Musterlösung Serie 21

NORMALE UND SEPARABLE KÖRPERERWEITERUNGEN

---

104. Sei p ein Primzahl, sei $L := \mathbb{F}_p(t)$ der Körper der rationalen Funktionen über $\mathbb{F}_p$ in der Variabel t (d.h. der Quotientenkörper des Polynomrings $\mathbb{F}_p[t]$), und sei $K := \mathbb{F}_p(t^p)$. Beweisen Sie: Das Polynom $X^p - t^p$ ist irreduzibel und inseparabel über K, und L ist sein Zerfällungskörper.

Lösung: Der Ring $\mathbb{F}_p[t^p]$ ist isomorph zum Polynomring $\mathbb{F}_p[Y]$ durch den Isomorphismus $\mathbb{F}_p[Y] \to \mathbb{F}_p[t^p],\ Y \mapsto t^p$. Da Y ein irreduzibles Element im Hauptidealring $\mathbb{F}_p[Y]$ ist, ist auch $t^p \in \mathbb{F}_p[t^p]$ irreduzibel. Nach dem Schönemann-Eisenstein-Kriterium ist nun $X^p - t^p$ ein irreduzibles Polynom in $\mathbb{F}_p[t^p][X]$, also ist es nach dem Lemma von Gauss irreduzibel in $\mathbb{F}_p(t^p)[X] = K[X]$. In L gilt $X^p - t^p = (X - t)^p$, also hat das Polynom die p-fache Nullstelle t und ist somit, da es irreduzibel ist, nicht separabel. Da $L = K(t)$ ist, ist L der Zerfällungskörper.

105. Sei K ein Körper mit $\mathrm{char}(K) = p$ für eine Primzahl p. Beweisen Sie: Ein irreduzibles Polynom $f \in K[X]$ ist genau dann inseparabel über K, falls $a_i \in K$ existieren so dass $f = \sum_{i=0}^{n} a_i X^{ip}$ gilt.

Lösung: ($\Leftarrow$): Ist f von dieser Form, so ist

$$Df = p \cdot a_1 X^{p-1} + 2p \cdot a_2 X^{2p-1} \ldots + np \cdot a_n X^{np-1},$$

und weil $\mathrm{char}(K) = p$ ist $Df = 0$. Somit ist f inseparabel.

($\Rightarrow$): Mit Kontraposition. Ist $f = \sum_{i=0}^{n} a_i X^{n_i}$ nicht von dieser Form, so existiert ein j mit $1 \leqslant j \leqslant n$ sodass $a_j \neq 0$ und $p \nmid n_j$. Dann ist $Df \neq 0$, und weil f irreduzibel ist und $\deg(Df) < \deg(f)$, existiert kein gemeinsamer Faktor von Df und f. Somit ist f separabel.

106. Sei K ein Körper, $L : K$ eine Körpererweiterung, und $f \in K[X]$ ein Polynom über K. Beweisen Sie folgende universelle Eigenschaft von $R := K[X]/(f)$. Für jedes $x \in L$ existiert ein Ringhomomorphismus $\varphi\colon R \to L$ mit $\varphi(a) = a$ für alle $a \in K$ und $\varphi(\overline{X}) = x$ dann und nur dann falls $f(x) = 0$. Falls der Ringhomomorphismus existiert, so ist er eindeutig durch x bestimmt.

Lösung: Sei $x \in L$ und $f = \sum_{n=0}^{d} a_n X^n \in K[X]$ mit $f(x) = 0$. Die Inklusionsabbildung $i\colon K \to L, a \mapsto a$ ist ein Ringhomomorphismus. Also existiert nach der universellen Eigenschaft von Polynomringen (Algebra I, Kapitel 12, Thm. 12. 3.) ein Ringhomomorphismus $\varphi_0\colon K[X] \to L$ mit $\varphi_0(X) = x$ und $\varphi_0(a) = i(a) = a$ für alle $a \in K$. Falls $f(x) = 0$, dann gilt $f \in \ker(\varphi_0)$ weil

$$\varphi_0(f) = \varphi_0\Big(\sum_{n=0}^{d} a_n X^n\Big) = \sum_{n=0}^{d} \varphi_0(a_n)\varphi_0(X^n) = \sum_{n=0}^{d} a_n x^n = f(x) = 0. \tag{1}$$

