UNIVERSITÄT ULM

Prof. Dr. S. Wewers
WS 2013/2014

Lösungen Elemente der Algebra: Blatt 15

A1. Zerlegen Sie das Polynom f im Ring R in irreduzible Faktoren.

(a) $f = x^4 + x^2 + 1$, $R = \mathbb{F}_2[x]$ (+4)

Lösung: Es ist $f = (x^2 + x + 1)^2$ und die Faktoren sind irreduzibel, da sie keine Nullstelle in $\mathbb{F}_2$ haben.

(b) $f = x^4 + x^2 + 1$, $R = \mathbb{F}_4[x]$ (+4)

Lösung: Es ist $f = (x + a)^2(x + a + 1)^2$ wobei a die Nullstelle von $x^2 + x + 1$ ist.

(c) $f = x^3 + x + 1$, $R = \mathbb{F}_3[x]$ (+4)

Lösung: $f = (x + 2)(x^2 + x + 2)$ und der Faktor von Grad 2 ist irreduzibel, da er keine Nullstelle in $\mathbb{F}_3$ hat.

(d) $f = x^4 - x^2 + 1$, $R = \mathbb{F}_5[x]$ (+4)

Lösung: f hat keine Nullstelle, könnte also nur in Faktoren von Grad 2 zerfallen. Durch Koeffizientenvergleich bestimmt eine solche Faktorisierung als $f = (x^2+2x+4)(x^2 + 3x + 4)$.

(e) $f = x^6 - 1$, $R = \mathbb{F}_{25}[x]$ (+4)

Lösung: Durch iterierte Abspaltung von Nullstellen findet man $f = (x + 1)(x + 4)(x+2a+1)(x+2a+2)(x+3a+3)(x+3a+4)$ wobei a Nullstelle von $t^2+4t+2 = 0$ ist.

A2. (a) Bestimmen Sie alle irreduziblen Polynome in $\mathbb{F}_2[x]$ von Grad 4. (Hinweis: Beachten Sie Aufgabe A3.) (+8)

Lösung: In der Terminologie von A3 ist die Menge $P(4)$ zu bestimmen, d.h., die irreduziblen Teiler vom Grad 4 von $x^{16} - x$. Man teilt zunächst die offensichtlichen Teiler aus, d.h. x, $x - 1$, es bleibt $x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Nach Teilaufgabe (b) von A3 ist jedes Element von $P(2)$ auch ein Teiler von $x^{16} - x$. Dort gibt es aber nur ein Element $x^2 + x + 1$. Teilt man dies aus bleibt $x^{12} + x^9 + x^6 + x^3 + 1$. Wegen Teilaufgabe (c) von A3 muss dieses Polynom Produkt dreier irreduzibler Polynome von Grad 4 sein. Der konstante Koeffizient dieser Polynom muss jeweils 1 sein. Man rät die Faktoren $x^4 + x^3 + 1, x^4 + x + 1, x^4 + x^3 + x^2 + x + 1$.

(b) Betrachten Sie das irreduzible Polynom $f := x^4+x+1 \in \mathbb{F}_2[x]$. Sei α eine Nullstelle von f in $\mathbb{F}_{16}$. Wie Sie in der Vorlesung gesehen haben ist dann $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$, da f irreduzibel ist. Bestimmen Sie über $\mathbb{F}_2$ das Minimalpolynom von α^2 und α^4. (+5)

Lösung: Es ist $\alpha^4 = \alpha + 1$ und $\alpha^8 = \alpha^2 + 1$ und $\alpha^{16} = \alpha^4 + 1$ und also $(x^4 + x + 1)(\alpha^2) = 0$ wobei das Polynom nach (a) irreduzibel ist und $(x^4+x+1)(\alpha^4) = 0$. Es ist also das Minimalpolynom von $\alpha, \alpha^2, \alpha^4$ gleich. Das ist auch nicht verwunderlich, denn $f(x^2) = (f(x))^2$.

(c) Finden Sie einen Erzeuger der zyklischen Gruppe $\mathbb{F}_{16}^\times$. (+5)

Lösung: Die Ordnung der Elemente muss die Ordnung der Gruppe teilen, somit hat jedes Element Ordnung $1, 3, 5$ oder 15. Man könnte versuchen einfach ein Element der Ordnung 3 und eines der Ordnung 5 zu finden; deren Produkt hat dann Ordnung 15. Es ist aber $\alpha^3 \neq 1$ und $\alpha^5 = \alpha(\alpha + 1) = \alpha^2 + \alpha \neq 1$. Somit hat α keine der Ordnungen $1, 3, 5$ und also Ordnung 15.

