde{y} \in \mathbb{F}_{p^{\tilde{m}}!}$ mit $x_0 = [\tilde{x}]$ und $y_0 = [\tilde{y}]$. Wir wählen ein $N \geq 1$ mit $N \geq \max(m, n, \tilde{m}, \tilde{n})$. Dann gilt $\varphi_{nN}(x) = \varphi_{\tilde{n}N}(\tilde{x})$ und $\varphi_{mN}(y) = \varphi_{\tilde{m}N}(\tilde{y})$ nach Definition der Äquivalenzrelation. Also erhalten wir nun

$$[\varphi_{nN}(x) + \varphi_{mN}(y)] = [\varphi_{\tilde{n}N}(\tilde{x}) + \varphi_{\tilde{m}N}(\tilde{y})].$$

Dies besagt, dass die Definition der Addition unabhängig von den gewählten Repräsentanten x und y ist. Also sind die Addition und die Multiplikation wohldefiniert.

- (c) Sei $x \in \overline{\mathbb{F}}_p$ ein Element mit $x \neq [0]$. Dann existiert $n \geq 1$ und $y \in \mathbb{F}_{p^{n!}}$, so dass $x = [y]$. Nun kann nicht $y = 0$ gelten, weil dies würde $x = [0]$ implizieren. Nun gilt

$$x[y^{-1}] = [yy^{-1}] = [1].$$

Also ist $\overline{\mathbb{F}}_p$ ein Körper.

- (d) Wir haben Abbildungen

$$i_n: \mathbb{F}_{p^{n!}} \rightarrow \overline{\mathbb{F}}_p, x \mapsto [x].$$

Nach der Definition der Addition, der Multiplikation, und dem Einselement sind diese Abbildungen Körperhomomorphismen. Insbesondere ist $\overline{\mathbb{F}}_p$ eine Erweiterung von $\mathbb{F}_p$.

Um zu beweisen, dass $\overline{\mathbb{F}}_p$ ein algebraisch abgeschlossener Körper ist, reicht es aus zu beweisen, dass dieser algebraisch über $\mathbb{F}_p$ ist und dass das Polynom $X^{p^n} - X$ über $\overline{\mathbb{F}}_p$ mindestens p^n verschiedene Nullstellen hat. Dies folgt aus Aufgabe 95 (b), Serie 18.

Sei $x_0 \in \overline{\mathbb{F}}_p$. Dann existiert $n \geq 1$ und $x \in \mathbb{F}_{p^{n!}}$ mit $x_0 = [x]$. Also gilt $x^{p^{n!}} - x = 0$. Nun gilt

$$x_0^{p^{n!}} - x_0 = [x^{p^{n!}} - x] = [0].$$

Also ist dies eine algebraische Erweiterung.

Das Polynom $X^{p^n} - X$ zerfällt über $\mathbb{F}_{p^{n!}}$ und der Körperhomomorphismus i_n bildet eine Nullstelle des Polynoms auf eine Nullstelle des Polynoms ab. Also hat das Polynom p^n Nullstellen in $\overline{\mathbb{F}}_p$, da es p^n verschiedene Nullstellen in $\mathbb{F}_{p^{n!}}$ hat und i_n injektiv ist.