Also existiert nach der universellen Eigenschaft des Quotienten ein eindeutiger Ringhomomorphismus $\varphi\colon K[X]/(f) \to L$ mit $\varphi(\overline{g}) = \varphi_0(g)$ für alle $g \in K[X]$. Für diesen Homomorphismus gilt

$$\varphi(\overline{X}) = \varphi_0(X) = x$$

und

$$\varphi(a) = \varphi(\overline{a}) = \varphi_0(a) = a$$

wobei $\overline{a} = a$ gilt in $K[X]/(f)$, weil so die Inklusion $K \to K[X]/(f)$ definiert wird. Also haben wir den gewünschten Homomorphismus konstruiert.

Sei $\varphi'\colon R \to L$ ein Homomorphismus mit $\varphi'(a) = a$ für alle $a \in K$ und $\varphi'(\overline{X}) = x$. Sei $g = \sum_{n=0}^{d} b_n X^n \in K[X]$. Dann gilt wie in (1)

$$\varphi'(\overline{g}) = \sum_{n=0}^{d} b_n x^n = \varphi_0(g).$$

Also erfüllt φ' die universelle Eigenschaft, von φ, nämlich $\varphi(\overline{g}) = \varphi_0(g)$ für alle $g \in K[X]$. Die Eindeutigkeit von φ besagt, dass φ der einzige Homomorphismus mit dieser Eigenschaft ist. Also folgt

$$\varphi = \varphi'.$$

Wir nehmen nun an, es existiert ein $\varphi\colon R \to L$ und ein $x \in L$ mit $\varphi(\overline{X}) = x$ und $\varphi(a) = a$ für alle $a \in K$. Nun erhalten wir wie in (1)

$$0 = \varphi(0) = \varphi(\overline{f}) = f(x).$$

Also folgt $f(x) = 0$.

107. Sei K ein Körper und $f = X^2 + aX + b \in K[X]$ ein irreduzibles Polynom über K. Sei $L := K[X]/(f)$ der Zerfallungskörper von f über K und $z := \overline{X} \in L$.

(a) Beweisen Sie die Gleichung

$$f = (X - z)(X + (z + a)).$$

(b) Konstruieren Sie einen K-Automorphismus $\sigma\colon L \to L$ mit $\sigma(z) = -z - a$. Beweisen Sie, dass σ eindeutig ist.

(c) Beweisen Sie, dass $-z - a = z$ dann und nur dann falls f inseparabel ist.

(d) Schliessen Sie aus (c), dass $\mathrm{Gal}(L : K)$ isomorph zu $\mathbb{Z}/2\mathbb{Z}$ ist, wenn f separabel ist, und isomorph zur trivialen Gruppe ist, falls f inseparabel ist.

(e) Sei K ein Körper mit Charakteristik $\neq 2$ und $\Delta := a^2 - 4b$. Beweisen Sie $L = K(\sqrt{\Delta})$ mit quadratischer Ergänzung. Bestimmen Sie $\sigma(\sqrt{\Delta})$.

Hinweis: Die Annahme an die Charakteristik ist äquivalent zur Existenz von $2^{-1} \in K$ weil $2 \neq 0$ in K. Also kann man in K durch 2 dividieren.

Lösung:

(a) Es gilt

$$f(z) = f(\overline{X}) = \overline{f} = 0.$$

Eine Polynomdivision zeigt, dass f in L als

$$f = (X - z)(X + (z + a))$$

zerfällt. Also ist $-(z + a)$ die zweite Nullstelle von f in K.

(b) Es gilt $f(-z - a) = 0$. Also existiert nach der universellen Eigenschaft aus Aufgabe 105 ein eindeutiger Ringhomomorphismus $\sigma\colon L \to L$ mit $\sigma(a) = a$ für alle $a \in K$ und $\sigma(z) = -z - a$. Die Abbildung σ ist K-linear, denn es gilt $\sigma(ab) = \sigma(a)\sigma(b) = a\sigma(b)$ für alle $a \in K$ und $b \in L$. Da es ein Körperhomomorphismus ist, ist er injektiv. Der K-Vektorraum L ist endlichdimensional, also ist σ eine Bijektion.

