Musterlösung Serie 11

DER POLYNOMRING $\mathbb{F}_p[X]$

Im Folgenden sei p eine Primzahl und $\mathbb{F}_p[X]$ sei der Ring der Polynome mit der Unbestimmten X und Koeffizienten in $\mathbb{F}_p$. Für Polynome

$$f = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{F}_p[X]$$

ist der **Grad** von f die Zahl $\deg(f) := \max\{k \in \mathbb{N} : a_k \neq 0\}$, falls solch eine Zahl existiert, sonst sei $\deg(f) := -\infty$.

38. Für $f, g \in \mathbb{F}_p[X]$ sei $d \in \mathbb{F}_p[X]$ ein ggT von f und g, falls $d \mid f$ und $d \mid g$ sowie aus $h \mid f$ und $h \mid g$ folgt $h \mid d$.

(a) Bestimme einen ggT der beiden Polynome

$$2X^4 + 5X^3 + 6X^2 + 6X + 1,\ X^3 + 6X + 1 \in \mathbb{F}_7[X]$$

Hinweis: Verwende den vEA.

(b) Zeige: Ist $d \in \mathbb{F}_p[X]$ ein ggT von $f, g \in \mathbb{F}_p[X]$, so ist für alle $a \in \mathbb{F}_p\backslash\{0\}$ auch $a \cdot d$ ein ggT von f und g.

(c) Zeige: Sind d_1 und d_2 zwei ggT von $f, g \in \mathbb{F}_p[X]$, dann existiert ein $a \in \mathbb{F}_p$ mit $a \cdot d_1 = d_2$.

Lösung:

(a) Wir möchten den verallgemeinerten Euklid'schen Algorithmus auf die Polynome $2X^4 + 5X^3 + 6X^2 + 6X + 1 \in \mathbb{F}_7[X]$ und $X^3 + 6X + 1 \in \mathbb{F}_7[X]$ anwenden. Deshalb müssen wir zuerst die Koeffizienten b_n berechnen

$$2X^4 + 5X^3 + 6X^2 + 6X + 1 = (2X + 5) \cdot \left(X^3 + 6X + 1\right) + \left(X^2 + 2X + 3\right)$$
$$X^3 + 6X + 1 = (X + 5)\left(X^2 + 2X + 3\right).$$

Also ist $X^2 + 2X + 3 \in \mathbb{F}_7[X]$ der ggT von $2X^4 + 5X^3 + 6X^2 + 6X + 1$ und $X^3 + 6X + 1$ nach der Definition im Skript. Wir wollen nun auch zeigen, dass $X^2 + 2X + 3 \in \mathbb{F}_7[X]$ auch die Definition des ggT auf dem Aufgabenblatt erfüllt. Mit den Berechnungen oben sieht man, dass $(X^2 + 2X + 3) \,|\, (X^4 + 5X^3 + 6X^2 + 6X + 1)$ und $(X^2 + 2X + 3) \,|\, (X^3 + 6X + 1)$ gelten muss. Die Tabelle des verallgemeinerten Euklid'schen Algorithmus können wir nun wie folgt ausfüllen:

n	*-2*	*-1*	*0*	*1*
b_n			$2X + 5$	$X + 5$
P_n	**0**	**1**	$2X + 5$	$2X^2 + X + 5$
Q_n	**1**	**0**	1	$X + 5$

Nun gilt $1 \cdot (2X^2 + X + 5) - (2X + 5) \cdot (X + 5) = 1$. und wenn wir die Gleichung mit $X^2 + 2X + 3$ multiplizieren, dann erhalten wir:

$$2X^4 + 5X^3 + 6X^2 + 6X + 1 - (2X + 5) \cdot \big(X^3 + X + 1\big) = X^2 + 2X + 3$$

Das heisst, falls die Polynome $2X^4+5X^3+6X^2+6X+1 \in \mathbb{F}_7[X]$ und $X^3+6X+1 \in \mathbb{F}_7[X]$ einen Teiler haben, dann ist dieses Teiler auch ein Teiler von $X^2 + 2X + 3 \in \mathbb{F}_7[X]$. Daraus folgt die Aussage.

