C. Dietzel, M. Künzer

Algebra für Lehramt, SoSe 20

Lösung 12

Aufgabe 45 Sei K ein algebraisch abgeschlossener Körper.
Sei $n \geqslant 1$. Sei $M_n := \{\, y \in K \,:\, y^n = 1 \,\}$.

(1) Ist M_n eine endliche Untergruppe von $\mathrm{U}(K)$?

(2) Sei $\mathrm{char}(K) = 0$.
Gibt es ein $\zeta \in K$ derart, daß in $K[X]$ sich $X^n - 1 \;=\; \prod_{k\in[0,n-1]}(X - \zeta^k)$ ergibt?

(3) Sei $\mathrm{char}(K) = 3$. Man bestimme $|M_6|$.

(4) Sei $\mathrm{char}(K)$ beliebig.
Gibt es ein $\zeta \in K$ derart, daß in $K[X]$ sich $X^n - 1 \;=\; \prod_{k\in[0,n-1]}(X - \zeta^k)$ ergibt?

Lösung zu Aufgabe 45:

(1) Ja. Die Teilmenge M_n ist in der Tat eine endliche Untergruppe von $\mathrm{U}(K)$.

Es ist $f : \mathrm{U}(K) \to \mathrm{U}(K) : y \mapsto y^n$ ein Abbildung, da für $y \in \mathrm{U}(K) = K^\times$ auch $y^n \in \mathrm{U}(K) = K^\times$ liegt.

Es ist f ein Gruppenmorphismus, da $f(y_1 \cdot y_2) = (y_1 \cdot y_2)^n = y_1^n \cdot y_2^n = f(y_1) \cdot f(y_2)$ ist.

Es ist $M_n = \mathrm{Kern}(f)$ also ein Normalteiler in $\mathrm{U}(K)$, was wegen $\mathrm{U}(K)$ abelsch gerade auf $M_n \leqslant \mathrm{U}(K)$ hinausläuft.

Endlichkeit: Ist $y \in M_n$, so ist y eine Nullstelle des Polynoms $X^n - 1 \in K[X]$. Da dieses maximal n Nullstellen besitzt (Bemerkung 205), ist $|M_n| \leqslant n$. Insbesondere ist M_n endlich.

(2) Ja. Wir zeigen zuerst, dass das Polynom $f(X) := X^n - 1 \in K[X]$ quadratfrei ist. Es ist $f'(X) = nX^{n-1}$. Es ist

$$1 = -(X^n - 1) + \frac{1}{n}X \cdot nX^{n-1} = -f(X) + \frac{1}{n}X \cdot f'(X),$$

also ist $\mathrm{ggT}(f(X), f'(X)) = 1$.

> Alternativ kann man auch anführen, daß $f(X)$ nicht durch X teilbar ist und daß dies der einzige normierte irreduzible Teiler von $f'(X)$ ist.

Nach Lemma 215.(1) ist $f(X)$ quadratfrei, hat also n paarweise verschiedene Nullstellen, da K algebraisch abgeschlossen ist.

Nun ist M_n die Menge der Nullstellen von $f(X)$ (s. Teil (1) der Aufgabe), also ist $|M_n| = n$.

Da M_n eine endliche Untergruppe von $\mathrm{U}(K)$ ist, ist M_n nach Lemma 206 zyklisch. Sei $\zeta \in M_n$ so, dass $M_n = \langle\zeta\rangle$ ist. Mit einem solchen ζ ist

$$M_n = \{\zeta^k : k \in [0, n-1]\}.$$

Folglich ist

$$\begin{aligned} X^n - 1 &= \prod_{y\in M_n}(X - y) \\ &= \prod_{k\in[0,n-1]}(X - \zeta^k). \end{aligned}$$

(3) Es ist $y \in M_6$ genau dann, wenn y Nullstelle des Polynoms $f(X) := X^6 - 1$ ist. Da $\mathrm{char}(K) = 3$ ist, können wir $f(X)$ über K in folgender Weise faktorisieren:

$$X^6 - 1 = (X^2)^3 - 1^3 = (X^2 - 1)^3 = ((X + 1) \cdot (X - 1))^3 = (X + 1)^3 \cdot (X - 1)^3.$$

Es hat $f(X)$ also gerade die Nullstellen 1 und -1. Da $1 \neq -1$ in K gilt, ist $M_6 = \{1, -1\}$. Demnach ist $|M_6| = 2$.

