Polynomfunktionen und Polynompermutationen auf $\mathbb{Z}/p^n\mathbb{Z}$

Teil I – Bakkalaureatsseminar

Daniel Krenn*

10. September 2008

Zusammenfassung. Wir betrachten diejenigen Funktionen von $\mathbb{Z}/p^n\mathbb{Z}$ nach $\mathbb{Z}/p^n\mathbb{Z}$, welche als Polynome dargestellt werden können und dann weiter diejenigen, welche Permutationen sind, also die Automorphismen. Die Kardinalität dieser Mengen ist gut bekannt, die Struktur hingegen ist noch relativ wenig erforscht.

In Teil I werden wir uns mit Bedingungen befassen, wann solche Funktionen Polynome bzw. Permutationen sind und wie diese dargestellt werden können. Dann werden wir die Anzahl der Elemente von diesen Mengen bestimmen und zum Schluss noch eine Beschreibung des Kerns der Abbildung von $\mathbb{Z}[X]$ nach den Polynomfunktionen modulo p^n geben.

In Teil II werden wir die Polynompermutationsgruppe modulo p^n in ein Kranzprodukt $\mathcal{S}_p \wr \cdots \wr \mathcal{S}_p$ von symmetrischen Gruppen einbetten. Wir sehen uns die p-Sylowgruppen der Polynompermutationsgruppe modulo p^n genauer an. Dabei werden wir die Anzahl dieser Sylowgruppen bestimmen und die Struktur näher beschreiben.

Inhaltsverzeichnis

*daniel.krenn@student.tugraz.at

Vorbemerkungen

Die *natürlichen Zahlen* werden mit $\mathbb{N} = \{1, 2, 3, \dots\}$ bezeichnet und die *nicht-negativen ganzen Zahlen* mit $\mathbb{N}_0 = \{0, 1, 2, \dots\}$. Mit eckigen Klammern ist *Iverson-Notation* gemeint, also

$$[\textit{Bedingung}] = \begin{cases} 1, & \text{wenn } \textit{Bedingung} \text{ erfüllt ist,} \\ 0, & \text{sonst.} \end{cases}$$

Für die Elemente $a + m\mathbb{Z}$ aus $\mathbb{Z}/m\mathbb{Z}$ schreibe einfach nur a und $a = b$ im Restklassenring $\mathbb{Z}/m\mathbb{Z}$ meint $a \equiv b \mod m$. Mit f' ist die *formale Ableitung* des Polynoms $f(X)$ nach X gemeint.

1 Fallende Faktorielle und Co

Bevor wir nun endlich mit Polynomfunktionen und Polynompermutationen losstarten können, brauchen wir noch ein paar Kleinigkeiten.

Definition (fallende Faktorielle, steigende Faktorielle)**.** Sei $k \in \mathbb{N}_0$. Schreibe

$$X^{\underline{k}} := X(X-1)\dots(X-k+1) \tag{1.1}$$

und

$$X^{\bar{k}} := X(X+1)\dots(X+k-1), \tag{1.2}$$

mit der Konvention $X^{\underline{0}} = X^{\bar{0}} = 1$.

Wir werden uns im weiteren (fast) ausschließlich mit den fallenden Faktoriellen beschäftigen, weil wir diese später dann brauchen werden.

Viele von den nachfolgenden Eigenschaften sind in [4] nachzulesen.

Proposition. *1. Für $k \geq 0$ ist $X^{\underline{k}} \in \mathbb{Z}[X]$ und der Leitkoeffizient ist* 1

2. $X^m = \sum_{j=0}^{m} \left\{ {m \atop j} \right\} X^{\underline{k}}$, wobei $\left\{ {m \atop j} \right\}$ die Stirlingzahlen 2. Art *sind.*

3. Die Menge $\left\{X^{\underline{k}}\right\}_{k \in \mathbb{N}_0}$ bildet eine $\mathbb{Z}$-Basis von $\mathbb{Z}[X]$

Beweis. 1. Ergibt sich durch ausmultiplizieren.