(b) Sei $d \in \mathbb{F}_p[X]$ ein ggT von $f \in \mathbb{F}_p[X]$ und $g \in \mathbb{F}_p[X]$ und $a \in \mathbb{F}_p\backslash\{0\}$. Dann existieren $h, l \in \mathbb{F}_p[X]$, sodass gilt $f = h \cdot d$ und $g = l \cdot d$ und a ist invertierbar. Wir haben also auch $f = (a^{-1}h) \cdot (ad)$ und $g = (a^{-1}l) \cdot (ad)$. Also gilt $ad|f$ und $ad|g$. Falls nun für $d' \in \mathbb{F}_p[X]$ ebenfalls gilt $d'|f$ und $d'|g$, dann folgt aus der Definition des ggT, dass $d'|d$ gilt und so folgt auch $d'|ad$.

(c) Falls d_1, d_2 zwei ggTs von $f, g \in \mathbb{F}_p[X]$ sind, dann gilt $d_1|f$, $d_1|g$ und $d_2|f$, $d_2|g$. Aus der Definition des ggT folgt nun aber auch $d_1|d_2$ und $d_2|d_1$. Das heisst, es existieren $b, c \in \mathbb{F}_p[X]\backslash\{0\}$, sodass gilt:

$$d_2 = d_1 \cdot b = d_2 \cdot (bc)$$

Es folgt, dass der Grad von b, c verschwinden muss und damit gilt $b, c \in \mathbb{F}_p$. Setzte $a := b$ und dann gilt $a \cdot d_1 = d_2$.

39. Für $f \in \mathbb{F}_p[X]$ sei $(f) := \big\{g \cdot f : g \in \mathbb{F}_p[X]\big\}$.

(a) Zeige, dass für alle $f \in \mathbb{F}_p[X]$, $(f) \subseteq \mathbb{F}_p[X]$ ein Ideal ist.

(b) Bestimme $\mathbb{F}_p[X]/(0)$, $\mathbb{F}_p[X]/(r)$ für $r \in \mathbb{F}_p\backslash\{0\}$, $\mathbb{F}_p[X]/(X)$, $\mathbb{F}_p[X]/(X + 1)$, und $\mathbb{F}_p[X]/(X^5)$.

(c) Zeige: Das Ideal $(f) \subseteq \mathbb{F}_p[X]$ für $f \in \mathbb{F}_p[X]$ mit $\deg(f) > 0$ ist genau dann maximal, wenn aus $g \cdot h = f$ für $g, h \in \mathbb{F}_p[X]$ folgt $\deg(g) = 0$ oder $\deg(h) = 0$.

Lösung:

(a) Wir müssen die folgenden drei Punkte von der Definition eines Ideals nachweisen:

($\mathbf{I_0}$) Da $f \in (f)$, gilt $(f) \neq \varnothing$.

($\mathbf{I_1}$) Falls $g, h \in \mathbb{F}_p[X]$, dann existieren $r, s \in \mathbb{F}_p[X]$, sodass gilt $g = r \cdot f$ und $h = s \cdot f$. Daraus folgt $g + h = r \cdot f + s \cdot f = (r + s) \cdot f \in (f)$.

($\mathbf{I_2}$) Falls $r \in \mathbb{F}_p[X]$ und $g \in (f)$, dann existiert $h \in \mathbb{F}_p[X]$, sodass gilt $g = h \cdot f$. Dann gilt $r \cdot g = r\,(h \cdot f) = (rh) \cdot f \in (f)$. Daraus folgt, dass (f) ein Ideal ist.

(b) Wir bestimmen für jede Menge ein minimales Repräsentantensystem:

- Bei $\mathbb{F}_p[X]/(0)$ bildet jedes Element eine eigene Äquivalenzklasse, da für ein $h \in \mathbb{F}_p[X]$ gilt $h + (0) = \{h + a : a \in (0)\} = \{h + a : a = 0\} = \{h\}$. Somit besteht ein minimales Repräsentantensystem von $\mathbb{F}_p[X]/(0)$ aus allen Elementen der Form $h + (0)$ mit $h \in \mathbb{F}_p[X]$.
- Bei $\mathbb{F}_p[X]/(r)$ sind alle Polynome in derselben Äquivalenzklasse. Denn für $r \in \mathbb{F}_p\backslash\{0\}$ existiert ein inverses Element $r^{-1} \in \mathbb{F}_p\backslash\{0\}$ und somit ist $1 = r^{-1} \cdot r \in (r)$, also auch $h = h \cdot 1 \in (r)$ für $h \in \mathbb{F}_p[X]$ beliebig. Daher gilt $\mathbb{F}_p[X] = (r)$ und für zwei Elemente $s, t \in \mathbb{F}_p[X]$ gilt $s = t + (s - t)$, also gilt auch $s + (r) = t + (r)$. Da s, t beliebig waren, folgt die Behauptung. Ein minimales Repräsentantensystem von $\mathbb{F}_p[X]/(r)$ besteht somit aus einem beliebigen Element aus $\mathbb{F}_p[X]/(r)$.

