Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 27. Januar 2009

Algebra

13. Übung mit Lösungshinweisen

Aufgabe 59 (Primkörper) Sei $\mathbb{K}$ ein Körper und $\sigma \in \mathrm{Aut}(\mathbb{K})$ ein Automorphismus. Zeige, daß der Primkörper $\mathbb{P}$ von $\mathbb{K}$ im Fixkörper von σ liegt.

Lösung: Der Primkörper ist der von $1 \in \mathbb{K}$ erzeugte Unterkörper $\mathbb{P}$. Da $\sigma(1) = 1$ gilt, ist jedes Element in $\mathbb{K}$, was durch endlich viele algebraische Operationen aus Einsen erzeugt wird, unter σ fix. Dies sind die Elemente des Primkörpers, also gilt $\mathbb{P} \subseteq \mathrm{Fix}(\sigma)$.

Aufgabe 60 (Zyklische Galoiserweiterungen) Es sei $\mathbb{K}$ ein Körper mit Charakteristik $p > 0$, $f(X) := X^p - X - a$ sei ein irreduzibles Polynom in $\mathbb{K}[X]$ und es sei $\mathbb{L}$ ein Zerfällungskörper von f.

(a) Zeige: Ist $\alpha \in \mathbb{L}$ eine Nullstelle von f, so auch $\alpha + 1$.

(b) Zeige, daß $\mathbb{L}/\mathbb{K}$ eine Galoiserweiterung mit zyklischer Galoisgruppe ist und bestimme die Ordnung der Galoisgruppe.

(c) Bestimme alle Zwischenkörper der Galoiserweiterung $\mathbb{L}/\mathbb{K}$.

Lösung: (a) Die Abbildung $x \to x^p$ ist ein Körperhomomorphismus, also erhalten wir

$$\begin{aligned} f(\alpha+1) &= (\alpha+1)^p - (\alpha+1) - a \\ &= \alpha^p + 1 - \alpha - 1 - a \\ &= \alpha^p - \alpha - a \\ &= f(\alpha) = 0. \end{aligned}$$

Somit folgt die Aussage.

(b) Die Nullstellen von f sind genau $\{\alpha, \alpha+1, ..., \alpha+p-1\}$ und wir sehen, daß f separabel ist. Weiter gilt

$$\mathbb{L} = \mathbb{K}(\alpha),$$

da die Nullstellen durch Addition von $\mathbb{K}$-Elementen zu α entstehen. Somit gilt $[\mathbb{L} : \mathbb{K}] = [\mathbb{K}(\alpha) : \mathbb{K}] = p$. Wir wissen außerdem, daß einen $\mathbb{K}$-Automorphismus σ gibt, mit $\sigma(\alpha) = \alpha+1$, da f irreduzibel war. Betrachten wir die Potenzen von σ, so sehen wir

$$\sigma^m(\alpha) = \alpha + m,$$

dies sind p verschiendene Automorphismen, also wird $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ durch σ erzeugt und die Erweiterung ist zyklisch.

(c) Da $\mathbb{Z}_p$ eine einfache Gruppe ist, gibt es nur die beiden trivialen Zwischenkörper $\mathbb{L}$ und $\mathbb{K}$.

Aufgabe 61 (Abelsche Galoiserweiterungen) Sei $\mathbb{L}/\mathbb{K}$ eine galoissche Körpererweiterung. Wir nennen $\mathbb{L}/\mathbb{K}$ abelsch, bzw. zyklisch, wenn die Galoisgruppe $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ abelsch bzw. zyklisch ist.

(a) Es sei $\mathbb{L}/\mathbb{K}$ eine abelsche Galoiserweiterung. Zeige, daß dann für jeden Zwischenkörper $\mathbb{F}$ auch $\mathbb{F}/\mathbb{K}$ eine abelsche Galoiserweiterung ist.

(b) Es sei $\mathbb{L}/\mathbb{K}$ eine zyklische Galoiserweiterung. Zeige, daß dann für jeden Zwischenkörper $\mathbb{F}$ auch $\mathbb{F}/\mathbb{K}$ eine zyklische Galoiserweiterung ist.

(c) Es sei $f \in \mathbb{K}[X]$ ein separables irreduzibles Polynom und $\mathbb{L}$ ein Zerfällungskörper von f über $\mathbb{K}$, so daß $\mathbb{L}/\mathbb{K}$ eine endliche abelsche Galoiserweiterung ist. Zeige, daß jede Nullstelle $\alpha \in \mathbb{L}$ von f ein primitives Element ist, also $\mathbb{L} = \mathbb{K}(\alpha)$ gilt.

