Tutorium 5 von Alexander Zellner: Faktorisierung von nichtkonstanten normierten Polynomen mit einer Unbekannten über einem endlichen Körper in seine Primpotenzen

Sei p eine Primzahl, $e \in \mathbb{N}_+$, $q = p^e$ und K der Körper mit q Elementen.
Unser Ziel ist es die (im wesentlichen eindeutige) Primpotenzzerlegung eines nichtkonstantes, normiertes Polynom $f \in K[x] \setminus K$ vom Grad $d = \deg(f)$ zu berechnen.
Sei $R = K[x]/(f)$ und X die Restklasse von x in R.

a. Beweisen Sie, dass der Ring R ein d-dimensionaler K-Vektorraum mit Basis $B := (1, X, X^2, \dots, X^{d-1})$ ist.
Beweis:
Dass R ein K-Vektorraum ist, ist klar. Ebenso hat jede Linearkombination l von Elementen aus $\{1, \dots, x^{d-1}\}$ einen Grad$\leq d$. Ist die zugehörige Restklasse 0, heißt dies dass sie von f geteilt wird. Dies ist wegen $\deg(f) = d$ nur möglich falls $l = 0$. Damit ist gezeigt, dass die Vektoren aus B linear unabhängig sind.
Ist andererseits $g + (f) \in R$ beliebig mit $g \in K[x]$, so schreibe $g = qf + r$ mit $q, r \in K[x]$ und $\deg(r) < \deg(f) = d$. Hieraus folgt $g - r \in (f)$, d.h. $g + (f) = r + (f)$. Wegen $\deg(r) \leq d - 1$, ist nun gezeigt, dass B ein Erzeugendensystem von R ist. $\square$

b. Sei $Q = (q_{ij}) \in M(d, K)$, deren i-ter Zeilenvektor der Vektor von Koordinaten von $X^{q(i-1)}$ bzgl. der Basis B ist.
Weiterhin sei $g \in K[x]$ beliebig und $\gamma_0, \dots, \gamma_{d-1} \in K$ d.d. $g + (f) = \gamma_0 + \dots + \gamma_{d-1}X^{d-1}$.
Behauptung: $\overline{g}^q = (\gamma_0, \dots, \gamma_{d-1}) \cdot Q \cdot (1, X, \dots, X^{d-1})^{\text{transp.}}$.
Beweis:
Vorbemerkungen:
Aus der Algebra ist bekannt, dass die multiplikative Gruppe eines endlichen Körpers mit q Elementen, eine zyklische Gruppe mit $q-1$ Elementen ist. Folglich gilt $x^q = x$ für alle $x \in K$.
$p | \binom{p^e}{i}$ für $1 \leq i < p^e$, denn für ein derartiges i gilt $\binom{p^e}{i} = \frac{p^e}{i}\binom{p^e-1}{i-1}$ und $p | \frac{p^e}{i}$.
Deshalb folgt weil Char$K = p$ für $a, b \in K$: $(a+b)^q = \sum_{i=0}^{q} \binom{q}{i} a^i b^{q-i} = a^q + b^q$.
Induktiv folgt für $a_0, \dots, a_n \in K$: $(a_0 + \dots a_n)^q = a_0^q + \dots a_n^q$. Dies gilt sogar falls $a_i \in R$ und von der Form $b_i X^i$ mit $b_i \in K$ für $i = 0, \dots, n$, da die Koeffizienten b_i für $i = 1, \dots, n-1$ verschwinden.
Nun zum eigentlichen Beweis:
$\overline{g}^q = (\gamma_0 + \dots + \gamma_{d-1}X^{d-1})^q = \sum_{i=1}^{d} \gamma_{i-1}^q X^{q(i-1)}$
$\sum_{i=1}^{d} \gamma_{i-1} X^{q(i-1)} = \sum_{i=1}^{d} \gamma_{i-1} \sum_{j=1}^{d} q_{ij} X^{j-1} =$
$\sum_{i=1}^{d} \sum_{j=1}^{d} \gamma_{i-1} q_{ij} X^{j-1} =$
$(\gamma_0, \dots, \gamma_{d-1}) \cdot (\sum_{j=1}^{d} q_{1j} X^{j-1}, \dots, \sum_{j=1}^{d} q_{dj} X^{j-1})^{\text{transp.}} =$

$(\gamma_0, \dots, \gamma_{d-1}) \cdot Q \cdot (1, X, \dots, X^{d-1})^{\text{transp.}}$ $\square$

Sei nun $\beta := (\beta_0, \dots, \beta_{d-1}) := (\gamma_0, \dots, \gamma_{d-1}) \cdot (Q - E_d)$.