- Ein minimales Repräsentantensystem von $\mathbb{F}_p[X]/(X)$ besteht aus allen Elementen der Form $s + (X)$ für $s \in \mathbb{F}_p$. Denn für jedes Polynom $f \in \mathbb{F}_p[X]$, findet man mit Division mit Rest ein $g \in \mathbb{F}_p[X]$ und $r \in \mathbb{F}_p$, sodass gilt $f = g \cdot X + r$. Es gilt nun $g \cdot X \in (X)$ und somit ist $f + (X) = r + (X)$. Zudem gilt $r + (X) = s + (X)$ für $r, s \in \mathbb{F}_p$ genau dann, wenn $s - r \in (X)$, wobei das Letztere genau dann gilt, wenn $s - r = 0$ ist, also wenn $s = r$ gilt, da alle vom Nullpolynom verschiedene Polynome in (X) mindestens den Grad 1 haben. Dies zeigt die Behauptung.
- Die Elemente $r + (X + 1) \in \mathbb{F}_p[X]/(X + 1)$ für $r \in \mathbb{F}_p$ bilden ein minimales Repräsentantensystem für $\mathbb{F}_p[X]/(X + 1)$. Mit Division mit Rest findet man für ein $f \in \mathbb{F}_p[X]$ ein $g \in \mathbb{F}_p[X]$ und $r \in \mathbb{F}_p$, sodass gilt $f = g \cdot (X+1) + r$. Somit gilt $f + (X + 1) = r + (X + 1)$. Wir müssen noch zeigen, dass alle die Repräsentanten $r+(X+1)$ für $r \in \mathbb{F}_p$ verschieden sind. Dies folgt mit der analogen Argumentation wie bei $\mathbb{F}_p[X]/(X)$, wenn alle (X) durch $(X + 1)$ ersetzt werden und daraus auch die Behauptung.
- Sei $f \in \mathbb{F}_p[X]$ beliebig. Dann finden wir mit Division mit Rest ein $g \in \mathbb{F}_p[X]$ und $h \in \mathbb{F}_p[X]$ mit $\deg(h) \leqslant 4$, sodass gilt $f = g \cdot X^5 + h$. Dann gilt auch $f + (X^5) = h + (X^5)$. Also ist $h + (X^5)$ für $h \in \mathbb{F}_p[X]$ höchstens vom Grad 4 ein Repräsentantensystem von $\mathbb{F}_p[X]/(X^5)$. Zudem sind diese Elemente alle verschieden, denn für $r, s \in \mathbb{F}_p[X]$ höchstens vom Grad 4 ist $r + (X^5) = s + (X^5)$ genau dann, wenn $r - s \in (X^5)$ ist. Da aber $r - s$ höchstens den Grad 4 hat und alle vom Nullpolynom verschiedene Elemente in (X^5) mindestens vom Grad 5 sind, gilt in diesem Fall $r - s = 0$ und somit $r = s$. Dies zeigt, dass das Repräsentantensystem minimal ist.

(c) Sei $(f) \subseteq \mathbb{F}_p[X]$ maximal mit $\deg(f) > 0$ und seien $g, h \in \mathbb{F}_p[X]$ mit $f = g \cdot h$. Dann sind g und h offenbar verschieden vom Nullpolynom wegen $\deg(f) > 0$. Wir wollen nun zeigen, dass g oder h den Grad 0 hat. Es ist $f \in (h)$ und somit auch $(f) \subseteq (h)$. Da $(f) \subseteq \mathbb{F}_p[X]$ maximal ist, ist f in keinem echten Ideal echt enthalten. Das heisst, entweder ist $(h) = \mathbb{F}_p[X]$ oder es muss $(f) = (h)$ gelten. Wir betrachten nun beide Fälle einzeln und zeigen, dass die gewünschte Aussauge folgt:
Falls $(h) = \mathbb{F}_p[X]$, dann ist $1 \in (h)$, also existiert $q \in \mathbb{F}_p[X]$, sodass gilt $1 = q \cdot h$. Dann muss gelten $\deg(h) = 0$, da in $\mathbb{F}_p[X]$ nur die Elemente aus $\mathbb{F}_p$ invertierbar sind.
Ansonsten ist $(f) = (h)$. Daraus folgt $h \in (f)$ und somit existiert $q \in \mathbb{F}_p[X]$ mit $h = q \cdot f = q \cdot g \cdot h$, also gilt auch $h \cdot (q \cdot g - 1) = 0$. Da h vom Nullpolynom verschieden ist, gilt $q \cdot g - 1 = 0$ und somit $q \cdot g = 1$. Das heisst, dass $g \in \mathbb{F}_p[X]$ invertierbar sein muss und somit ist $g \in \mathbb{F}_p$ und es ist $\deg(g) = 0$.