LÖSUNG: (a) Ist $\mathbb{L}/\mathbb{K}$ abelsch, so auch jede Untergruppe. Insbesondere ist $\mathrm{Gal}(\mathbb{L}, \mathbb{F})$ eine normale Untergruppe von $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$. Somit ist auch $\mathbb{F}/\mathbb{K}$ nach dem Hauptsatz galoissch. Weiter ist der Quotient einer abelschen Gruppe abelsch, somit ist

$$\mathrm{Gal}(\mathbb{F}, \mathbb{K}) \cong \mathrm{Gal}(\mathbb{L}, \mathbb{K})/\mathrm{Gal}(\mathbb{L}, \mathbb{F})$$

abelsch und $\mathbb{F}/\mathbb{K}$ eine abelsche Galoiserweiterung.

(b) Ist $\mathbb{L}/\mathbb{K}$ zyklisch, so ist $\mathbb{L}/\mathbb{K}$ insbesondere abelsch. Also ist $\mathrm{Gal}(\mathbb{L}, \mathbb{F})$ eine normale Untergruppe von $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$. Somit ist auch $\mathbb{F}/\mathbb{K}$ nach dem Hauptsatz galoissch. Weiter ist die Quotientengruppe

$$\mathrm{Gal}(\mathbb{F}, \mathbb{K}) \cong \mathrm{Gal}(\mathbb{L}, \mathbb{K})/\mathrm{Gal}(\mathbb{L}, \mathbb{F})$$

zyklisch und somit ist $\mathbb{F}/\mathbb{K}$ eine zyklische Galoiserweiterung.

(c) Nach (a) ist $\mathbb{K}(\alpha)/\mathbb{K}$ ebenfalls eine Galoiserweiterung, insbesondere ist $\mathbb{K}(\alpha)/\mathbb{K}$ eine normale Erweiterung. Da f irreduzibel ist und in $\mathbb{K}(\alpha)$ eine Nullstelle hat, zerfällt f bereits in $\mathbb{K}(\alpha)$ in Linearfaktoren. Somit ist $\mathbb{K}(\alpha)$ der Zerfällungskörper von f und wir erhalten $\mathbb{L} = \mathbb{K}(\alpha)$.

Aufgabe 62 (Einheitswurzeln) Es sei $\mathbb{K}$ ein Körper und $m, n \in \mathbb{N}$ seien teilerfremd.

(a) Zeige, daß dann die Abbildung

$$h : U_m \times U_n \ni (\xi, \eta) \to \xi \cdot \eta \in U_{mn}$$

ein Isomorphismus von Gruppen ist.

(b) Es sei $\xi_m \in U_m$ eine primitive m-te Einheitswurzel und $\xi_n \in U_n$ eine primitive n-te Einheitswurzel. Zeige, daß $\xi_m \cdot \xi_n \in U_{m \cdot n}$ eine primitive mn-te Einheitswurzel ist.

LÖSUNG: (a) OBdA. werde mn nicht von der Charakteristik des Körpers geteilt. Weiter sind U_m, U_n und U_{mn} zyklische Gruppen der Ordnung m, n bzw. mn. Somit gilt

$$|U_m \times U_n| = |U_{mn}|.$$

Weiter sind U_m und U_n Untergruppen von U_{mn} und alle Gruppen sind abelsch, daher ist h ein Gruppenhomomorphismus. Dieser ist genau dann bijektiv, wenn er injektiv ist, da alle beteiligten Gruppen endlich sind. Sei $(\xi, \eta) \in \ker(h)$. Dann gilt $\xi \cdot \eta = 1$, also folgt $\eta \in U_m$ und $\xi \in U_n$. Somit ist h genau dann bijektiv, wenn $U_m \cap U_n = \{1\}$ gilt.
Da m und n teilerfremd sind, gibt es Zahlen $a, b \in \mathbb{Z}$ mit $am + bn = 1$, also

$$\begin{aligned}(\xi, \eta) &= (\xi, \eta)^{am+bn} = (\xi, \eta)^{am} \cdot (\xi, \eta)^{bn} \\ &= ((\xi, \eta)^m)^a \cdot ((\xi, \eta)^n)^b \\ &= (\xi^m, \eta^m)^a \cdot (\xi^n, \eta^n)^b \\ &= (1, 1)^a \cdot (1, 1)^b = (1, 1).\end{aligned}$$

Also ist der Kern von h trivial und somit ist h ein Ismorphismus.