Offensichtlich gilt $\overline{g} = (\gamma_0, \dots, \gamma_{d-1}) \cdot (1, X, \dots, X^{d-1})^{\text{transp.}}$, folglich $\overline{g}^q - \overline{g} = \beta \cdot (1, X, \dots, X^{d-1})^{\text{transp.}}$, wobei E_d $d \times d$-Einheitsmatrix.

Gilt $\beta = 0$, so folgt $\overline{g}^q - \overline{g} = 0$. Gilt andererseits $\overline{g}^q - \overline{g} = 0$, so folgt $\beta_0 + \beta_1 X + \dots + \beta_{d-1} X^{d-1} = 0$ und somit $\beta = 0$, weil B Basis von R.

Insgesamt gilt also $\beta = 0 \Leftrightarrow \overline{g}^q - \overline{g} = 0$.

c. Sei $g \in K[x]$ ein Polynom mit $\overline{g}^q - \overline{g} = 0$ in R, so gilt $f = \prod_{\kappa \in K} \mathrm{ggT}(f, g - \kappa)$.

Beweis:

Beh. 1: $\prod_{\kappa \in K} \mathrm{ggT}(f, g - \kappa) | f$ (mit ggT ist der normierte ggT gemeint)

Trivialerweise teilt jeder Faktor rechten Seite f. Es genügt folglich zu zeigen, dass die Faktoren der rechten Seite teilerfremd sind. Dies ist klar, denn gäbe es ein Primelement $p \in R$ mit $p | g - \kappa_1$ und $p | g - \kappa_2$ ($\kappa_1, \kappa_2 \in K$, $\kappa_1 \neq \kappa_2$), so würde p auch das konstante Polynom $\kappa_1 - \kappa_2 \neq 0$ teilen. Widerspruch !

Beh. 2: $f | \prod_{\kappa \in K} \mathrm{ggT}(f, g - \kappa)$

Sei $f = \prod_{i=1}^{r} p_i^{\alpha_i}$ die Primfaktorzerlegung von f, wobei $\alpha_i > 0$ für $i = 1, \dots, r$ und $p_1, \dots, p_r$ die verschiedenen irreduziblen Faktoren von f sind.

Zwischenbeh: $x^q - x = (x - 0)(x - 1) \cdot \ldots \cdot (x - (q - 1))$ ($\in K[x]$)

Jedes $k \in K$ ist eine Nullstelle in $x^q - x$, folglich teilt jedes Polynom der Form $(x - k)$ das Polynom $x^q - x$. Für verschiedene k sind die Faktoren $(x - k)$ teilerfremd (dieselbe Schlussweise wie oben). Es gilt also $(x - 0) \cdot \ldots \cdot (x - (q - 1)) | (x^q - x)$. Weil beide normiert sind und beide den selben Grad besitzen müssen sie folglich identisch sein.

Sei $g \in K[x]$ nun ein Polynom mit $\overline{g}^q - \overline{g} = 0$,

Setze nun g in obige Gleichung ein und erhalte $g^q - g = (g - 0)(g - 1) \cdot \ldots \cdot (g - (q - 1))$. Um Beh. 2 zu zeigen, genügt es offensichtlich aus $f | ((g - 0) \cdot \ldots \cdot (g - (p - 1))$ zu zeigen. Dies ist aber äquivalent dazu, daß die Restklasse der rechten Seite=0 ist (*). Die kanonische Abbildung in den Restklassenring ist ein Homomorphismus, deshalb ist (*) äquivalent zu $(\overline{g} - 0) \cdot \ldots \cdot (\overline{g} - (q - 1)) = 0$. Die linke Seite dieses Terms ist aber gerade $\overline{g}^q - \overline{g}$ und gleich 0 nach Voraussetzung.

Bemerkung: Weil die $g - \kappa$ für verschiedene κ teilerfremd sind, gibt es zu jedem $i \in \{1, \dots, r\}$ genau ein $\kappa \in K$ mit $p_i^{\alpha_i} | (g - \kappa)$. $\square$

d. Beweis des folgenden Spezialfalls des chinesischen Restsatzes:

Beweis:

Die kanonische Abbildung $\epsilon : R \to K[x]/(p_1^{\alpha_1}) \times \ldots \times K[x]/(p_r^{\alpha_r})$ ist ein K-Algebrenisomorphismus.

Nach Konstruktion gilt offensichtlich, dass ϵ ein K-Algebrenhomomorphismus ist. Auch die Injektivität ist sofort klar, weil offensichtlich $\ker \epsilon = \{0\}$ gilt.

Zu zeigen bleibt lediglich die Surjektivität.