Umgekehrt nehmen wir an, dass $f \in \mathbb{F}_p[X]$ mit $\deg(f) > 0$ nicht in ein Produkt von Polynomen mit echt positivem Grad zerlegbar ist. Falls $(f) \subseteq \mathbb{F}_p[X]$ nicht maximal ist, dann gilt $(f) = \mathbb{F}_p[X]$ oder es existiert ein echtes Ideal $I \subsetneq \mathbb{F}_p[X]$ mit $(f) \subsetneq I$.
Wir zeigen zuerst, dass $(f) = \mathbb{F}_p[X]$ zu einem Widerspruch führt: Falls $(f) = \mathbb{F}_p[X]$, dann ist $1 \in (f)$, also existiert $q \in \mathbb{F}_p[X]$ mit $1 = q \cdot f$. Daraus folgt, dass $f \in \mathbb{F}_p$ liegt und somit $\deg(f) = 0$ sein muss.
Somit ist I ein Ideal mit $(f) \subsetneq I \subsetneq \mathbb{F}_p[X]$. Sei $q \in I$ beliebig. Wir möchten nun zeigen, dass $q \in (f)$ ist. Da sowieso $0 \in (f)$ ist, können wir weiter annehmen, dass $d \neq 0$ gilt. Mit dem Euklid'schen Algorithmus finden wir dann $d := \mathrm{ggT}(f, q)$. Nach Definition des ggT gilt $d|f$, also gibt es ein $r \in \mathbb{F}_p[X]$ mit $f = d \cdot r$. Da f aber nicht in zwei Faktoren von echt positivem Grad zerlegbar ist, gilt entweder $\deg(d) = 0$ oder $\deg(r) = 0$.
Falls $\deg(d) = 0$, so können wir mit dem verallgemeinerten Euklid'schen Algorithmus

$g, h \in \mathbb{F}_p[X]$ finden mit $g \cdot f + h \cdot q = d$. Da $f, q \in I$, wäre dann aber auch $d \in I$ und somit ist auch $1 = d^{-1} \cdot d \in I$, also ist $I = \mathbb{F}_p[X]$, was ein Widerspruch ist.
Es muss also gelten $\deg(r) = 0$. Dann ist $r \in \mathbb{F}_p \backslash \{0\}$ und es gilt $d = r^{-1} \cdot f \in (f)$. Da d ein Teiler von q ist, gilt somit auch $q \in (f)$. Nun war $q \in I$ beliebig. Wir folgern daraus, dass $I \subseteq (f)$ gilt, was ein Widerspruch ist zu $(f) \subsetneq I$.
Wir haben nun die Annahme, dass $(f) \subseteq \mathbb{F}_p[X]$ nicht maximal ist, zum Widerspruch geführt. Somit muss $(f) \subseteq \mathbb{F}_p[X]$ maximal sein.

40. Sei $f = X^3 + X + 1 \in \mathbb{F}_7[X]$.

(a) Zeige, dass das Ideal $(f) \subseteq \mathbb{F}_7[X]$ ein maximales Ideal ist.

(b) Wie viele Elemente besitzt der Körper $\mathbb{F}_7[X]/(f)$?

(c) Berechne $(X^2 + 2)^{-1}$ im Körper $\mathbb{F}_7[X]/(f)$.
Hinweis: Vergleiche mit Aufgabe 37.

Lösung:

(a) Wir möchten zeigen, dass $(f) \subseteq \mathbb{F}_7[X]$ ein maximales Ideal ist mit Hilfe von Aufgabe 39 (c): Falls f in zwei Faktoren von echt positivem Grad zerlegbar ist, so besitzt f einen Teiler vom Grad 1. Das heisst, f hat einen Teiler der Form $g := aX + b$ für $a, b \in \mathbb{F}_7$ und $a \neq 0$. Da a invertierbar ist, sehen wir schnell, dass g die Nullstelle $a^{-1}(-b)$ hat. Dann muss aber auch $f \subseteq \mathbb{F}_7[X]$ dieselbe Nullstelle haben. Durch Einsetzten aller 7 Elemente in $\mathbb{F}_7[X]$ sehen wir jedoch, dass f keine Nullstelle besitzen kann. Dies ist ein Widerspruch. Somit ist f nicht in ein Produkt von Faktoren mit echt positivem Grad zerlegbar und mit Aufgabe 39 (c) folgt, dass $(f) \subseteq \mathbb{F}_7[X]$ maximal ist.