(b) die Ordnung des Elements $(\xi_m, \xi_n) \in U_m \times U_n$ ist genau das kleinste gemeinsame Vielfache der Zahlen m und n. Da aber m und n teilerfremd waren, hat (ξ_m, ξ_n) die Ordnung mn. Damit hat auch $h((\xi_m, \xi_n))$ die Ordnung mn, denn h ist ein Gruppenisomorphismus. Somit erzeugt $h((\xi_m, \xi_n)) = \xi_m \cdot \xi_n$ die Gruppe U_{mn}, also ist $\xi_m \cdot \xi_n$ eine primitive mn-te Einheitswurzel.

Aufgabe 63 (Eine Klasse irreduzibler Polynome) Sei $\mathbb{K}$ ein Körper, $a \in \mathbb{K}$ und p eine Primzahl. Zeige, daß das Polynom $X^p - a$ genau dann irreduzibel ist, wenn es keine Nullstelle in $\mathbb{K}$ hat.

LÖSUNG: Es habe $\mathbb{K}$ Charakteristik p und $f := X^p - a$ in $\mathbb{K}$ keine Nullstelle in $\mathbb{K}$. Sei α eine Nullstelle von f in einem algebraischen Abschluß, so sehen wir $X^p - a = (X - \alpha)^p$. Wäre f nicht irreduzibel, so wäre es das Produkt $g \cdot h$, also hätten wir in $\mathbb{K}(\alpha)[X]$ die Zerlegung

$$X^p - a = (X - \alpha)^r \cdot (X - \alpha)^s = g \cdot h.$$

Somit, da das Absolutglied von $(X - \alpha)^r$ genau α^r ist, hätten wir, läge dieses Polynom in $\mathbb{K}[X]$, auch $\alpha^r \in \mathbb{K}$. Damit läge aber auch $(\alpha^r)^s \in \mathbb{K}$ für jedes $s \in \mathbb{Z}$. Wähle $m, n \in \mathbb{Z}$ mit $rs - np = 1$. Dann erhalten wir

$$\begin{aligned} \alpha^{rs} &= \alpha^{1+np} \\ &= \alpha^1 \cdot (\alpha^p)^n \\ &= \alpha \cdot a^n. \end{aligned}$$

Da a^n und α^{rs} Elemente aus $\mathbb{K}$ sind, ist auch $\alpha = \frac{\alpha^{rs}}{a^n}$ ein Element aus $\mathbb{K}$ und f hätte eine Nullstelle. Somit kann es keine Zerlegung in Nichteinheiten von f geben, also ist f irreduzibel.
Sei nun $\mathrm{char}(\mathbb{K}) \neq p$ und ξ eine primitive p-te Einheitswurzel. Ist f nicht irreduzibel in $\mathbb{K}[X]$, $f = g \cdot h$ und besitzt f in $\mathbb{K}(\xi)$ eine Nullstelle α, so gilt in $\mathbb{K}(\xi)[X]$:

$$f = \prod_{k=0}^{p-1} (X - \alpha \cdot \xi^k).$$

Ist nun $g = \prod_{i_1,\ldots,i_l} (X - \xi^{i_j} \cdot \alpha)$, so hätte g als Absolutglied $\xi^s \cdot \alpha^l$ für $s \in \{0, \ldots, p-1\}$ geeignet. Da g in $\mathbb{K}[X]$ angenommen wurde, liegt somit auch $\xi^s \cdot \alpha^l$ in $\mathbb{K}$. Da $l = \deg(g) > 0$, existiert ein $t \in \mathbb{N}$ mit

$$\left(\xi^s \cdot \alpha^l\right)^t = \xi^{st} \cdot a^m \cdot \alpha.$$

Damit läge die Zahl $\xi^{st} \cdot \alpha$ in $\mathbb{K}$ und f hätte in $\mathbb{K}$ eine Nullstelle.
Es habe nun also *oBdA.* das Polynom f keine Nullstelle in $\mathbb{K}(\xi)$. Ist α eine Nullstelle von f in einem algebraischen Abschluß und $\mathbb{L}$ der Zerfällungskörper von f über $\mathbb{K}(\alpha)$, so ist $\mathbb{L}/\mathbb{K}$ galoissch. Es sei $\xi \in \overline{\mathbb{K}}$ eine primitive p-te Einheitswurzel. Auf Grund der Geometrie der Nullstellen erhalten wir $\mathbb{L} = \mathbb{K}(\xi)(\alpha)$. Da $\mathbb{L}/\mathbb{K}(\xi)$ galoissch ist und α nicht in $\mathbb{K}(\xi)$ liegen kann, gibt es einen $\mathbb{K}(\xi)$-Automorphismus σ mit