(4) Ja. Dank (2) ist der Fall $\mathrm{char}(K) = 0$ erledigt, und wir dürfen $p := \mathrm{char}(K) > 0$ voraussetzen. Es ist p prim.

Wir schreiben $n = p^t m$ mit $m \not\equiv_p 0$.

Wir zeigen zuerst, dass das Polynom $f(X) = X^m - 1 \in K[X]$ quadratfrei ist und demnach m paarweise verschiedene Nullstellen in K besitzt: Es ist $f'(X) = mX^{m-1}$. Da $m \not\equiv_p 0$ ist, ist $m \neq 0$ in K. Folglich ist

$$1 = -(X^m - 1) + \frac{1}{m} X \cdot mX^{m-1} = -f(X) + \frac{1}{m} X \cdot f'(X),$$

woraus $\mathrm{ggT}(f(X), f'(X)) = 1$ folgt, und somit $f(X)$ nach Lemma 215.(1) quadratfrei ist.

Es hat also M_m als Nullstellenmenge von $f(X)$ genau m Elemente. Weiterhin ist M_m nach Lemma 206 eine zyklische Untergruppe von $\mathrm{U}(K)$. Es gibt also ein $\zeta \in M_m$ so, dass $M_m = \langle \zeta \rangle$ ist. Für dieses ζ gilt

$$M_m = \{\zeta^k : k \in [0, m-1]\}.$$

Es ist also

$$\begin{aligned} X^m - 1 &= \prod_{y \in M_m} (X - y) \\ &= \prod_{k \in [0, m-1]} (X - \zeta^k). \end{aligned}$$

In $K[X]$ haben wir die Identität

$$(f(X) + g(X))^p = f(X)^p + g(X)^p$$

für alle $f(X), g(X) \in K[X]$, da $\mathrm{char}(K[X]) = p$ und da $K[X]$ kommutativ ist. Eine t-fache Iteration ($t \in \mathbb{Z}_{\geqslant 0}$) liefert für $f(X), g(X) \in K[X]$ die Identität

$$(f(X) + g(X))^{p^t} = f(X)^{p^t} + g(X)^{p^t}.$$

Verwenden wir dies und die Tatsache, dass $\zeta^m = \zeta^{|M_m|} = 1$ ist, so erhalten wir

$$\begin{aligned}
X^n - 1 &= X^{p^t m} - 1^{p^t} \\
&= (X^m - 1)^{p^t} \\
&= \left(\prod_{k \in [0, m-1]} (X - \zeta^k) \right)^{p^t} \\
&= \prod_{k \in [0, m-1]} (X - \zeta^k)^{p^t} \\
&= \prod_{k \in [0, m-1]} \left(\prod_{l \in [0, p^t - 1]} (X - \zeta^{l \cdot m} \zeta^k) \right) \\
&= \prod_{k \in [0, m-1]} \left(\prod_{l \in [0, p^t - 1]} (X - \zeta^{l \cdot m + k}) \right) \\
&= \prod_{k' \in [0, n-1]} (X - \zeta^{k'}).
\end{aligned}$$

Letzteres folgt hierbei aus der Überlegung, dass sich jede Zahl $k' \in [0, n-1]$ eindeutig in der Form $k' = l \cdot m + k$ mit $l \in [0, p^t - 1]$ und $k \in [0, m-1]$ darstellen lässt.

Aufgabe 46

(1) Sei $A|\mathbb{Q}$ ein algebraischer Abschluß.

Ist $A|\mathbb{Q}$ eine endliche Erweiterung?

(2) Sei p eine Primzahl. Sei $A|\mathbb{F}_p$ ein algebraischer Abschluß.

Ist $A|\mathbb{F}_p$ eine endliche Erweiterung?

Lösung zu Aufgabe 46:

(1) *Angenommen*, es wäre $A|\mathbb{Q}$ eine endliche Erweiterung. Sei dann $n := [A : \mathbb{Q}] < \infty$ ihr Grad.

Ist $y \in A$, so ist y algebraisch über $\mathbb{Q}$, insbesondere ist $\mathbb{Q}(y)$ ein Unterkörper von A mit $[\mathbb{Q}(y) : \mathbb{Q}] = \deg(\mu_{y,\mathbb{Q}}(X))$ (Lemma 182).