2. Durchrechnen mittels vollständige Induktion.

3. Ergibt sich aus der Beziehung aus 2. und weil $\left\{X^{\underline{k}}\right\}_{k\in\mathbb{N}_0}$ eine Basis bildt.

□

Proposition (Rechenregeln)**.** *1.* $X^{\underline{k}} = X^{\underline{k-1}}(X-k+1)$

2. $X^{\underline{k+l}} = X^{\underline{k}}(X-k)^{\underline{l}} = X - l^{\underline{k}}(X)^{\underline{l}}$

3. $(X+Y)^{\underline{k}} = \sum_i \binom{k}{i} X^{\underline{i}} Y^{\underline{k-i}}$

4. $(X+1)^{\underline{k}} = X^{\underline{k}} + kX^{\underline{k-1}}$

5. $XX^{\underline{k}} = X^{\underline{k+1}} + kX^{\underline{k}}$

6. $(-X)^{\bar{k}} = (-1)^k X^{\underline{k}}$

7. $X^{\bar{k}} = (X+k-1)^{\underline{k}}$

Beweis. Durch nachrechnen. □

Bemerkung. Mittels fallender und steigender Faktorielle können auch die *Fakultät* $k! = k^{\underline{k}} = 1^{\bar{k}}$ und der *Binomialkoeffizient* $\binom{X}{k} = \frac{X^{\underline{k}}}{k!}$ geschrieben werden.

Definition. Sei p eine Primzahl und $k \in \mathbb{N}_0$. Definiere

$$\alpha_p(k) := \max\left\{s \in \mathbb{N}_0 : p^s | k!\right\} \tag{1.3}$$

und

$$\beta_p(k) := \min\left\{t \in \mathbb{N}_0 : p^k | t!\right\}. \tag{1.4}$$

Proposition. *Sei $k \in \mathbb{N}_0$. Dann gilt*

$$\beta_p(k) = \min\left\{t \in \mathbb{N}_0 : \alpha_p(t) \geq k\right\}. \tag{1.5}$$

Beweis.

$$\begin{aligned}
\beta_p(k) &= \min\left\{t \in \mathbb{N}_0 : p^k | t!\right\} \\
&= \min\left\{t \in \mathbb{N}_0 : \max\left\{s \in \mathbb{N}_0 : p^k | p^s | t!\right\}\right\} \\
&= \min\left\{t \in \mathbb{N}_0 : \max\left\{s \in \mathbb{N}_0 : s \geq k \text{ und } p^s | t!\right\}\right\} \\
&= \min\left\{t \in \mathbb{N}_0 : \max\left\{s \in \mathbb{N}_0 : p^s | t!\right\} \geq k\right\} = \min\left\{t \in \mathbb{N}_0 : \alpha_p(t) \geq k\right\}
\end{aligned} \tag{1.6}$$

□

Proposition. *Sei $k \in \mathbb{N}_0$ und $f(X) = X^{\underline{k}}$. Dann gilt $k! | f(a)$ für alle $a \in \mathbb{Z}$, insbesondere also $p^{\alpha_p(k)} | f(a)$ für alle $a \in \mathbb{Z}$ und $f(a) \equiv 0 \mod p^n$, falls $\alpha_p(k) \geq n$.*

Beweis. Ohne Beschränkung der Allgemeinheit gilt $a \geq 0$, weil

$$(-a)^{\underline{k}} = (-1)^k a^{\bar{k}} = (-1)^k (a-k+1)^{\underline{k}}. \tag{1.7}$$

Ist $a < k$, dann ist $f(a) = 0$ und die Teilbarkeitsrelation trivialerweise erfüllt. Für $a = k$ gilt klarerweise $k!|k!$. Betrachten wir also $a+1$. Gilt $k!|a^{\underline{k-1}}$, dann sind wir fertig, denn der Faktor $a-k+1$ wird für die Teilbarkeit nicht benötigt.