$$\sigma(\alpha) = \xi \cdot \alpha.$$

Weiter hat σ die Ordnung p, denn $\sigma^k \neq \mathrm{id}$ für $1 \leq k \leq p-1$. Somit teilt p die Gruppenordnung der Galoisgruppe $\mathrm{Gal}(\mathbb{L}, \mathbb{K}(\xi))$. Weiter ist aber $[\mathbb{L} : \mathbb{K}(\xi)] \leq \deg(f) = p$. Also folgt

$$p \leq [\mathbb{L} : \mathbb{K}(\xi)] \leq p,$$

also gilt $\mathrm{Gal}(\mathbb{L}, \mathbb{K}(\xi)) =< \sigma >$. Da diese Gruppe transitiv auf den Nullstellen von f wirkt, ist f als Polynom in $\mathbb{K}(\xi)[X]$ irreduzibel, also insbesondere irreduzibel in $\mathbb{K}[X]$.

Hausübungen

Aufgabe H25 (Eulersche φ-Funktion) Sei $\varphi : \mathbb{N} \to \mathbb{N}$ die eulersche φ-Funktion.

(a) Zeige, daß φ für teilerfremde Zahlen $m, n \in \mathbb{N}$ multiplikativ ist, es gilt also

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

(b) Sei p prim und $k \in \mathbb{N}$. Berechne $\varphi(p^k)$.

(c) Berechne $\varphi(1980)$.

LÖSUNG: (a) Da $\varphi(n) = |\mathbb{Z}_n^\times|$ gilt, folgt die Behauptung aus dem chinesischen Restsatz:

$$\mathbb{Z}_{m \cdot n} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

für m, n teilerfremd. Somit sind die invertierbaren Elemente aus $\mathbb{Z}_{m \cdot n}$ genau die invertierbaren Elemente in $\mathbb{Z}_m \times \mathbb{Z}_n$. Ein Element ist aber genau dann in $\mathbb{Z}_m \times \mathbb{Z}_n$ invertierbar, wenn es in jeder Koordinate invertierbar ist. Somit erhalten wir

$$\mathbb{Z}_{m \cdot n}^\times \cong (\mathbb{Z}_m \times \mathbb{Z}_n)^\times = \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times.$$

Daraus folgt durch Elemente zählen

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

(b) Im Ring $\mathbb{Z}_{p^k}$ sind alle Zahlen invertierbar, die zu p^k teilerfremd sind. Somit ist der Unterring, der von p erzeugt wird, genau der Ring der nicht invertierbaren Elemente in $\mathbb{Z}_{p^k}$. Da dies sogar ein Ideal ist und der Quotient der Körper $\mathbb{Z}_p$ ist, erhalten wir durch den Satz von Lagrange

$$p^k = |\mathbb{Z}_{p^k}| = |\mathbb{Z}_p| \cdot | < p > | = p \cdot p^{k-1},$$

also gilt mit $|\mathbb{Z}_{p^k}^\times| = |\mathbb{Z}_{p^k}| - | < p > |$ für den Wert der φ-Funktion

$$\varphi(p^k) = p^k - | < p > | = p^k - p^{k-1}.$$

(c) Wir folgern aus der Primfaktorzerlegung $1980 = 9 \cdot 4 \cdot 5 \cdot 11$ und der Multiplikativität von φ das Ergebnis

$$\varphi(1980) = \varphi(9) \cdot \varphi(4) \cdot \varphi(5) \cdot \varphi(11) = 9 \cdot 2 \cdot 4 \cdot 10 = 720.$$

Aufgabe H26 (Charakterisierung von Galoiserweiterungen)

(a) Es sei $\mathbb{L}/\mathbb{K}$ eine endliche Körpererweiterung. Zeige, daß folgende Aussagen äquivalent sind:

(1) Die Erweiterung $\mathbb{L}/\mathbb{K}$ ist galoissch.

(2) Der Körper $\mathbb{K}$ ist Fixkörper der Gruppe $\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$.

(3) Es gilt $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})| = [\mathbb{L} : \mathbb{K}]$.