(b) Ähnlich wie bei Aufgabe 39 (b) können wir zeigen, dass wir für $\mathbb{F}_7[X]/(f)$ ein minimales Repräsentantensystem der Form $aX^2 + bX + c + (f)$ für $a, b, c \in \mathbb{F}_7$ finden. Das heisst, für jede Wahl von a, b, c erhalten wir ein anderes Element in $\mathbb{F}_7[X]/(f)$ und für jedes Element in $\mathbb{F}_7[X]/(f)$ existiert ein Repräsentant in der obigen Form. Daraus folgt

$$|\mathbb{F}_7[X]/(f)| = 7^3 = 343.$$

(c) Wir möchten den Euklid'schen Algorithmus auf die Polynome $X^3 + X + 1$ und $X^2 + 2$ anwenden. Dafür berechnen wir zuerst die Koeffizienten b_n für das Schema:

$$\begin{aligned} X^3 + X + 1 &= X \cdot \left(X^2 + 2\right) + (6X + 1) \\ X^2 + 2 &= (6X + 6)(6X + 1) + 3 \\ 6X + 1 &= (2X + 5) \cdot 3. \end{aligned}$$

Wir können nun die Tabelle unten ausfüllen wie im Vorlesungsskript beschrieben:

n	*-2*	*-1*	*0*	*1*	*2*
b_n			X	$6X + 6$	$2X + 5$
P_n	$\mathbf{0}$	$\mathbf{1}$	X	$6X^2 + 6X + 1$	$5(X^3 + X + 1)$
Q_n	$\mathbf{1}$	$\mathbf{0}$	1	$6X + 6$	$5(X^2 + 2)$

Offenbar gilt nun

$$(6X + 6)\, 5\left(X^3 + X + 1\right) - \left(6X^2 + 6X + 1\right) 5\left(X^2 + 2\right) = 6,$$

also gilt $-(6X^2+6X+1)\,5\,(X^2+2)+(f) = 6+(f)$ und dies lässt sich weiter vereinfachen zu $(2X^2+2X+5)\,(X^2+2)+(f) = 1+(f)$, das heisst, es gilt in $\mathbb{F}_7[X]/(f)$

$$\left(X^2+2\right)^{-1} = \left(2X^2+2X+5\right).$$

Bemerkung: Im Prinzip können wir alle Schritte von Aufgabe 37 übernehmen bis zur Zeile

$$(-X-1)\,\tfrac{1}{3}\left(X^3+X+1\right) - \left(-X^2-X+1\right)\tfrac{1}{3}\left(X^2+2\right) = -1,$$

wobei wir alle Zahlen der Zwischenschritte aus $\mathbb{Q}$ nach $\mathbb{F}_7$ konvertieren. Zum Beispiel wird dann $-X$ zu $6X$ oder $\frac{1}{3}$ zu 5. Im Allgemeinen können wir Berechnungen in einem endlichen Körper ohne Probleme zuerst mit rationalen Zahlen durchführen und dann diese in Zahlen des jeweiligen Körpers $\mathbb{F}_p$ umrechnen.

41. Konstruiere einen Körper mit 8 Elementen.

Lösung:

Betrachte $f := X^3+X+1 \in \mathbb{F}_2[X]$. Da sowohl $f(0) \neq 0$, als auch $f(1) \neq 0$, besitzt f in $\mathbb{F}_2$ keine Nullstellen. Mit den analogen Argumenten wie bei Aufgabe 40 (a), lässt sich nun zeigen, dass $(f) \subseteq \mathbb{F}_2[X]$ ein maximales Ideal ist und deshalb ist $\mathbb{F}_2[X]/(f)$ ein Körper nach Proposition 10.4. im Skript. Ein minimales Repräsentantensystem von $\mathbb{F}_2[X]/(f)$ besteht aus den Elementen aX^2+bX+c, wobei $a,b,c \in \{0,1\}$. Das heisst, es gilt

$$|\mathbb{F}_2[X]/(f)| = 2^3 = 8.$$