(c) Falls f inseparabel ist, dann hat es nur eine Nullstelle und somit folgt $-z - a = z$. Also muss die Charakteristik von K gleich zwei sein, weil nach Aufgabe 104 haben alle irreduziblen, inseparablen Polynome in einem Körper mit Charakteristik p Grad p^n für ein $n \geqslant 1$.

Umgekehrt, falls f inseparabel ist, dann folgt aus Aufgabe 104, dass K Charakteristik 2 hat und $a = 0$ gilt. Dies impliziert $z = -z - a$.

(d) Sei σ' ein K-Automorphismus von L. Dann folgt

$$f(\sigma'(z)) = \sigma'(f(z)) = 0,$$

also gilt $f(\sigma'(z)) = z$ und somit $\sigma'(z) = z$ oder $\sigma'(z) = -z-a$. Im ersten Fall erhalten wir die Identität, im zweiten Falls impliziert die Eindeutigkeit von σ die Gleichung $\sigma = \sigma'$. Also sind $\{1, \sigma\}$ die K-Automorphismen von L.

Falls f separabel ist, dann folgt aus Aufgabe (c) die Gleichung $z \neq -z - a$. Also ist σ nicht die Identität. Damit hat die Galois-Gruppe $\mathrm{Gal}(L : F)$ Ordnung 2. Die einzige Gruppe der Ordnung 2 ist die zyklische Gruppe, also folgt $\mathrm{Gal}(L : F) \cong \mathbb{Z}/2\mathbb{Z}$.

Fall f inseparabel ist, dann folgt $z = -z - a$ aus Aufgabe (a). Somit gilt $\sigma = \mathrm{id}$, in diesem Fall ist die Galois-Gruppe also isomorph zur trivialen Gruppe.

(e) Wir können f umschreiben zu

$$f = (X + a/2)^2 - \Delta/4.$$

Also gilt $(2z + a)^2 = \Delta$. Wir setzen $\sqrt{\Delta} := 2z + a$. Dann gilt $L = K(z) = K(\sqrt{\Delta})$ weil $z = (\sqrt{\Delta} - a)/2$. Weiters gilt

$$\sigma(\sqrt{\Delta}) = \sigma(2z + a) = -2z - 2a + a = -2z - a = -\sqrt{\Delta}.$$

108. Seien $K : L : F$ Erweiterungen von Körpern mit Charakteristik $\neq 2$, so dass die Erweiterungen $K : L$ und $L : F$ Grad 2 haben. In dieser Aufgabe beweisen Sie, dass $K : F$ durch eine Wurzel eines irreduziblen Polynoms $X^4 + aX^2 + b \in F[X]$ generiert wird.

(a) Verwenden Sie quadratische Ergänzung um ein $x \in K$ mit $x \notin L$ und $x^2 \in L$ zu konstruieren.

(b) Sei $x^2 \notin F$. Beweisen Sie, dass das Minimalpolynom von x über F Grad 4 hat. Schliessen Sie $K = F(x)$.

(c) Sei $x^2 \notin F$. Sei $X^2 + aX + b$ das Minmalpolynom von x^2 über F. Schliessen Sie aus Aufgabe (b), dass das Minimalpolynom x über F das Polynom $X^4 + aX^2 + b$ ist. Schliessen Sie in diesem Fall den Beweis der Behauptung aus der Aufgabe ab.

(d) Wir nehmen von nun an $x^2 \in F$ an. Konstruieren Sie $y \in L$ mit $y \notin F$ und $y^2 \in F$.

(e) Beweisen Sie, dass $\{1, x, y, xy\}$ eine Basis des F-Vektorraums K ist. Schliessen Sie daraus, dass das Minimalpolynom von $z := x + y$ über F Grad 4 hat und $K = F(z)$ gilt.

(f) Beweisen Sie, dass $a, b \in F$ mit

$$(X - (x + y))(X - (-x + y))(X - (x - y))(X - (-x - y)) = X^4 + aX^2 + b$$

existieren. Schliessen Sie nun den Beweis der Behauptung ab.

Hinweis: Sie können das Polynom auf `wolframalpha.com` ausfaktorisieren.