(d) Nach Aufgabe A4 gilt $\mathbb{F}_4 \subseteq \mathbb{F}_{16}$. Finden Sie ein Element $\gamma \in \mathbb{F}_{16}$ sodass $\mathbb{F}_4 = \mathbb{F}_2[\gamma]$. (+5)

Lösung: Gesucht ist also eine Nullstelle von $x^2 + x + 1$ in $\mathbb{F}_{16}$. Durch Probieren findet man $x = \alpha^2 + \alpha$.

A3. Sei p eine Primzahl. Es bezeichne $P(n)$ die Menge der normierten irreduziblen Polynome vom Grad n in $\mathbb{F}_p[x]$.

(a) Sei $n \in \mathbb{N}$ und $f \in P(n)$. Zeigen Sie, dass f das Polynom $x^{p^n} - x$ teilt. (Hinweis: Betrachten Sie die Polynome als Elemente von $\mathbb{F}_{p^n}[x]$.) (+7)

Lösung: Sei $L := \mathbb{F}_p[x]/(f)$. Dies ist ein Körper mit p^n Elementen. Es bezeichne α die Klasse von x. Der Satz aus der Vorlesung zeigt, dass $x^{p^n} - x$ über L in Linearfaktoren zerfällt und die Nullstellen die Elemente von L sind. Insbesondere ist α Nullstelle von $x^{p^n} - x$. Da f irreduzibel ist, ist es das Minimalpolynom von α. Daraus folgt $f | x^{p^n} - x$.

(b) Sei $n \in \mathbb{N}$, d ein Teiler von n und sei f in $P(d)$. Zeigen Sie, dass f das Polynom $x^{p^n} - x$ teilt. (Hinweis: Verwenden Sie das Ergebnis aus Aufgabe A4.) (+3)

Lösung: Nach Voraussetzung gibt es ein m mit $dm = n$. Nach Aufgabe A4 ist $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. Sei $\alpha \in \mathbb{F}_{p^d}$ Nullstelle von f. Dann gilt $\alpha^{p^d} - \alpha = 0$. Somit ist $\alpha^{p^n} = \alpha^{p^d p^{d(m-1)}} = (\alpha^{p^d})^{p^{d(m-1)}} = \alpha^{p^{d(m-1)}} = \alpha^{p^d p^{d(m-2)}} = \cdots = \alpha$. Es ist also α Nullstelle von $x^{p^n} - x$ und somit teilt f dieses Polynom.

(c) Sei $n \in \mathbb{N}$. Zeigen Sie, dass gilt (+7)

$$x^{p^n} - x = \prod_{d|n} \prod_{f \in P(d)} f.$$

Lösung: Wir betrachten die Gleichung über $\mathbb{F}_{p^n}$. Dort zerfallen beide Seiten der Gleichung in Linearfaktoren. Es ist also zu zeigen, dass jede Nullstelle der linken Seite einfache Nullstelle der rechten Seite ist und umgekehrt. Sei $\alpha \in \mathbb{F}_{p^n}$ mit $\alpha^{p^n} - \alpha = 0$. Dann ist α Nullstelle eines irreduziblen Faktors von $x^{p^n} - x$ über $\mathbb{F}_p$, d.h. eines $f \in P(d)$ für ein $d \in \mathbb{N}$. Es ist jedoch $d|n$, da $\mathbb{F}_p[\alpha] \subseteq \mathbb{F}_{p^n}$ mit A4. Ferner ist α einfache Nullstelle, denn wäre $f(\alpha) = f'(\alpha) = 0$ für $f, f' \in P(d)$, dann ist $(f, f')(\alpha) = 0$ und somit $f = f'$ da die Polynome irreduzibel sind. Sei nun $\alpha \in \mathbb{F}_{p^n}$ Nullstelle der rechten Seite. Dann gibt es ein $d|n$ und $f \in P(d)$ mit $f(\alpha) = 0$. Da nach voriger Teilaufgabe f Teiler von $x^{p^n} - x$ ist, ist α Nullstelle von $x^{p^n} - x$. Es ist ferner eine einfache Nullstelle, da $x^{p^n} - x$ nur einfache Nullstellen hat.

(d) Bestimmen Sie für $p = 2$ die Mächtigkeit von $P(4)$. (+3)

Lösung: Nach A1.(a) ist das 3.

(e) Bestimmen Sie für $p = 3$ die Mächtigkeit von $P(3)$. (+3)

Lösung: Man entnimmt der Formel aus Teilaufgabe (c), dass für diese Mächtigkeit y gilt $3^3 = 3 + 3 \cdot y$ und somit $y = 8$.

A4. Sei p eine Primzahl, n, m in $\mathbb{N}$. In dieser Aufgabe soll gezeigt werden, dass der Körper $\mathbb{F}_{p^m}$ genau dann im Körper $\mathbb{F}_{p^n}$ enthalten ist, wenn $m|n$.