Ansonsten gibt es ein $1 \leq l \leq k$, welches nur den Faktor $(a-k+1)$ teilt. Da es alle anderen $k-1$ Faktoren nicht teilt, muss $l = k$ gelten, und damit $l = k|(a+1)$. □

2 Allgemeines über Polynomfunktionen

In diesem Kapitel sei p eine beliebige, aber fixe Primzahl und $n \in \mathbb{N}$.

Definition. Bezeichne die Menge der Abbildungen von $\mathbb{Z}/p^n\mathbb{Z}$ in sich selbst mit Φ_n.

Zwei Funktionen $g, h \in \Phi_n$ heißen *gleich*, $g = h$, falls

$$\forall a \in \mathbb{Z}/p^n\mathbb{Z} : g(a) \equiv h(a) \mod p^n. \tag{2.1}$$

Definition (Polynomfunktion)**.** Sei φ_n die natürliche Abbildung von $\mathbb{Z}[X]$ nach Φ_n, also Auswertung in $\mathbb{Z}/p^n\mathbb{Z}$.

Eine Funktion $g \in \Phi_n$ heißt *induziert durch ein Polynom*, falls es ein Polynom $f(X) \in \mathbb{Z}[X]$ mit $\varphi_n(f) = g$ gibt. Bezeichne die Menge der durch Polynome induzierten Funktionen von Φ_n mit $\mathcal{F}_n$. Die Elemente von $\mathcal{F}_n$ heißen *Polynomfunktionen modulo* p^n.

Notation. Sofern nicht anders angegeben, schreibe f_n für ein Element aus $\mathcal{F}_n$ welches durch ein Polynom $f \in \mathbb{Z}[X]$ induziert wird.

Proposition. $(\mathcal{F}_n, \circ)$ *ist einen Monoid bezüglich Hintereinanderausführung*

Beweis. „$\circ$“ ist eine innere Verknüpfung und Assiziativität ergeben sich durch einsetzen. Dass $\mathrm{id}_{\mathcal{F}_n} = X$ das neutrale Element ist, ist ebenfalls leicht zu erkennen. □

Satz 2.1. *Sei $\mathbb{F}_q$ der endliche Körper mit q Elementen, q Primzahlpotenz, und sei $f : \mathbb{F}_q \to \mathbb{F}_q$ eine Funktion. Dann kann f eindeutig als Polynom vom Grad* $\deg f \leq q-1$ *dargestellt werden.*

Beweis. Sei f eine Funktion auf $\mathbb{F}_q$. Für jedes $\alpha \in \mathbb{F}_q \backslash \{0\}$ gilt $\alpha^q - \alpha = 0$ beziehungsweise $\alpha^{q-1} = 1$. Setze

$$g(X) := \sum_{\alpha \in \mathbb{F}_q} f(\alpha) \left(1 - (X-\alpha)^{q-1}\right). \tag{2.2}$$

Damit gilt $f = g$ in $\mathbb{F}_q$.

Sei $h(X)$ ein weiteres Polynom, für welches $f = h$ in $\mathbb{F}_q$ gilt. Dann gilt für die Differenz

$$(g-h)(\alpha) = g(\alpha) - h(\alpha) = f(\alpha) - f(\alpha) = 0 \tag{2.3}$$

in jedem Punkt $\alpha \in \mathbb{F}_q$ und somit die Gleichheit bezüglich $\mathbb{F}_q$. □

Für uns ist der Fall $\mathbb{F}_p$ interessant, da $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Dort können also alle Funktionen als Polynome dargestellt werden, und somit natürlich auch alle Permutationen von $\mathcal{S}_p$ (siehe Kapitel 3).

Für $\mathbb{Z}/p^n\mathbb{Z}$ mit $n \geq 2$ gilt das nicht mehr. Wählen wir zum Beispiel $f(0) = 0$ und $f(\alpha) = 1$ sonst, so hat das zugehörige Polynom die Gestalt $a_nX^n + \cdots + a_1X$. Für ein $\alpha \neq 0$ gilt dann

$$1 = a_n\alpha^n + \cdots + a_1\alpha = \alpha\left(a_n\alpha^{n-1} + \cdots + a_1\right), \tag{2.4}$$

und somit ist α eine Einheit, was im Allgemeinen in $\mathbb{Z}/p^n\mathbb{Z}$ nicht der Fall sein muss.