Lösung:

(a) Es existiert $x' \in K$ mit $x' \notin L$. Das Minimalpolynom von x' über L hat Grad 2, wir schreiben es als $f = X^2 + cX + d$. Wir können dieses Polynom auch schreiben als

$$X^2 + cX + d = (X + c/2)^2 + (d - c^2/4).$$

Wir definieren $x := x' + c/2$. Dann gilt also $x^2 = c^2/4 - d$. Insbesondere folgt $x^2 \in L$. Falls $x' \in L$, dann würde $x \in L$ folgen. Dies ist ein Widerspruch, also $x' \notin L$.

(b) Wir verwenden die Notation aus Aufgabe (a). Das Minimalpolynom von x über F hat Grad 2 oder Grad 4 weil $x \notin F$. Wir nehmen an es hat Grad 2. Das Minimalpolynom von x über F teilt das Minimalpolynom von x über L. Das Minimalpolynom von x über L ist $X^2 - x^2$. Also ist das Minimalpolynom von x über F auch $X^2 - x^2$. Dies ist ein Widerspruch, also hat das Minimalpolynom von x über F Grad 4.

(c) Das Polynom $X^4 + aX^2 + b$ ist ein monisches Polynom welches bei x verschwindet. Also ist $X^4 + aX^2 + b$ das Minimalpolynom von x über F. Insbesondere ist es irreduzibel. Weiter hat die Erweiterung $F(x) : F$ Grad 4, also gilt $F(x) = K$.

(d) Man kann das Argument aus Aufgabe (a) wieder anwenden.

(e) Sei $w \in K$. Die Menge $\{1, x\}$ definiert eine L-Basis von K über L, also existieren $\alpha, \beta \in L$ mit

$$w = \alpha + \beta x.$$

Die Menge $\{1, y\}$ definiert eine Basis von L über F, also existieren $\alpha', \alpha'', \beta', \beta'' \in F$ mit

$$w = (\alpha' + \alpha'' y) + (\beta' + \beta'' y)x = \alpha' + \alpha'' y + \beta' x + \beta'' xy.$$

Also erzeugt die Menge $\{1, y, x, xy\}$ den F-Vektorraum K. Dieser hat Dimension 4, also ist die Menge $\{1, y, x, xy\}$ eine Basis von K über F.

Das Minimalpolynom von z über F kann Grad $1, 2$ oder 4 haben. Wir nehmen an, das Minimalpolynom hat Grad 1. Dann gilt $z \in F$. Dies widerspricht jedoch der linearen

Unabhängigkeit der Menge $\{1, y, x, xy\}$. Wir nehmen an, das Minimalpolynom hat Grad 2. Dann existieren $\alpha, \beta \in F$ mit

$$0 = z^2 + \alpha z + \beta = 2xy + \alpha x + \alpha y + (x^2 + y^2 + \beta).$$

Da $2 \neq 0$ in F gilt, ist dies ein Widerspruch zur linearen Unabhängigkeit der Menge $\{1, y, x, xy\}$ über F. Also hat das Minimalpolynom Grad 4. Insbesondere hat die Erweiterung $F(z) : F$ Grad 4, also folgt $F(z) = K$.

(f) Wir betrachten das Polynom

$$f = (X - (x + y))(X - (-x + y))(X - (x - y))(X - (-x - y)).$$

Dieses Polynom faktorisiert aus zu

$$f = X^4 + (-2x^2 - 2y^2)X^2 + (x^4 + y^4 - 2x^2y^2).$$

Das Polynom f verschwindet bei z, hat Grad 4, ist normiert und hat Koeffizienten in F weil $x^2, y^2 \in F$. Also ist es das Minimalpolynom von z. Weiters generiert z die Erweiterung $K : F$.

109. Finden Sie ein Gegenbeispiel zu Aufgabe 107 in Charakteristik 2.

Hinweis: Betrachten Sie die Erweiterungen $\mathbb{F}_{16} : \mathbb{F}_4 : \mathbb{F}_2$.

Lösung: Wir betrachten die Erweiterungen im Hinweis. Wir nehmen an, es existiert ein irreduzibles Polynom $X^4 + aX^2 + b \in \mathbb{F}_2[X]$. Dieses Polynom ist inseparabel weil seine formale Ableitung verschwindet. Der Körper $\mathbb{F}_2$ ist perfekt, also ist das Polynom nicht irreduzibel. Dies ist ein Widerspruch.