Sei nun $k \in \mathbb{Z}_{\geqslant 1}$ und $y \in A$ eine Nullstelle des Polynoms $\Phi_k(X) \in \mathbb{Q}[X]$. Ein solches y existiert deshalb, da A algebraisch abgeschlossen ist. Da $\Phi_k(X) \in \mathbb{Q}[X]$ irreduzibel und normiert ist, ist $\mu_{y,\mathbb{Q}}(X) = \Phi_k(X)$. Weiterhin ist $[\mathbb{Q}(y) : \mathbb{Q}] = \deg(\Phi_k(X)) = \varphi(k)$ (Bemerkung 226.(1)).

Nach der Multiplikationsformel (Lemma 193) ist nun

$$\begin{aligned}
[A : \mathbb{Q}] &= [A : \mathbb{Q}(y)] \cdot [\mathbb{Q}(y) : \mathbb{Q}] \\
&\Leftrightarrow n = [A : \mathbb{Q}(y)] \cdot \varphi(k) \\
&\Rightarrow \varphi(k) \leqslant n.
\end{aligned}$$

Setzen wir in dieser Ungleichung nun $k = p$, wobei p eine Primzahl mit $p > n + 1$ ist, so erhalten wir (Bemerkung 226.(4))

$$n < p - 1 = \varphi(p) \leqslant n,$$

ein *Widerspruch*.

Folglich war unsere Annahme falsch, und es ist $A|\mathbb{Q}$ eine unendliche Erweiterung.

Eine genauere Betrachtung des Beweises zeigt, dass man anstelle der Polynome $\Phi_n(X)$ eine beliebige Familie irreduzibler Polynome in $\mathbb{Q}[X]$ verwenden kann, deren Grade nicht nach oben beschränkt sind. So tut es zum Beispiel auch die Familie der Polynome $X^n - 2$, wobei $n \in \mathbb{Z}_{\geqslant 1}$ ist.

(2) *Angenommen*, es ist $A|\mathbb{F}_p$ eine endliche Erweiterung. Sei $n := [A : \mathbb{F}_p] < \infty$ ihr Grad. Es ist

$$|A| = |\mathbb{F}_p|^{[A:\mathbb{F}_p]} = p^n.$$

Es wäre also A ein endlicher Körper. Nach Aufgabe 41.(4) kann A nicht algebraisch abgeschlossen sein. Unsere Annahme ist also falsch und $A|\mathbb{F}_p$ ist eine unendliche Erweiterung.

Aufgabe 47 Sei K ein algebraisch abgeschlossener Körper.

(1) Sei $\tilde{K}$ ein Körper mit $\tilde{K} \simeq K$. Ist auch $\tilde{K}$ ein algebraisch abgeschlossener Körper?

(2) Gibt es eine Körpererweiterung $L|K$ mit $K \neq L$?

(3) Gibt es eine Körpererweiterung $L|K$ mit $K \neq L$, für welche jedes Element von L algebraisch über K ist?

Lösung zu Aufgabe 47:

(1) Ja. Wir wählen zunächst einen Isomorphismus $\sigma : K \xrightarrow{\sim} \tilde{K}$.

Sei nun $f(X) \in \tilde{K}[X]^\times$ gegeben mit $\deg(f(X)) \geqslant 1$. Wir haben zu zeigen, daß $f(X)$ in $\tilde{K}$ eine Nullstelle hat.

Wir schreiben

$$f(X) = \sum_{i \in [0,n]} a_i X^i,$$

wobei $n = \deg(f(X))$ und $a_i \in \tilde{K}$ für $i \in [0, n]$. Wir definieren nun das Polynom

$$g(X) := \sum_{i \in [0,n]} \sigma^{-1}(a_i) X^i \in K[X].$$

Da K algebraisch abgeschlossen ist und $\deg(g(X)) = n \geqslant 1$ ist, besitzt $g(X)$ eine Nullstelle $y \in K$. Wir rechnen nun nach, dass $\sigma(y)$ eine Nullstelle von $f(X)$ ist:

$$\begin{aligned} f(\sigma(y)) &= \sum_{i \in [0,n]} a_i \sigma(y)^i \\ &= \sum_{i \in [0,n]} \sigma(\sigma^{-1}(a_i)) \sigma(y)^i \\ &= \sigma\left(\sum_{i \in [0,n]} \sigma^{-1}(a_i) y^i \right) \\ &= \sigma(g(y)) \\ &= \sigma(0) = 0. \end{aligned}$$

Es hat also $f(X)$ eine Nullstelle in $\tilde{K}$.