Wir wollen nun untersuchen, wann sich eine Funktion als Polynom darstellen lässt. Dafür sind in einem Artikel von L. Carlitz in der *Acta Arithmetica* [2] die folgenden Äquivalenzen zu finden.

Satz 2.2 (Charakterisierung von Polynomfunktionen)**.** *Sei f eine Funktion über $\mathbb{Z}/p^n\mathbb{Z}$ und sei $\nu(r) = \min(n, \alpha_p(r))$. Setze*

$$\Delta^r(f, X) := \sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}f(X+s). \tag{2.5}$$

und

$$\delta^r(f, X) := \sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}f(X+sp). \tag{2.6}$$

Dann sind folgende Aussagen äquivalent.

(1) f ist eine Polynomfunktion modulo p^n.

(2) Für alle $c \in \mathbb{Z}/p^n\mathbb{Z}$ und alle $r \geq 0$ gilt

$$\Delta^r(f, c) \equiv 0 \mod p^{\nu(r)}. \tag{2.7}$$

(3) Für $r \in \{0, \ldots, p^n - 1\}$ gilt

$$\Delta^r(f, 0) \equiv 0 \mod p^{\nu(r)}. \tag{2.8}$$

(4) Es existieren $f_0, \ldots, f_{n-1}$ Funktionen über $\mathbb{Z}/p^n\mathbb{Z}$, sodass

$$f(X+kp) \equiv f_0(X) + kpf_1(X) + \cdots + (kp)^{n-1}f_{n-1}(X) \mod p^n \tag{2.9}$$

für alle $k \in \mathbb{Z}$ erfüllt ist.

(5) Für alle $r \in \{0, \ldots, p^n - 1\}$ und alle $c \in \mathbb{Z}/p^n\mathbb{Z}$ gilt

$$\delta^r(f, c) \equiv 0 \mod p^{\nu(rp)}. \tag{2.10}$$

Beweis. *(1) $\Longrightarrow$ (2).* Sei $f = a_m X^m + \cdots + a_1 X + a_0$. Für beliebiges $r \in \mathbb{N}_0$ ist damit

$$\sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} f(c+s) = \sum_{j=0}^{m} a_j \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} (c+s)^j \equiv 0 \mod p^{\alpha_p(r)}, \tag{2.11}$$

da

$$\sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} (c+s)^j = 0 \quad \text{für } 0 \leq j < r \tag{2.12}$$

und $r!$ diesen Ausdruck teilt, falls $j \geq r$. Dies gilt, weil für $c = 0$ (2.12) gleich $\left\{ {j \atop r} \right\} r!$ ist (wobei $\left\{ {j \atop r} \right\}$ die *Stirlingzahlen 2. Art* sind), siehe [4]. Für allgemeine $c \in \mathbb{Z}$ ist dies dann durch Auspotenzieren von $(c+s)^j$ ersichtlich.

Die Kongruenz (2.11) gilt klarerweise auch für alle kleineren Potenzen, somit auch für $\nu(r)$.

(2) $\Longrightarrow$ (3). Trivial.

(3) $\Longrightarrow$ (1). Sei g eine beliebige Funktion auf $\mathbb{Z}/p^n\mathbb{Z}$ mit $\Delta^r(g,0) \equiv 0 \mod p^{\nu(r)}$. Definiere

$$f(X) := \sum_{j=0}^{N} \frac{1}{j!} \Delta^j(g,0) X^{\underline{j}}, \tag{2.13}$$

wobei wir N später noch geeignet wählen.

$f(X)$ ist ein Polynom auf $\mathbb{Z}/p^n\mathbb{Z}$, da nach Voraussetzung die $\frac{\Delta^j(g,0)}{j!}$ ganzzzahlig modulo p sind.

