M. Truong, M. Künzer

Algebra für Lehramt, SoSe 22

Lösung 13

Aufgabe 49 Für Kreisteilungspolynome verfügen wir über die Formel $X^n - 1 = \prod\limits_{\substack{d \in [1,n] \\ d \text{ teilt } n}} \Phi_d(X)$.

(1) Für jedes $n \in [1, 8]$ bestimme man das Kreisteilungspolynom $\Phi_n(X)$ unter Verwendung dieser Formel.

(2) Sei $p \in \mathbb{Z}_{\geqslant 1}$ eine Primzahl. Man bestimme $\Phi_{p^2}(X)$ unter Verwendung dieser Formel.

Ist das Bild von $\Phi_{p^2}(X)$ in $\mathbb{F}_p[X]$ unter koeffizientenweiser Restklassenbildung wieder irreduzibel?

Lösung.

Zu (1).

Es ist

$$X^1 - 1 \;=\; \prod_{\substack{d \in [1,1] \\ d \text{ teilt } 1}} \Phi_d(X) \;=\; \Phi_1(X)\,.$$

Also ist $\Phi_1(X) = X - 1$.

Es ist

$$X^2 - 1 \;=\; \prod_{\substack{d \in [1,2] \\ d \text{ teilt } 2}} \Phi_d(X) \;=\; \Phi_1(X) \cdot \Phi_2(X) \;=\; (X-1) \cdot \Phi_2(X)\,.$$

Also ist $\Phi_2(X) = \frac{X^2-1}{X-1} = X + 1$.

Es ist

$$X^3 - 1 \;=\; \prod_{\substack{d \in [1,3] \\ d \text{ teilt } 3}} \Phi_d(X) \;=\; \Phi_1(X) \cdot \Phi_3(X) \;=\; (X-1) \cdot \Phi_3(X)\,.$$

Also ist $\Phi_2(X) = \frac{X^3-1}{X-1} = X^2 + X + 1$.

Es ist

$$X^4 - 1 \;=\; \prod_{\substack{d \in [1,4] \\ d \text{ teilt } 4}} \Phi_d(X) \;=\; \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) \;=\; (X-1) \cdot (X+1) \cdot \Phi_4(X)\,.$$

Also ist $\Phi_4(X) = \frac{X^4-1}{X^2-1} = X^2 + X + 1$.

Es ist

$$X^5 - 1 \;=\; \prod_{\substack{d \in [1,5] \\ d \text{ teilt } 5}} \Phi_d(X) \;=\; \Phi_1(X) \cdot \Phi_5(X) \;=\; (X-1) \cdot \Phi_5(X)\,.$$

Also ist $\Phi_5(X) = \frac{X^5-1}{X-1} = X^4 + X^3 + X^2 + X + 1$.

Es ist

$$X^6 - 1 \;=\; \prod_{\substack{d \in [1,6] \\ d \text{ teilt } 6}} \Phi_d(X) \;=\; \Phi_1(X) \cdot \Phi_3(X) \cdot \Phi_2(X) \cdot \Phi_6(X) \;=\; (X^3-1) \cdot (X+1) \cdot \Phi_6(X)\,.$$

Also ist $\Phi_6(X) = \frac{X^6-1}{(X^3-1)(X+1)} = \frac{X^3+1}{X+1} = X^2 - X + 1$.

Es ist

$$X^7 - 1 \;=\; \prod_{\substack{d \in [1,7] \\ d \text{ teilt } 7}} \Phi_d(X) \;=\; \Phi_1(X) \cdot \Phi_7(X) \;=\; (X-1) \cdot \Phi_7(X)\,.$$

Also ist $\Phi_7(X) = \frac{X^7-1}{X-1} = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$.

Es ist

$$X^8 - 1 \;=\; \prod_{\substack{d \in [1,8] \\ d \text{ teilt } 8}} \Phi_d(X) \;=\; \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_4(X) \cdot \Phi_8(X) \;=\; (X^4-1) \cdot \Phi_8(X)\,.$$

Also ist $\Phi_8(X) = \frac{X^8-1}{X^4-1} = X^4 + 1$.