Damit hat also jedes Polynom $f(X) \in \tilde{K}[X]$ mit $\deg(f(X)) \geqslant 1$ eine Nullstelle in $\tilde{K}$. Also ist auch $\tilde{K}$ algebraisch abgeschlossen.

(2) Ja. Sei $L = K(X) = \mathrm{Quot}(K[X])$ der rationale Funktionenkörper über K (Beispiel 35.(2)). Dann ist $K \subset K[X] \subset L$. Es ist also $L|K$ eine Körpererweiterung mit $K \neq L$.

(3) Nein. Sei $L|K$ eine algebraische Körpererweiterung.

Wir wollen $L \overset{!}{=} K$ zeigen. Es genügt, $L \overset{!}{\subseteq} K$ zu zeigen.

Sei $y \in L$. Wir werden zeigen, dass $y \in K$ ist.

Sei zunächst $f(X) := \mu_{y,K}(X) \in K[X]$. Da K algebraisch abgeschlossen ist, zerfällt $f(X)$ in Linearfaktoren, d.h. es ist

$$f(X) = \prod_{i=1}^{n}(X - a_i)$$

mit $a_i \in K$ für $i \in [1, n]$. Andererseits ist $f(X)$ als Minimalpolynom von y irreduzibel in $K[X]$. Folglich ist $n = 1$, und es ist $f(X) = X - a$ mit $a \in K$. Da y Nullstelle von $f(X)$ ist, muss $y = a$ sein. Somit ist $y = a \in K$, was zu zeigen war.

Aufgabe 48

Sei $\mathbb{F}_9 := \mathbb{F}_3[X]/(X^2 + 1)$ und $\iota := X + (X^2 + 1)$. In $\mathbb{F}_9$ ist $3 = 0$ und $\iota^2 = -1$.
Sei $\widetilde{\mathbb{F}_9} := \mathbb{F}_3[X]/(X^2 - X - 1)$ und $\kappa := X + (X^2 - X - 1)$. In $\widetilde{\mathbb{F}_9}$ ist $3 = 0$ und $\kappa^2 = \kappa + 1$.

(1) Man konstruiere zwei verschiedene Körperisomorphismen φ und ψ von $\widetilde{\mathbb{F}_9}$ nach $\mathbb{F}_9$.

(2) Sind dies alle Isomorphismen von $\widetilde{\mathbb{F}_9}$ nach $\mathbb{F}_9$?

(3) Ist $\varphi \circ \psi^{-1} = \mathrm{Fr}_{\mathbb{F}_9} : \mathbb{F}_9 \to \mathbb{F}_9$?

Lösung zu Aufgabe 48:

(1) Es ist $\mu_{\kappa,\mathbb{F}_3}(X) = X^2 - X - 1$.

Wir bestimmen nun die Elemente $y \in \mathbb{F}_9$ mit $\mu_{\iota,\mathbb{F}_3}(X) = X^2 - X - 1$. Wir haben für $y \in \mathbb{F}_9$ die Äquivalenzen

$$y^2 - y - 1 = 0 \Leftrightarrow (y + 1)^2 + 1 = 0 \Leftrightarrow y + 1 \in \{\iota, -\iota\} \Leftrightarrow y \in \{-1 + \iota, -1 - \iota\}.$$

Sei nun $c := -1 + \iota$. Es ist $\mu_{\kappa,\mathbb{F}_3}(c) = 0$. Nach Lemma 189 gibt es also den Körpermorphismus

$$\begin{aligned} \varphi : \widetilde{\mathbb{F}_9} &\to \mathbb{F}_9 \\ f(\kappa) &\mapsto f(c) \quad (f(X) \in \mathbb{F}_3[X]), \end{aligned}$$

welcher dadurch eindeutig bestimmt ist, dass $\varphi(\kappa) = c$ ist und der Unterkörper $\mathbb{F}_3 \subseteq \mathbb{F}_9$ elementweise fix gelassen wird. Da φ als Körpermorphismus zwangsläufig injektiv ist und $|\widetilde{\mathbb{F}_9}| = |\mathbb{F}_9| = 9$ ist, ist φ bijektiv und somit ein Körperisomorphismus.

Analog definiert man mit $c' := -1 - \iota$ den Körpermorphismus

$$\begin{aligned} \psi : \widetilde{\mathbb{F}_9} &\to \mathbb{F}_9 \\ f(\kappa) &\mapsto f(c') \quad (f(X) \in \mathbb{F}_3[X]), \end{aligned}$$

welches der eindeutige Körpermorphismus mit $\psi(\kappa) = c'$ ist, der ebenfalls $\mathbb{F}_3 \subseteq \mathbb{F}_9$ elementweise fix lässt, und nach der gleichen Argumentation wie oben ein Isomorphismus ist.