Für $0 \leq c < p^n$ gilt

$$\begin{aligned} f(c) &= \sum_{j=0}^{N} \frac{1}{j!} \Delta^j(f,0) c^{\underline{j}} \\ &= \sum_{j=0}^{N} \binom{c}{j} \Delta^j(f,c) \\ &= \sum_{j=0}^{N} \binom{c}{j} \sum_{s=0}^{j} (-1)^{j-s} \binom{j}{s} g(s) \\ &= \sum_{s=0}^{N} \binom{s}{s} g(s) \sum_{j=s}^{N} (-1)^{j-s} \binom{c-s}{j-s}. \end{aligned} \tag{2.14}$$

Ist $N \geq p^n$ so bleibt für die innere Summe nur der Term für $s = c$ übrig, und somit gilt für $c \in \{0, \ldots, p^n - 1\}$

$$f(c) = g(c) \tag{2.15}$$

und damit dir Gleichheit von f und g modulo p^n.

(1) $\Longrightarrow$ *(4).* Ist klar, auspotenzieren und sortieren nach Potenzen von kp.

(4) $\Longrightarrow$ *(5).* Es gilt

$$\delta^r(f,c) = \sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}f(c+sp) \equiv \sum_{j=0}^{n-1}p^j f_j(c)\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}s^j \mod p^n. \tag{2.16}$$

Da die innere Summe wieder durch $p^{\alpha_p(r)}$ teilbar ist und für $j < r$ verschwindet, gilt

$$\delta^r(f,c) \equiv 0 \mod p^{\nu(rp)}. \tag{2.17}$$

(5) $\Longrightarrow$ *(2).* Auch dieser Beweisteil ist nicht schwer, ich möchte aber hier auf [2] verweisen. □

3 Allgemeines über Polynompermutationen

In diesem Kapitel sei p eine beliebige, aber fixe Primzahl und $n \in \mathbb{N}$.

Definition (Polynompermutation)**.** Die *Gruppe der Polynompermutationen modulo* p^n ist die Teilmenge der Automorphismen von $\mathcal{F}_n$, bezeichne diese mit $\mathcal{P}_n$. Die Elemente von $\mathcal{P}_n$ heißen *Polynompermutationen modulo* p^n.

Proposition. *Die Polynompermutationsgruppe* $(\mathcal{P}_n, \circ)$ *ist eine Gruppe bezüglich Komposition, und die Elemente sind tatsächlich Permutationen.*

Beweis. Gruppe klar, weil die Menge der Automorphismen eine Gruppe bilden. Ein Element ist eine Permutationen, weil es eine bijektive Abbildung einer endlichen Menge in sich selbst ist. □

Da laut Satz 2.1 jede Funktion modulo p als Polynom dargestellt werden kann, sind auch alle möglichen Permutationen mit p Elementen vorhanden, d.h. $\mathcal{P}_1 = \mathcal{S}_p$. Für $n \geq 2$ gilt dies nicht mehr. Wir wollen uns nun im Folgenden anschauen, wie es sich da verhält.

Satz 3.1 kann in [5, Theorem 123] oder in einer verallgemeinerten Form in [8] nachgelesen werden.

Satz 3.1. *Sei* $n \geq 2$ *und* $f \in \mathbb{Z}[X]$*. Die Anzahl der Lösungen von*

$$f(X) \equiv 0 \mod p^n, \tag{3.1}$$

die zu einer Lösung von

$$f(X) \equiv 0 \mod p^{n-1} \tag{3.2}$$

gehören, ist

1. *Null, wenn* $f'(\xi) \equiv 0 \mod p$ *und* ξ *keine Lösung von* (3.2) *ist,*

2. *Eins, wenn* $f'(\xi) \not\equiv 0 \mod p$ *und*

3. p*, wenn* $f'(\xi) \equiv 0 \mod p$ *und* ξ *Lösung von* (3.2) *ist.*

Beweis. Sei α eine Lösung von (3.1) mit $0 \leq \alpha \leq p^n - 1$. Dann ist α auch Lösung von (3.2) und kann in der Form

$$\alpha = \xi + sp^{n-1} \tag{3.3}$$

mit $0 \leq s \leq p-1$ und $0 \leq \xi \leq p^{n-1} - 1$ geschrieben werden, wobei ξ eine Lösung von (3.2) ist.