Sei dazu $(g_1 + (p_1^{\alpha_1}), \dots, g_r + (p_r^{\alpha_r})) \in K[x]/(p_1^{\alpha_1}) \times \ldots \times K[x]/(p_r^{\alpha_r})$ beliebig. Setze $h_l := \prod_{i \neq l} p_i^{\alpha_i}$ für $l = 1, \dots, r$. Die h_l sind paarweise teilerfremd, folglich

gibt es nach Euklid $a_1, \ldots, a_r \in K[x]$ mit $a_1 h_1 + \ldots + a_r h_r = 1$. Hieraus folgt $a_i h_i + (p_i^{\alpha_i}) = 1 + (p_i^{\alpha_i})$ für $i = 1, \ldots, r$.
Setze $y := \sum_{i=1}^r g_i a_i h_i$.
$\epsilon(y) = (y + (p_1^{\alpha_1}), y + (p_r^{\alpha_r})) = (g_1 a_1 h_1 + (p_1^{\alpha_1}), \ldots, g_r a_r h_r + (p_r^{\alpha_r})) = (g_1 + (p_1^{\alpha_1}), \ldots, g_r + (p_r^{\alpha_r}))$. Damit ist auch die Surjektivität gezeigt. □

Sei nun V definiert durch $V := \{\overline{g} \in R \mid \overline{g}^q - \overline{g} = 0\}$. Es ist leicht nachzurechnen, dass V ein Untervektorraum des Vektorraums R ist (denn $(g+h)^q = g^q + h^q$ für $g, h \in K[x]$). In c) wurde gezeigt, dass es zu jedem $i \in \{1, \ldots, r\}$ und jedem $g \in K[x]$ mit $\overline{g} \in V$ ein $\kappa_i \in K$ gibt, mit $p_i^{\alpha_i} | (g - \kappa_i)$. Folglich gilt $g + (p_i) = \kappa_i + (p_i)$. ϵ induziert folglich einen Vektorraummonomorphismus $\varphi : V \to K^r$.

Seien andererseits $\kappa_1, \ldots, \kappa_r \in K$ vorgeben. Nach dem chin. Restsatz gibt es ein $\overline{g} \in R$ mit $\epsilon(\overline{g}) = (\overline{\kappa}_1, \ldots, \overline{\kappa}_r)$. Um zu zeigen, daß φ sogar ein Vektorraumisomorphismus ist, genügt es nun offensichtlich zu zeigen, dass $\overline{g} \in V$, d.h. dass $\overline{g}^q - \overline{g} = 0$. Nun gilt aber für alle $i \in \{1, \ldots, r\}$: $g + (p_i^{\alpha_i}) = \kappa_i + (p_i^{\alpha_i})$.
Nun folgt: $g^q + (p_i^{\alpha_i}) = \kappa_i^q + (p_i^{\alpha_i}) = \kappa_i + (p_i^{\alpha_i}) = g + (p_i^{\alpha_i})$. Also gilt insgesamt $(p_i^{\alpha_i}) | (g^q - g)$ für alle $i \in \{1, \ldots, r\}$ und weil die p_i paarweise teilerfremd sind, folgt weiter $f | (g^q - g)$, also $g \in V$.

Nun zurück zu Teilaufgabe b). Die Menge W aller Elemente $(\gamma_0, \ldots, \gamma_{d-1}) \in K^d$ mit $(\gamma_0, \ldots, \gamma_{d-1}) \cdot (Q - E_d)$ ist offensichtlich ein K-Vektorraum.

e. Nach b) gilt $V \cong \ker(Q - E_d)$ und nach d) $K^r \cong V$. Folglich gilt $\dim_K(\ker(Q - E_d)) = r$.
Die Anzahl r der irreduziblen Faktoren von f wird folglich durch $\dim_K(\ker(Q - E_d))$ gegeben.

f. Betrachten Sie nun den folgenden Algorithmus:
1. Berechnung der oben definierten Matrix Q und der Zahl r.
Sei $\{(v_{i1}, \ldots, v_{id}) \mid 1 \leq i \leq r\}$ eine K-Basis von $\ker(Q - E_d)$ und seien $g_i = v_{i1} + \ldots + v_{id} x^{d-1} \in K[x]$ für $1 \leq i \leq r$. O.E. können wir annehmen, dass $g_r = 1$ und $\deg(g_i) > 0$ für $1 \leq i < r$.
2. Berechne für alle $\kappa \in K$ den $\mathrm{ggT}(f, g_1 - \kappa)$ und erhalte eine Darstellung $f = \prod_{\kappa \in K} \mathrm{ggT}(f, g_1 - \kappa)$. Wenn die Darstellung r verschiedene nichtkonstante Faktoren enthält, sind wir fertig.
3. Sei für $i = 1, 2, \ldots$ $f = f_{i1} \cdot \ldots \cdot f_{i\mu_i}$ die bereits berechnete Darstellung von f. Dabei sei o.E. kein $f_{ij} = 1$.
Für jedes $\kappa \in K$ und jedes $j \in \{1, \ldots, \mu_i\}$ berechne $\mathrm{ggT}(f_{ij}, g_{i+1} - \kappa)$. Überprüfe dann, ob die Darstellung $f = \prod_{j=1}^{\mu_i} \prod_{\kappa \in K} \mathrm{ggT}(f_{ij}, g_{i+1} - \kappa)$ aus r verschiedenen Faktoren$\neq 1$ besteht. Wenn nicht erhöhe i um eins und wiederhole 3., andernfalls gebe diese Darstellung als Ergebnis zurück. Bemerkung: Eine Aufspaltung der einzelnen Primzahlpotenzen in verschiedene Faktoren kann dabei nie stattfinden (vgl. Bem. in Teil c).