Zu (2). Es ist

$$X^{p^2} - 1 \;=\; \prod_{\substack{d \in [1,p^2] \\ d \text{ teilt } p^2}} \Phi_d(X) \;=\; \Phi_1(X) \cdot \Phi_p(X) \cdot \Phi_{p^2}(X) \;=\; (X^p - 1) \cdot \Phi_{p^2}(X)\;.$$

Also wird

$$\Phi_{p^2}(X) \;=\; \frac{X^{p^2}-1}{X^p-1} \;=\; \frac{(X^p)^p-1}{X^p-1} \;=\; \sum_{i \in [0,p-1]} (X^p)^i \;=\; \sum_{i \in [0,p-1]} X^{p \cdot i} \;=\; X^{p^2-p} + X^{p^2-2p} + \ldots + X^p + 1\;.$$

In $\mathbb{F}_p[X]$ wird $X^{p^2-p} + X^{p^2-2p} + \ldots + X^p + 1 = (X^{p-1} + X^{p-2} + \ldots + X + 1)^p$, was nicht irreduzibel ist.

Aufgabe 50 Man untersuche folgende Polynome aus $\mathbb{Q}[X]$ auf Irreduzibilität.

(1) $X^7 - 6X^3 + 4X^2 + 6$

(2) $X^4 + 4X^3 + 6X^2 + 4X + 3$

(3) $X^6 + 3X^3 + 2$

(4) $X^4 - 3X^3 + 9$

Lösung.
Zu (1). Es sind von $X^7 - 6X^3 + 4X^2 + 6 \in \mathbb{Z}[X]$ alle Koeffizienten durch 2 teilbar. Der Koeffizient von X^0 ist 6, welcher nicht durch 2^2 teilbar ist. Also ist das fragliche Polynom dank Eisenstein irreduzibel in $\mathbb{Q}[X]$.

Zu (2). Es ist $X^4 + 4X^3 + 6X^2 + 4X + 3 = (X+1)^4 + 2$.
Es sind von $u(T) := T^4 + 2 \in \mathbb{Z}[T]$ alle Koeffizienten durch 2 teilbar. Der Koeffizient von X^0 ist 2, welcher nicht durch 2^2 teilbar ist. Also ist $u(T)$ dank Eisenstein irreduzibel in $\mathbb{Q}[X]$.
Nun ist $X^4 + 4X^3 + 6X^2 + 4X + 3 = u(X+1)$ dank Translation irreduzibel in $\mathbb{Q}[X]$.

Zu (3). Sei $u(T) := T^2 + 3T + 2 \in \mathbb{Q}[T]$. Es ist $u(X^3) = X^6 + 3X^3 + 2$.
Es ist $u(T) = (T+1)(T+2)$.
Also ist $X^6 + 3X^3 + 2 = u(X^3) = (X^3+1)(X^3+2)$ in $\mathbb{Q}[X]$ nicht irreduzibel.

Zu (4). Das Polynom $X^4 - 3X^3 + 9$ ist irreduzibel in $\mathbb{Q}[X]$.
Um dies zu zeigen, genügt es zu zeigen, daß sein Bild $X^4 - 3X^3 + 9 = X^4 + X^3 + 1$ in $\mathbb{F}_2[X]$ irreduzibel ist.
Dieses Polynom hat keine Nullstelle in $\mathbb{F}_2$ und ist damit nicht durch ein Polynom von Grad 1 teilbar.
Bleibt zu zeigen, daß $X^4 + X^3 + 1$ nicht durch ein irreduzibles Polynom von Grad 2 teilbar ist in $\mathbb{F}_2[X]$.
Das einzige irreduzible Polynom von Grad 2 in $\mathbb{F}_2[X]$ ist $X^2 + X + 1$.
Division mit Rest in $\mathbb{F}_2[X]$ gibt

$$(X^4 + X^3 + 1) = (X^2 + X + 1)(X^2 + 1) + X\;,$$

mit einem Rest X ungleich 0. Also ist $X^4 + X^3 + 1$ nicht durch $X^2 + X + 1$ teilbar in $\mathbb{F}_2[X]$.

Aufgabe 51

(1) Man finde eine Primzahl $p \geqslant 5$, für welche $\mathrm{U}(\mathbb{F}_p) \neq \langle 3 \rangle$ ist.

