M. Künzer

Galoistheorie, WS 08/09

Lösung 8

Aufgabe 26

(1) Es ist $\operatorname{char} L > 0$, da $\operatorname{char} L = 0$ zur Folge hätte, daß $\mathbf{Z} \xrightarrow{\varepsilon_L} L$ den Kern $(\operatorname{char} L)\mathbf{Z} = \{0\}$ hätte, und somit injektiv wäre, was wegen L endlich nicht geht.

Schreibe also $\operatorname{char} L =: p > 0$. Wir haben den Primkörper $\mathbf{F}_p \subseteq L$; vgl. §2.1.

Es ist L ein $\mathbf{F}_p$-Vektorraum; vgl. die erste Bemerkung in §1.7.5. Da L endlich ist, ist L ein endlichdimensionaler $\mathbf{F}_p$-Vektorraum. Sei $\ell := \dim_{\mathbf{F}_p} L = [L : \mathbf{F}_p]$. Es folgt $|L| = p^\ell$.

(2) Erste Lösung. Es ist $\ell = [L : \mathbf{F}_p] = [L : K][K : \mathbf{F}_p]$. Folglich ist $[K : \mathbf{F}_p] =: k$ ein Teiler von ℓ. Ferner ist $|K| = p^k$.

Zweite Lösung, alternativ. Es ist L ein endlichdimensionaler K-Vektorraum. Schreibe $m := [L : K]$. Mit (1) gibt es ein $k \geqslant 1$ mit $K = p^k$; beachte $\operatorname{char} K = \operatorname{char} L = p$. Also ist $(p^k)^m = p^\ell$. Mithin ist $km = \ell$.

(3) Nach (2) haben alle Teilkörper von $\mathbf{F}_{27}$ eine Kardinalität 3^k mit k einem Teiler von 3. Es folgt, daß diese Kardinalität $3^1 = 3$ oder $3^3 = 27$ haben. Also sind der Primkörper $\mathbf{F}_3$ und der gesamte Körper $\mathbf{F}_{27}$ die einzigen Teilkörper von $\mathbf{F}_{27}$.

Vgl. auch Aufgabe 21.

Aufgabe 27

(1) Zum einen ist $(ab)^{\mathrm{o}(a)\mathrm{o}(b)} = (a^{\mathrm{o}(a)})^{\mathrm{o}(b)}(b^{\mathrm{o}(b)})^{\mathrm{o}(a)} = 1^{\mathrm{o}(b)}1^{\mathrm{o}(a)} = 1$.

Sei zum anderen $(ab)^k = 1$ für ein $k \in \mathbf{Z}_{\geqslant 1}$.

Dann ist $a^k = b^{-k}$. Es ist $a^k \in \langle a \rangle$, und $\langle a \rangle$ ist eine Gruppe mit $|\langle a \rangle| = \mathrm{o}(a)$ nach Aufgabe 11.(1.b). Nach Aufgabe 11.(1.c), angewandt auf diese Gruppe $\langle a \rangle$, ist $\mathrm{o}(a^k)$ ein Teiler von $\mathrm{o}(a)$.

(Hierfür kann man alternativ auch folgendes vorbringen. Schreibe $\mathrm{o}(a) = \mathrm{o}(a^k)q + r$ mit $q \in \mathbf{Z}$ und $r \in [0, \mathrm{o}(a^k) - 1]$. Dann ist

$$1 \;=\; (a^{\mathrm{o}(a)})^k \;=\; (a^k)^{\mathrm{o}(a)} \;=\; (a^k)^{\mathrm{o}(a^k)q+r} \;=\; (a^k)^r \;,$$

und also $r = 0$ wegen der Minimalität von $\mathrm{o}(a^k)$.)

Analog ist $\mathrm{o}(b^{-k})$ ein Teiler von $\mathrm{o}(b)$.

Somit ist $\mathrm{o}(a^k) = \mathrm{o}(b^{-k})$ ein gemeinsamer Teiler von $\mathrm{o}(a)$ und von $\mathrm{o}(b)$, und also gleich 1, da $\mathrm{ggT}(\mathrm{o}(a), \mathrm{o}(b)) = 1$. Dies aber hat $a^k = b^{-k} = 1$ zur Folge.

Wir *behaupten,* daß k ein Vielfaches von $\mathrm{o}(a)$ ist. Schreibe $k = \mathrm{o}(a)q + r$ mit $r \in [0, \mathrm{o}(a) - 1]$. Es folgt $1 = a^k = a^{\mathrm{o}(a)q+r} = a^r$ und also $r = 0$ wegen der Minimalität von $\mathrm{o}(a)$. Dies zeigt die *Behauptung.*

Analog ist k ein Vielfaches von $\mathrm{o}(b)$.

Da $\mathrm{ggT}(\mathrm{o}(a), \mathrm{o}(b)) = 1$, ist k damit ein Vielfaches von $\mathrm{o}(a)\mathrm{o}(b)$, und insbesondere ist $k \geqslant \mathrm{o}(a)\mathrm{o}(b)$.

Somit ist $\mathrm{o}(a)\mathrm{o}(b)$ der minimale positive Exponent, dessen Potenz von ab gleich 1 ist. In anderen Worten, es ist in der Tat $\mathrm{o}(ab) = \mathrm{o}(a)\mathrm{o}(b)$.

(2) Zum einen ist $(a^{\frac{\mathrm{o}(a)}{d}})^d = a^{\mathrm{o}(a)} = 1$.