Mittels Taylorentwicklung modulo p^n erhält man

$$\begin{aligned} f(\xi + sp^{n-1}) &= f(\xi) + sp^{n-1}f'(\xi) + \frac{1}{2}s^2p^{2(a-1)}f''(\xi) + \dots \\ &\equiv f(\xi) + sp^{n-1}f'(\xi) \mod p^n, \end{aligned} \tag{3.4}$$

da $k(a-1) \geq a$ für $k \geq 2$ und $\frac{1}{k!}f^{(k)}(\xi)$ ganzzahlig ist.

Sei $f'(\xi) \not\equiv 0 \mod p$. α ist genau dann Lösung von (3.1), wenn

$$f(\xi) + sp^{n-1}f'(\xi) \equiv 0 \mod p^n \tag{3.5}$$

beziehungsweise

$$sf'(\xi) \equiv -\frac{f(\xi)}{p^{n-1}} \mod p. \tag{3.6}$$

Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, gibt es genau ein s, welches diese Bedingung erfüllt, und somit ist die Anzahl der Lösungen von (3.2) dieselbe wie die Zahl der Lösungen von (3.1).

Sei nun $f'(\xi) \equiv 0 \mod p$. Dann ist

$$f(\xi + sp^{n-1}) \equiv f(\xi) \mod p^n. \tag{3.7}$$

Falls $f(\xi) \not\equiv 0 \mod p^n$, so ist (3.1) unlösbar. Anderenfalls, also wenn $f(\xi) \equiv 0 \mod p^n$, dann gibt es für jedes s in (3.3) eine Lösung. Somit p Lösungen von (3.1) für jede Lösung von (3.2). □

Wie in [7] können wir nun bestimmen, wann ein Polynom eine Polynompermutation modulo p^n ist.

Satz 3.2 (Charakterisierung von Polynompermutationen)**.** *Sei* $n \geq 2$ *und* $f \in \mathbb{Z}[X]$*. Dann sind folgende Aussagen äquivalent.*

(1) f_n *ist eine Polynompermutation auf* $\mathbb{Z}/p^n\mathbb{Z}$*.*

(2) f_1 *ist eine Polynompermutation auf* $\mathbb{Z}/p\mathbb{Z}$ *und* $\forall a \in \mathbb{Z} : f'(a) \not\equiv 0 \mod p$*.*

Beweis. Verwende dafür den vorherigen Satz 3.1.

(1) $\Longrightarrow$ (2). Dass f_1 Polynompermutation auf $\mathbb{Z}/p\mathbb{Z}$ ist klar, wegen Reduktion modulo p. Weil f_n eine Permutation ist, gibt es genau ein ξ, welches

$$f(\xi) \equiv 0 \mod p^n \tag{3.8}$$

löst. Mit vorherigem Satz folgt damit

$$f'(\xi) \not\equiv 0 \mod p. \tag{3.9}$$

(2) $\Longrightarrow$ (1). Mit dem vorherigen Satz und

$$\forall a \in \mathbb{Z} : f'(a) \not\equiv 0 \mod p \tag{3.10}$$

gibt es zu jedem

$$f(\xi) - c \equiv 0 \mod p^n \tag{3.11}$$

genausoviele Lösungen wie modulo p^{n-1}. Weil f_1 eine Permutation ist, gibt es genau eine Lösung modulo p und somit überall genau eine Lösung. □

Korollar. *Sei $n \geq 3$ und $f \in \mathbb{Z}[X]$. Dann ist f_n genau dann eine Permutation auf $\mathbb{Z}/p^n\mathbb{Z}$, wenn f_{n-1} eine Permutation auf $\mathbb{Z}/p^{n-1}\mathbb{Z}$ ist.*

Beweis. Folgt direkt aus dem Satz, da es nur von f und f' abhängt, ob f_n und f_{n-1} Permutationen sind. □

4 Die Anzahl von Polynomfunktionen und Polynompermutationen

In diesem Kapitel sei p eine beliebige, aber fixe Primzahl und $n \in \mathbb{N}$.