Nun ist noch zu zeigen, dass dieser Algorithmus nach höchstens r Schritten eine Darstellung von f als ein Produkt von Potenzen von r verschiedenen irreduziblen

Faktoren liefert.

Sei $A = (a_{ij})$ die zu φ bzgl. der Basis $(\overline{g}_1, \dots, \overline{g}_r)$ zugehörige Matrix.

Beh. 1: Die Anzahl der verschiedenen Einträge in der i-ten Spalte der Matrix A ist gleich μ_i für $i \in \{1, \dots, r-1\}$

Nach Definition der Matrix A gilt $\varphi(\overline{g}_i) = (a_{1i}, \dots, a_{ri})$ (*).

Nun ist $(*) \Leftrightarrow \epsilon(\overline{g}_i) = (a_{1i} + (p_1^{\alpha_1}), \dots, a_{ri} + (p_r^{\alpha_r}))$, aber andererseits ist $\epsilon(g_i) = (g_i + (p_1^{\alpha_1}), \dots, g_i + (p_r^{\alpha_r}))$. Es folgt $g_i - a_{1i} \in (p_1^{\alpha_1}), \dots, g_i - a_{ri} \in (p_r^{\alpha_r})$(**).

Betrachte zunächst die erste Spalte. Es gilt $f = \prod_{\kappa \in K} \mathrm{ggT}(f, g_1 - \kappa)$, insbesondere teilt jedes $p_i^{\alpha_i}$ genau ein $g - \kappa$. Es ist $f = f_{11} \cdot \dots \cdot f_{1\mu_1}$, wobei $f_{1j} = p_{k_1}^{\alpha_{k_1}} \cdot \dots \cdot p_{k_{\nu_j}}^{\alpha_{k_{\nu_j}}}$. Von den Einträgen von A in der ersten Spalte sind nach Konstruktion von f_{1j} nun offensichtlich die der k_1-ten,..., und k_{ν_j}-ten Zeile identisch. Zwei beliebige Einträge, die verschiedenen f_{1j} entsprechen, sind ebenso offensichtlich verschieden, weil die f_{ij} paarweise teilerfremd sind.

Betrachte nun Spalte i $(i > 1)$:

Nun ist $f_{(i-1)j} = \prod_{\kappa \in K} \mathrm{ggT}(f_{(i-1)j}, g_i - \kappa)$ nach Teilaufgabe c, weil trivialerweise $g^q - g + (f_{(i-1)j}) = 0$ ist. Der Rest folgt nun wie im Fall „erste Spalte“.

Beh. 2: Sei $j \in \{1, \dots, i-2\}$ beliebig und $i_1, i_2 \in \{1, \dots, r\}$ beliebig. Gilt $a_{i_1(j+1)} = a_{i_2(j+1)}$, so folgt $a_{i_1 j} = a_{i_2 j}$.

Beh. 2 ist klar, weil die Faktoren f_{ij} schrittweise aufgespaltet werden, d.h. es kann nicht vorkommen, dass es ein j gibt, so dass für alle j' gilt $f_{(i+1)j} \nmid f_{ij'}$.

Nun ist auch Beh. 2 gezeigt.

Würde der Algorithmus nicht spätestens für $i = r - 1$ eine Zerlegung von f in Primpotenzen liefern, so muss es nach Beh. 1 zwei Zeilen geben deren Eintrag der $r-1$-ten Spalte identisch sind.

Nach Beh. 2 ist dann aber auch die jeweiligen zwei Einträge in diesen Zeilen der Spalten links davon identisch. In der r-ten Spalte stehen offensichtlich sowieso nur Einsen $(g_r = 1!)$. Damit sind diese zwei Zeilen identisch.

Folglich gilt $\det(A) = 0$ im Widerspruch dazu, dass φ ein Isomorphismus ist.