Sei zum anderen $(a^{\frac{\mathrm{o}(a)}{d}})^k = 1$, i.e. $a^{\frac{\mathrm{o}(a)k}{d}} = 1$, wobei $k \in \mathbf{Z}_{\geqslant 1}$. Dann ist $\frac{\mathrm{o}(a)k}{d} \geqslant \mathrm{o}(a)$ wegen der Minimalität von $\mathrm{o}(a)$, also $k \geqslant d$.

Somit ist k der minimale positive Exponent, dessen Potenz von $a^{\frac{\mathrm{o}(a)}{d}}$ gleich 1 ist. In anderen Worten, es ist in der Tat $\mathrm{o}(a^{\frac{\mathrm{o}(a)}{d}}) = d$.

(3) Schreibe $\mathrm{o}(a) = p_1^{s_1} \cdots p_k^{s_k}$ und $\mathrm{o}(b) = p_1^{t_1} \cdots p_k^{t_k}$ mit $k \geqslant 0$, p_i prim und $s_i,\, t_i \in \mathbf{Z}_{\geqslant 0}$ für $i \in [1,k]$.

Sei $i \in [1,k]$ gegeben. Mit (2) gibt es ein Element von Ordnung $p_i^{s_i}$ in G, nämlich eine geeignete Potenz von a. Mit (2) gibt es auch ein Element von Ordnung $p_i^{t_i}$ in G, nämlich eine geeignete Potenz von b. Somit gibt es auch ein Element $x_i \in G$ von Ordnung $p_i^{\max\{s_i,t_i\}}$ in G.

Mit (1) folgt aus der Teilerfremdheit der Primpotenzen, daß

$$\mathrm{o}(x_1 \cdots x_k) \;=\; \mathrm{o}(x_1) \cdots \mathrm{o}(x_k) \;=\; p_1^{\max\{s_1,t_1\}} \cdots p_k^{\max\{s_k,t_k\}} \;=\; \mathrm{kgV}(\mathrm{o}(a), \mathrm{o}(b)) \;.$$

(4) *Wäre* $\mathrm{o}(g)$ kein Teiler von $\mathrm{o}(x)$ ist für ein $g \in G$, so wäre $\mathrm{o}(x) < \mathrm{kgV}(\mathrm{o}(x), \mathrm{o}(g))$. Sei $\tilde{g}$ ein mit (3) existentes Element von G von Ordnung $\mathrm{kgV}(\mathrm{o}(x), \mathrm{o}(g))$. Dann ist $\mathrm{o}(x) < \mathrm{o}(\tilde{g})$. Wir haben einen *Widerspruch* zur Maximalität von $\mathrm{o}(x)$.

(5) Sei $x \in K^\times$ von maximaler Ordnung.

Zunächst ist $\mathrm{o}(x)$ ein Teiler von $|K|-1$; vgl. Aufgabe 11.(1.c).

Mit (4) folgt andererseits, daß für alle $g \in K^\times$ gilt, daß $\mathrm{o}(g)$ ein Teiler von $\mathrm{o}(x)$ ist, und insbesondere, das $g^{\mathrm{o}(x)} = 1$. Folglich sind alle Elemente von $K^\times$ Nullstellen von $X^{\mathrm{o}(x)} - 1$. Ein Polynom mit $|K|-1$ Nullstellen hat aber Grad $\geqslant |K|-1$. Also ist $\mathrm{o}(x) \geqslant |K|-1$.

Insgesamt folgt $\mathrm{o}(x) = |K|-1$.

(6) Wir verwenden die Schreibweise der Lösung von Aufgabe 24.(4). Sei also $\delta \in \mathbf{F}_4$ mit $\delta^4 + \delta + 1 = 0$. Wir erhalten folgende Potenzen, ausgedrückt in der Standardbasis $(1, \delta, \delta^2, \delta^3)$ über $\mathbf{F}_2$.

$$\begin{array}{lcl}
\delta^0 & = & 1 \\
\delta^1 & = & \delta \\
\delta^2 & = & \delta^2 \\
\delta^3 & = & \delta^3 \\
\delta^4 & = & \delta + 1 \\
\delta^5 & = & \delta^2 + \delta \\
\delta^6 & = & \delta^3 + \delta^2 \\
\delta^7 & = & \delta^3 + \delta + 1 \\
\delta^8 & = & \delta^2 + 1 \\
\delta^9 & = & \delta^3 + \delta \\
\delta^{10} & = & \delta^2 + \delta + 1 \\
\delta^{11} & = & \delta^3 + \delta^2 + \delta \\
\delta^{12} & = & \delta^3 + \delta^2 + \delta + 1 \\
\delta^{13} & = & \delta^3 + \delta^2 + 1 \\
\delta^{14} & = & \delta^3 + 1 \\
\delta^{15} & = & 1 \qquad \text{(zur Probe)}
\end{array}$$

Vgl. auch Aufgabe 11.(2, 3) und Aufgabe 18.

Aufgabe 28

Schreibe $n := [L : K]$. Das Tupel $(x^0, x^1, \ldots, x^n)$ hat Länge $n+1$, ist also linear abhängig. Somit gibt es $\lambda_i \in K$ für $i \in [0,n]$ so, daß

$$\lambda_0 x^0 + \cdots + \lambda_n x^n \;=\; 0 \;,$$

aber so, daß $\lambda_j \neq 0$ für wenigstens ein $j \in [0,n]$. Setzen wir $f(X) = \sum_{i \in [0,n]} \lambda_i X^i \in K[X]$, so haben wir also ein Polynom ungleich 0 gefunden, welches $f(x) = 0$ erfüllt. Folglich ist x algebraisch über K.