Die nachfolgenden Sätze und Beweise sind alle in [7] zu finden. Der erste Satz wird uns eine eindeutige Darstellung einer Polynomfunktion liefern, welche wir anschließend verwenden werden, um die Anzahl der Elemente abzuzählen.

Satz 4.1. *Sei $g \in \mathcal{F}_n$. Dann gibt es genau ein Polynom $f \in \mathbb{Z}[X]$ der Form*

$$f(X) = \sum_{i+\alpha_p(j)<n} a_{ij} p^i X^{\underline{j}}, \tag{4.1}$$

mit $i, j \geq 0$ und $0 \leq a_{ij} \leq p-1$, sodass $f_n = g$ gilt.

Beweis. Da für $\alpha_p(j) \geq n$ laut letzter Proposition in Kapitel 1 $X^{\underline{j}}$ modulo p^n verschwindet, gibt es ein Polynom

$$f(X) = \sum_{\alpha_p(j)<n} b_j X^{\underline{j}} \tag{4.2}$$

mit $f_n = g$. Da wir immer modulo einer Primzahlpotenz auswerten, können wir $b_j \geq 0$ voraussetzen. Mittels p-adischer Entwicklung der $b_j = \sum a_{ij} p^i$ mit $0 \leq a_{ij} \leq p-1$ ergibt sich die gewünschte Darstellung (4.1), da $p^i X^{\underline{j}} \equiv 0 \mod p^n$ für $i + \alpha_p(j) \geq n$.

Sei nun h ein weiteres Polynom mit $h_n = g$. Dann ist $(f-h)_n = 0$ und

$$f - h = \sum_{i+\alpha_p(j)<n} c_{ij} p^i X^{\underline{j}} \tag{4.3}$$

mit $|c_{ij}| < p$. Setze

$$d_j = \sum_{i=0}^{n-\alpha_p(j)-1} c_{ij} p^i. \tag{4.4}$$

Da $|c_{ij}| < p$ sind die $|d_j| < p^{n-\alpha_p(j)}$. Damit folgt, wenn $\left(d_j X^{\underline{j}}\right)_n = 0$, dass dann $d_j = 0$ für jedes j und somit $f = h$ gilt.

Führen wir also eine Induktion nach j durch. Für die Induktionsbasis ergibt sich

$$d_0 X^{\underline{0}} \equiv (f-h)(0) \equiv 0 \mod p^n. \tag{4.5}$$

Damit also weiter zum Induktionsschritt.

$$0 \equiv (f-h)(j) = d_j j! \mod p^n, \tag{4.6}$$

weil durch die Induktionsvoraussetzung $\left(d_t X^{\underline{t}}\right)_n = 0$ für $t < j$ und $X^{\underline{t}} \equiv 0 \mod p^n$ für $t > j$ laut der letzten Proposition in Kapitel 1. Aus (4.6) folgt damit das gewünschte Resultat. □

Definition. Sei $n \geq 2$. Definiere die *Projektion auf* $\mathcal{F}_{n-1}$ als Abbildung

$$\pi_n : \mathcal{F}_n \to \mathcal{F}_{n-1} \quad \text{mit} \quad f_n \longmapsto f_{n-1}. \tag{4.7}$$

Proposition. *Die Projektion π_n ist ein wohldefinierter Homomorphismus.*

Beweis. Seien $f, g \in \mathbb{Z}[X]$ mit $f_n = g_n$. Laut Satz 3.2 gilt damit $f_{n-1} = g_{n-1}$, $n \geq 2$ und somit $\pi_n(f_n) = \pi_n(g_n)$. Also ist π_n wohldefiniert.