(a) Sei $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ der durch $\alpha \mapsto \alpha^p$ gegebene Automorphismus von $\mathbb{F}_{p^n}$ (siehe Satz 1 (iii) aus der Vorlesung vom 4.2.). Es lässt sich φ als Gruppenelement in der Gruppe der Automorphismen von $\mathbb{F}_{p^n}$ auffassen. Zeigen Sie, dass φ in dieser Gruppe Ordnung n hat, d.h. zeigen Sie, dass (+6)

$$n = \min\{k \in \mathbb{N} : \varphi^k = \mathrm{Id}\}.$$

Lösung: Es liegt n in der angegebenen Menge: Sei $\alpha \in \mathbb{F}_{p^n}$. Ist $\alpha = 0$, dann gilt offensichtlich $\varphi^n(\alpha) = \alpha$. Ansonsten liegt α in der zyklischen Gruppe $\mathbb{F}_{p^n}^\times$ und hat somit eine Ordnung, die $p^n - 1$ teilt. Es gilt also $a^{p^n - 1} = 1$ und also $\alpha^{p^n} = \alpha$. Insgesamt ist $\varphi^n = \mathrm{Id}$.
Es ist n das Minimum dieser Menge: Sei α ein Erzeuger von $\mathbb{F}_{p^n}^\times$. Damit ist $\alpha^{p^n} = \alpha$ und dies gilt für keinen kleineren Exponenten.

(b) Nehmen Sie an, dass $\mathbb{F}_{p^m}$ ein Teilkörper von $\mathbb{F}_{p^n}$ ist. Zeigen Sie, dass m dann n teilt. (Hinweis: Verwenden Sie die Einschränkung von φ auf $\mathbb{F}_{p^m}$ und die vorige Teilaufgabe.) (+6)

Lösung: Die Einschränkung hat nach obigem Ordnung m. Gleichzeitig muss aber weiterhin gelten, dass $\varphi^n = \mathrm{Id}$. Sei $a < m, b < n$ mit $(m,n) = an + bm$. Dann ist $\varphi^{an+bm} = (\varphi^n)^a \circ (\varphi^m)^b = \mathrm{Id}$. Nach Definition der Ordnung muss also gelten $(m,n) = m$, d.h. $m|n$.

(c) Nehmen Sie nun an, dass $m|n$. Zeigen Sie, dass dann $\mathbb{F}_{p^m}$ ein Teilkörper von $\mathbb{F}_{p^n}$ ist. (Hinweis: Argumentieren Sie wie im Beweis des Satzes aus der Vorlesung: Die Teilmenge der $\alpha \in \mathbb{F}_{p^n}$ mit $\alpha^{p^m} = \alpha$ ist ein Teilkörper.) (+10)

Lösung: Es bezeichne A die Menge der $\alpha \in \mathbb{F}_{p^n}$ mit $\alpha^{p^m} = \alpha$. Diese Menge ist nicht leer (sie enthält 0 und 1). Sie bildet eine additive abelsche Gruppe, denn mit $\alpha, \alpha' \in A$ gilt $(\alpha + \alpha')^{p^m} = \alpha^{p^m} + \alpha'^{p^m} = \alpha + \alpha'$. Sie bildet einen Ring, denn für $\alpha, \alpha' \in A$ gilt $(\alpha\alpha')^{p^m} = \alpha^{p^m}\alpha'^{p^m} = \alpha\alpha'$. Sie bildet sogar einen Körper, denn für $\alpha \in A$ gilt $(\alpha^{-1})^{p^m} = (\alpha^{p^m})^{-1} = \alpha^{-1}$ und also $\alpha^{-1} \in A$. Somit ist A ein endlicher Teilkörper. Da A eine Untergruppe von $\mathbb{F}_{p^n}$ ist, teilt M, die Ordnung von A, die Zahl p^n, d.h. es ist $M = p^k$ mit $k \leq n$. Da die Elemente von A Nullstellen von $x^{p^m} - x$ sind, welches höchstens p^m Nullstellen hat, ist $k \leq m$.

Um zu zeigen, dass $k \geq m$ konstruiert man ein Element in $A^\times$ mit Ordnung $p^m - 1$. Sei β ein Erzeuger von $\mathbb{F}_{p^n}^\times$ und setze $\alpha := \beta^{\frac{p^n-1}{p^m-1}}$. (Der Exponent ist ein eine natürliche Zahl, denn da $m|n$ gibt es ein k mit $n = km$ und somit $p^n - 1 = p^{km} - 1 = (p^m - 1)(p^{(k-1)m} + p^{(k-2)m} + \cdots + 1$.) Es ist $\alpha \in A$, denn $\alpha^{p^m-1} = \beta^{p^n-1} = 1$.