(b) Zeige, daß eine algebraische Körpererweiterung $\mathbb{L}/\mathbb{K}$ genau dann galoissch ist, wenn $\mathbb{K}$ der Fixkörper unter der Automorphismengruppe $\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ ist.

LÖSUNG: (a) (1) $\Rightarrow$ (2) Ist die Erweiterung galoissch, so ist sie normal und separabel. Somit zerfällt jedes Minimalpolynom eines Elements $a \in \mathbb{L} - \mathbb{K}$. Ist das Minimalpolynom vom Grad > 1, so gibt es einen Automorphismus, welcher a auf eine andere Nullstelle seines

Minimalpolynoms abbildet und somit ist a kein Element des Fixkörpers der Automorphismengruppe.
(2) $\Rightarrow$ (3) Ist $\mathbb{K}$ der Fixkörper der $\mathbb{K}$-Automorphismen, so ist für jedes $a \in \mathbb{L}$ das Polynom

$$f_a(X) := \prod_{\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})} (X - \sigma(a))$$

ein separables Polynom mit Koeffizienten in $\mathbb{K}$. Also ist $\mathbb{L}/\mathbb{K}$ separabel und wir erhalten

$$[\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{K}].$$

Ist f ein irreduzibles Polynom in $\mathbb{K}[X]$, welches in $\mathbb{L}$ eine Nullstelle b hat, so ist dieses bis auf Normierung das Minimalpolynom von b. Da b aber auch eine Nullstelle von f_b ist, teilt f das Polynom f_b. Somit zerfällt f in Linearfaktoren, da f_b dies tut. Also ist $\mathbb{L}/\mathbb{K}$ normal und wir erhalten

$$|\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})| = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| = [\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{K}].$$

(3) $\Rightarrow$ (1) Es sei $\mathbb{F}$ der Fixkörper von $\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$. Dann ist $\mathbb{L}/\mathbb{F}$ galoissch und es gilt

$$[\mathbb{L} : \mathbb{F}] = |\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})| = [\mathbb{L} : \mathbb{K}].$$

Somit folgt aus dem Gradsatz

$$[\mathbb{F} : \mathbb{K}] = \frac{[\mathbb{L} : \mathbb{K}]}{[\mathbb{L} : \mathbb{F}]} = 1.$$

Damit ist $\mathbb{F}$ ein eindimensionaler Vektorraum über $\mathbb{K}$, also $\mathbb{F} = \mathbb{K}$ und $\mathbb{L}/\mathbb{K}$ ist galoissch.

(b) Sei $\mathbb{K}$ der Fixkörper der $\mathbb{K}$-Automorphismengruppe $G := \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$. Ist $a \in \mathbb{L}$, so gibt es ein maximales System von Automorphismen $\sigma_1, ..., \sigma_r$, so daß $\sigma_1(a), ..., \sigma_r(a)$ paarweise verschiedene Elemente von $\mathbb{L}$ sind. Dies folgt daher, daß $\sigma(a)$ immer eine Nullstelle des Minimalpolynoms von a über $\mathbb{K}$ sein muß für jeden Automorphismus $\sigma \in G$. Weiter permutiert jedes $\sigma \in G$ obige Menge, also folgt, daß das Polynom

$$f := \prod_{k=1}^{r} (X - \sigma_k(a))$$

Koeffizienten in $\mathbb{K}$ hat, denn es gilt $f = \sigma_*(f)$ für jedes $\sigma \in G$. Also ist a Nullstelle eines separablen Polynoms und somit ist die Erweiterung separabel.
Weiter ist $\mathbb{L}/\mathbb{K}$ normal, da $\mathbb{L}$ der Zerfällungskörper aller Polynome von obigem Typ ist. Also ist $\mathbb{L}/\mathbb{K}$ eine Galoiserweiterung.
Ist umgekehrt $\mathbb{L}/\mathbb{K}$ eine Galoiserweiterung und $a \in \mathbb{L} - \mathbb{K}$, so ist das Minimalpolynom von a vom Grad > 1 und es gibt eine Nullstelle $b \in \mathbb{L}$ des Minimalpolynoms von a mit $b \neq a$. Da die Erweiterung galoissch ist, existiert ein Automorphismus, welcher a nach b abbildet, also ist jedes Element aus $\mathbb{L} - \mathbb{K}$ kein Fixelement der K-Automorphismengruppe. Also gilt $\mathrm{Fix}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})) = \mathbb{K}$.