(2) Ja. Sei $\theta : \widetilde{\mathbb{F}_9} \to \mathbb{F}_9$ ein Isomorphismus.

Zunächst lässt θ das Element $1 \in \mathbb{F}_9$ fix, folglich lässt es den von 1 erzeugten Unterkörper $\mathbb{F}_3 \subseteq \mathbb{F}_9$ elementweise fix. Es ist also θ ein Isomorphismus über $\mathbb{F}_3$.

Wir setzen $f(X) := X^2 - X + 1$. Dann ist

$$f(\theta(\kappa)) = \theta(f(\kappa)) = \theta(0) = 0.$$

Es ist also nach den Überlegungen aus Teil (1) der Aufgabe entweder $\theta(\kappa) = -1 + \iota$, woraus $\theta = \varphi$ folgt, oder aber es ist $\theta(\kappa) = -1 - \iota$, woraus $\theta = \psi$ folgt.

Wir haben in Teil (1) also bereits alle Isomorphismen ermittelt.

(3) Ja. Setze $\gamma := \varphi \circ \psi^{-1}$. Dann ist $\gamma \neq \mathrm{id}_{\mathbb{F}_9}$.

Es ist $\gamma(a) = a$ für alle $a \in \mathbb{F}_3$ (Argumentation wie in Teil (2) der Aufgabe). Weiterhin ist ι eine Nullstelle des Polynoms $X^2 + 1 \in \mathbb{F}_3[X]$, kann also durch γ nur auf eine Nullstelle dieses Polynoms abgebildet werden. Es ist also entweder $\gamma(\iota) = \iota$ oder $\gamma(\iota) = -\iota$.

Im Fall, dass $\gamma(\iota) = \iota$ ist, ergäbe sich für alle $a, b \in \mathbb{F}_3$, dass

$$\gamma(a + b\iota) = \gamma(a) + \gamma(b)\gamma(\iota) = a + b\iota.$$

Es wäre also $\gamma = \mathrm{id}_{\mathbb{F}_9}$. Dies haben wir aber ausgeschlossen.

Es muss also $\gamma(\iota) = -\iota$ sein. Hiermit ergibt sich

$$\gamma(a + b\iota) = \gamma(a) + \gamma(b)\gamma(\iota) = a - b\iota = a + b \cdot \iota^2 \cdot \iota = a^3 + b^3 \cdot \iota^3 = (a + b\iota)^3 = \mathrm{Fr}_{\mathbb{F}_9}(a + b\iota).$$

Hierbei haben wir verwendet, dass $\mathrm{Fr}_{\mathbb{F}_3} = \mathrm{id}_{\mathbb{F}_3}$ ist und dass $\iota^2 = -1$ ist. Es ist also $\gamma = \mathrm{Fr}_{\mathbb{F}_9}$, was zu beweisen war.

Ein kürzerer Beweis geht folgendermaßen: es ist

$$\mathrm{Fr}_{\mathbb{F}_9}(\iota) = \iota^3 = \iota^2 \cdot \iota = -\iota \neq \iota,$$

also ist $\mathrm{Fr}_{\mathbb{F}_9} \neq \mathrm{id}_{\mathbb{F}_9}$. Damit ist auch der Isomorphismus $\mathrm{Fr}_{\mathbb{F}_9} \circ \psi \neq \psi$. Nach Teil (2) der Aufgabe muss also $\mathrm{Fr}_{\mathbb{F}_9} \circ \psi = \varphi$ bzw. $\varphi \circ \psi^{-1} = \mathrm{Fr}_{\mathbb{F}_9}$ sein.

Ein rein rechnerischer alternativer Beweis geht wie folgt. Es ist

$$\begin{aligned}
(\varphi \circ \psi^{-1})(a + b\iota) &= a + b(\varphi \circ \psi^{-1})(\iota) \\
&= a + b\varphi(-\kappa - 1) \\
&= a - b\iota \\
&= a^3 + b^3\iota^3 \\
&= (a + b\iota)^3 \\
&= \mathrm{Fr}_{\mathbb{F}_9}(a + b\iota)
\end{aligned}$$

für $a, b \in \mathbb{F}_3$. Also ist $\varphi \circ \psi^{-1} = \mathrm{Fr}_{\mathbb{F}_9}$.