UE Einführung in die Algebra und Diskrete Mathematik
KV Algebra und Diskrete Mathematik

9. Übungszettel, 28. Mai 2013

1. Zerlegen Sie $x^5+2x^4+4x^3+x+4 \in \mathbb{Z}_5[x]$ in quadratfreie Faktoren (mittels Ableitung und ggT).
Lösung: Sei $f = x^5+2x^4+4x^3+x+4$. Dann ist $f' = 3x^3+2x^2+1$ und $ggT(f, f') = x^3+4x^2+2$. Mittels Polynomdivision erhält man, dass $f = (x^3+4x^2+2)(x^2+3x+2)$ ist. Nun muss man diese beiden Faktoren noch auf Quadratfreiheit überprüfen: $ggT(x^2+3x+2, 2x+3) = 1$ und $ggT(x^3+4x^2+2, 3x^2+3x) = x+1$. Somit ist x^2+3x+2 quadratfrei. Mit Polynomdivision bekommt man noch, dass $x^3+4x^2+2 = (x+1)(x^2+3x+2)$ ist, wobei beide Faktoren quadratfrei sind. Somit erhalten wir die quadratfreie Faktorisierung $f = (x^2+3x+2)(x+1)(x^2+3x+2)$.

---

2. Zerlegen Sie $x^4+2x^3+2x+2 \in \mathbb{Z}_3[x]$ in irreduzible Faktoren (mittels Berlekamp-Algorithmus).
Lösung: Anwenden des Berlekamp- Algorithmus (Sei $f := x^4+2x^3+2x+2$):

   (a) Da $ggT(f, x^3+2) = 1$, ist das Polynom quadratfrei.

   (b) Nun müssen die Reste von x^0, x^3, x^6, x^9 bei Division durch f:

$$\begin{aligned} x^0 &= 1 \mod f \\ x^0 &= x^3 \mod f \\ x^0 &= 2x^3+2x^2+2x+1 \mod f \\ x^0 &= x \mod f \end{aligned}$$

   Somit erhält man die Matrix

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

   (c) Basis für $\{x \in (\mathbb{Z}_3)^4 : x(Q-E) = 0\}$: $v(1) = (1,0,0,0)$ und $v(2) = (0,1,0,1)$ bilden eine Basis. Somit gibt es 2 irreduzible Faktoren.

   (d) Relevant ist jetzt nur $v(2) = (0,1,0,1)$ für uns. Bilden das Polynom $h(2) = x^3+x$ und finden nun alle irreduziblen Faktoren unter den $ggT(f, h(2)-c)$ mit $c \in \mathbb{Z}_3$:

$$\begin{aligned} ggT(f, x^3+x) &= x^2+1 \\ ggT(f, x^3+x+1) &= 1 \\ ggT(f, x^3+x+2) &= x^2+2x+2 \end{aligned}$$

Somit haben wir die Darstellung in irreduziblen Faktoren, $f = (x^2+1)(x^2+2x+2)$.

---

3. (a) Bestimmen Sie den Exponent von $f = x+5 \in \mathbb{Z}_7[x]$. Ist f maximalperiodisch?
   (b) Finden Sie ein irreduzibles Polynom in $\mathbb{Z}_7[x]$, dessen Grad größer als 5000 ist.

   Lösung: ad a) Da $x+6 = 1\cdot f+1$, $x^2+6 = (x+2)\cdot f+3$ und $x^3+6 = (x^2+2x+4)\cdot f$ ist, ist $e = 3$ der Exponent von f. Da $3 \neq 7^1-1$, ist f nicht maximalperiodisch.
   ad b) Wir wissen, dass $f = x+5$ irreduzibel in $\mathbb{Z}_7[x]$ ist. Der Grad ist $n = 1$ und der Exponent ist $e = 1$. Sei nun $t = 3^8 = 6561 > 5000$. t ist also kein Vielfaches von 4 und alle Primfaktoren teilen e aber nicht $\frac{p^n-1}{3} = 2$. Somit weiß man wegen Satz 15.16, dass $x^{3^8}+5 = x^{6}561+5$ irreduzibel in $\mathbb{Z}_7[x]$ ist.