(2) Sei $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)$. Sei $\delta = X + (X^4 + X + 1)$.
In $\mathbb{F}_{16}$ ist also $2 = 0$ und $\delta^4 = -\delta - 1 = \delta + 1$.
Ist $\mathrm{U}(\mathbb{F}_{16}) = \langle \delta \rangle$?
Man bestimme $|\{\, x \in \mathbb{F}_{16}^\times \,:\, \mathrm{U}(\mathbb{F}_{16}) = \langle x \rangle \,\}|$.

Lösung.
Zu (1). Durch Probieren finden wir für $p = 11$ folgendes.

n	0	1	2	3	4	5
3^n	1	3	-2	5	4	1

Also ist $|\langle 3\rangle| = 5$ in $\mathrm{U}(\mathbb{F}_{11})$. Insbesondere ist $\langle 3\rangle < \mathrm{U}(\mathbb{F}_{11})$.

Zu (2). Wir rechnen.

n	0	1	2	3	4	5	6	7	8
δ^n	1	δ	δ^2	δ^3	$\delta+1$	$\delta^2+\delta$	$\delta^3+\delta^2$	$\delta^3+\delta+1$	δ^2+1

n	9	10	11	12	13	14	15
δ^n	$\delta^3+\delta$	$\delta^2+\delta+1$	$\delta^3+\delta^2+\delta$	$\delta^3+\delta^2+\delta+1$	$\delta^3+\delta^2+1$	δ^3+1	1

Somit ist $\mathrm{U}(\mathbb{F}_{16}) = \langle\delta\rangle$.
Für $x = \delta^n$, wobei $n \in [0, 14]$, ist $\mathrm{U}(\mathbb{F}_{16}) = \langle x\rangle$ genau dann, wenn n teilerfremd zu 15 ist.
Es muß dazu also $n \in \{1, 2, 4, 7, 8, 11, 13, 14\}$ liegen.
Somit ist $|\{\, x \in \mathbb{F}_{16}^\times : \mathrm{U}(\mathbb{F}_{16}) = \langle x\rangle \,\}| = |\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$.

Aufgabe 52 Sei K ein Körper. Sei $f(X) \in K[X]^\times$.
Es heiße $f(X)$ *kubusfrei*, falls es kein $u(X) \in K[X]$ gibt mit $\deg(u(X)) \geqslant 1$, für welches $u(X)^3$ ein Teiler von $f(X)$ ist.
Man zeige folgendes.

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

(2) Ist $\mathrm{char}(K) = 0$ und ist $f(X)$ kubusfrei, dann ist $\mathrm{ggT}(f(X), f'(X), f''(X)) = 1$.

Lösung.
Zu (1). Sei $f(X)$ nicht kubusfrei. Wir haben zu zeigen, daß $\mathrm{ggT}(f(X), f'(X), f''(X)) \neq 1$ ist.
Wir können $u(X)$, $h(X) \in K[X]$ wählen mit $\deg(u(X)) \geqslant 1$ und $f(X) = u(X)^3 \cdot h(X)$.
Es genügt zu zeigen, daß $u(X)$ ein Teiler von $\mathrm{ggT}(f(X), f'(X), f''(X))$ ist.
Dazu genügt es zu zeigen, daß $u(X)$ ein Teiler von $f(X)$, von $f'(X)$ und von $f''(X)$ ist.
Es ist $u(X)$ ein Teiler von $f(X) = u(X)^3 \cdot h(X)$.
Es ist $u(X)$ ein Teiler von $f'(X) = 3u(X)^2 \cdot u'(X) \cdot h(X) + u(X)^3 \cdot h'(X)$.
Es ist $u(X)$ ein Teiler von

$$\begin{array}{rl} & f''(X) \\ = & 6u(X) \cdot u'(X)^2 \cdot h(X) + 3u(X)^2 \cdot u''(X) \cdot h(X) + 3u(X)^2 \cdot u'(X) \cdot h'(X) + 3u(X)^2 \cdot u'(X) \cdot h'(X) + u(X)^3 \cdot h''(X) \\ = & 6u(X) \cdot u'(X)^2 \cdot h(X) + 3u(X)^2 \cdot u''(X) \cdot h(X) + 6u(X)^2 \cdot u'(X) \cdot h'(X) + u(X)^3 \cdot h''(X) \end{array}$$

Zu (2). Sei $\mathrm{char}(K) = 0$. Sei $f(X)$ kubusfrei. Wir schreiben

$$f(X) \;=\; s \cdot f_1(X)^{e_1} \cdot f_2(X)^{e_2} \cdot \ldots \cdot f_k(X)^{e_k}\ ,$$

wobei $s \in K^\times$, wobei $k \geqslant 0$, wobei $f_1(X), \ldots, f_k(X) \in K[X]$ paarweise verschiedene normierte Polynome sind, und wobei wegen $f(X)$ kubusfrei stets $e_i \in \{1, 2\}$ ist für $i \in [1, k]$.
Annahme, es ist $\mathrm{ggT}(f(X), f'(X), f''(X)) \neq 1$. O.E. ist $f_1(X)$ ein Teiler von $\mathrm{ggT}(f(X), f'(X), f''(X))$ und damit von $f'(X)$ und von $f''(X)$.
Es ist

$$\begin{array}{rcl} 0 & \equiv_{f_1(X)} & f'(X) \\ & = & s \cdot \sum_{i\in[1,k]} e_i f_i(X)^{e_i - 1} \cdot f_i'(X) \cdot \prod_{j\in[1,k]\smallsetminus\{i\}} f_j(X)^{e_j} \\ & \equiv_{f_1(X)} & s \cdot e_1 f_1(X)^{e_1-1} \cdot f_1'(X) \cdot \prod_{j\in[2,k]} f_j(X)^{e_j}\ . \end{array}$$

Da $\mathrm{char}(K) = 0$, ist $e_1 \neq 0$ in K und, aus Gradgründen, $f_1(X)$ kein Teiler von $f_1'(X)$. Da $f_1(X)$ auch kein Teiler von $f_j(X)$ ist für $j \in [2,k]$, folgt, daß $f_1(X)$ ein Teiler von $f_1(X)^{e_1 - 1}$ sein muß, d.h. daß

$$e_1 \; = \; 2$$

ist.
Wir beachten, daß $(f_1(X)^2 \cdot u(X))' = 2f_1(X) \cdot f_1'(X) \cdot u(X) + f_1(X)^2 \cdot u'(X) \equiv_{f_1(X)} 0$ ist für $u(X) \in K[X]$.
Es folgt

$$\begin{array}{rcl} 0 & \equiv_{f_1(X)} & f''(X) \\ & = & (s \cdot \sum_{i \in [1,k]} e_i f_i(X)^{e_i - 1} \cdot f_i'(X) \cdot \prod_{j \in [1,k] \smallsetminus \{i\}} f_j(X)^{e_j})' \\ & \equiv_{f_1(X)} & (s \cdot 2 f_1(X) \cdot f_1'(X) \cdot \prod_{j \in [2,k] \smallsetminus \{i\}} f_j(X)^{e_j})' \\ & \equiv_{f_1(X)} & s \cdot 2 f_1'(X) \cdot f_1'(X) \cdot \prod_{j \in [2,k] \smallsetminus \{i\}} f_j(X)^{e_j} \end{array}$$

Wegen $\mathrm{char}(K) = 0$ ist aber $2 \neq 0$ ist K und, aus Gradgründen, $f_1(X)$ kein Teiler von $f_1'(X)$. Da $f_1(X)$ auch kein Teiler von $f_j(X)$ ist für $j \in [2,k]$, folgt, daß $f_1(X)$ kein Teiler der rechten Seite ist.
Wir haben einen *Widerspruch.*

Die Voraussetzung $\mathrm{char}(K) = 0$ kann nicht weggelassen werden. Z.B. ist $X^3 - 1 = (X-1)^3$ in $\mathbb{F}_3[X]$ nicht kubusfrei, aber es ist $\mathrm{ggT}(X^3 - 1, (X^3 - 1)', (X^3 - 1)'') = \mathrm{ggT}(X^3 - 1, 0, 0) = X^3 - 1 \neq 1$.