---

4. Sei $g = x^3+x^2+2x+2 \in \mathbb{Z}_3[x]$.
   (a) Welche Vielfachheit hat 2 als Nullstelle von g? Hat g weitere Nullstellen? Wenn ja, mit welcher Vielfachheit?
   (b) Geben Sie ein Polynom $h \in \mathbb{Z}_3[x]$ mit $h \neq g$ an, sodass $\bar{h} = \bar{g}$.

   Lösung: ad a) Mit Polynomdivison bekommt man

$$\begin{aligned} g &= (x^2+2)(x+1) \\ g &= (x+2)(x+1)^2 \\ g &= 1\cdot(x+1)^3 + x^2 + 2x + 1 \end{aligned}$$

   Somit gilt $x+1|g$ und $(x+1)^2|g$ aber $(x+1)^3$ ist kein Teiler von g. daher ist 2 eine Nullstelle mit Vielfachheit 2 (Definition 16.6). Wegen $\bar{g}(1) = 0$ ist 1 noch eine weitere Nullstelle. Da der Grad von g aber 3 ist, kann 1 nur einen einfache Nullstelle sein (lt. Satz 16.7).
   ad b) Sei $h = (x+1)(x+1) = x^2+2$. Dann gilt $g \neq h$ aber $\bar{g} = \bar{h}$:

x	$\bar{h}$	$\bar{g}$
0	2	2
1	0	0
2	0	0

---

5. (a) Die formalen Potenzreihen $(\mathbb{Z}_p[[x]]\backslash\{\mathbf{o}\}, \cdot)$, bilden ein kommutatives Monoid. Zeigen Sie, dass die Kürzungsregel gilt.
   (b) Finden Sie durch unbestimmten Ansatz eine formale Potenzreihe $\sum_{i=0}^{\infty} a_i x^i$ über $\mathbb{Z}_p$, sodass

$$(1+x)\cdot\left(\sum_{i=0}^{\infty} a_i x^i\right) = 1$$

   gilt. (Beweis für für die zweite Aussage in Satz 17.4 b)

Lösung: ad a) Die formalen Potenzreihen sind über $\mathbb{Z}_p$ also einem Körper gegeben. Wir zeigen zuerst, dass die formalen Potenzreihen nullteilerfrei sind, d.h. falls $pq = \mathbf{o}$ dann ist $p = \mathbf{o}$ oder $q = \mathbf{o}$. Seien $p = (p_0, p_1, \ldots), q = (q_0, q_2, \ldots) \in \mathbb{Z}_p[[x]]$ mit $p \neq \mathbf{o}$ und $q \neq \mathbf{o}$. Dann gibt es minimale $s, t \in \mathbb{N}_0$ mit $p_s \neq 0$ und $q_t \neq 0$. Dann ist aber auch $(p \cdot q)_{s+t} = p_s q_t \neq 0$. Also ist $p \cdot q \neq \mathbf{o}$. Nun wissen wir, dass $\mathbb{Z}_p[[x]]$ nullteilerfrei ist. Es ist auch leicht zu überprüfen, dass die formalen Potenzreihen distributiv bzgl $+$ und $\cdot$ sind.
Nun zeigen wir die Kürzungsregel. Seien $a, b, c \in \mathbb{Z}_p[[x]] \backslash \{\mathbf{o}\}$ mit $a \cdot c = b \cdot c$. Daraus folgt $a \cdot c - b \cdot c = \mathbf{o}$ bzw. $(a - b) \cdot c = \mathbf{o}$. Da $c \neq \mathbf{o}$, muss $a - b = \mathbf{o}$ gelten. Somit aber $a = b$.
ad b)

$$\begin{aligned} 1 &= (1 + x) \cdot \left(\sum_{i=0}^{\infty} a_i x^i \right) \\ &= \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} a_i x^{i+1} \\ &= a_0 + \sum_{i=1}^{\infty} a_i x^i + \sum_{i=1}^{\infty} a_{i-1} x^i \\ &= a_0 + \sum_{i=1}^{\infty} (a_i + a_{i-1}) x^i \end{aligned}$$

Somit ist $a_0 = 1$ und für alle $i \geq 1$ gilt $a_i - a_{i-1} = 0$ bzw $a_i = a_{i-1}$. Also haben wir $a_{2n} = 1$ und $a_{2n+1} = -1$ für alle $n\mathbb{N}_0$. Die formale Potenzreihe ist also $1 - x + x^2 - x^3 + \ldots$.