Homomorphismus ist auch klar, da wir ja nur die Auswertung von modulo p^n auf modulo p^{n-1} reduzieren. □

Wir wollen nun den Kern genauer beschreiben. Für die Struktur dieses Kerns siehe Kapitel 6 bzw. [3, Satz 27] und [1].

Satz 4.2. *Jedes Element des Kerns von π_n kann eindeutig in der Form*

$$\sum_{i+\alpha_p(j)=n-1} a_{ij} p^i X^{\underline{j}} \tag{4.8}$$

mit $i, j \geq 0$ und $0 \leq a_{ij} \leq p-1$ geschrieben werden, und der Kern von π_n besteht aus $p^{\beta_p(n)}$ Elementen.

Beweis. Sei f aus dem Kern von π_n. Dann gilt

$$0 = \pi_n \left(\sum_{i+\alpha_p(j)<n} a_{ij} p^i X^{\underline{j}} \right) = \sum_{i+\alpha_p(j)<n-1} a_{ij} p^i X^{\underline{j}} \tag{4.9}$$

Aufgrund der eindeutigen Darstellung (Satz 4.1) folgt $a_{ij} = 0$ für $i + \alpha_p(j) < n - 1$.

Wählen wir nun w so, dass $\alpha_p(w) \leq n-1$ und $\alpha_p(w+1) \geq n$, dann gibt es für jedes j mit $0 \leq j \leq w$ genau eine Lösung von $i + \alpha_p(j) = n - 1$, für alle anderen j keine Lösung.

$\beta_p(n) = w + 1$, da ja $\beta_p(n)$ die kleineste natürliche Zahl t ist, für welche $p^n | t!$ gilt. Damit gibt es also $p^{\beta_p(n)}$ Elemente vom Kern von π_n. □

Mit der Kenntnis des Kerns können wir nun die Anzahl der Polynomfunktionen und anschließend dann die der Polynompermutationen bestimmen.

Korollar. *Für $n \geq 2$ gilt*

$$|\mathcal{F}_n| = p^{\beta_p(n)} \, |\mathcal{F}_{n-1}| \, . \tag{4.10}$$

Beweis. Die Aussage folgt direkt aus dem Satz, da $|\mathcal{F}_n|$ das Produkt aus Kardinalität des Kerns von π_n und der Kardinalität des Bildes von π_n ist. □

Korollar (Anzahl der Polynomfunktionen)**.** *Es gilt*

$$|\mathcal{F}_n| = p^{\sum_{k=1}^{n} \beta_p(k)}. \tag{4.11}$$

Beweis. $|\mathcal{F}_n| = p^p$ folgt direkt aus der eindeutigen Darstellung in Satz 4.1 und $\beta_p(1) = p$. Mit dem vorherigen Korollar und einer Induktion folgt der Rest. □

Korollar. *Für $n \geq 3$ gilt*

$$|\mathcal{P}_n| = |\mathcal{P}_2| \, p^{\sum_{k=3}^{n} \beta_p(k)}. \tag{4.12}$$

Beweis. Aus dem Satz und aus dem Korollar zu Satz 3.2 folgt, dass jedes Element von $\mathcal{P}_{n-1}$ genau $p^{\beta_p(n)}$ Urbilder in $\mathcal{P}_n$ hat. Eine Induktion erledigt wieder den Rest. □

Jetzt bleibt nur noch offen, wieviele Elemente in $\mathcal{P}_2$ vorhanden sind. Darüber gibt das folgende Lemma Aufschluss.

Lemma. *Es gilt*

$$|\mathcal{P}_2| = p!(p-1)^p p^p. \tag{4.13}$$

Beweis. Sei $f(X)$ aus $\mathcal{P}_2$. Laut Satz 4.1 kann dieses f eindeutig mit $0 \leq a_{ij} \leq p-1$ als

$$f(X) = \sum_{i+\alpha_p(j)<2} a_{ij} p^i X^{\underline{j}} = g(X) + h(X) + pk(X) \tag{4.14}$$

dargestellt werden. Für die Aufgespaltung verwenden wir

$$g(X) = \sum_{j=0}^{p-1} a_{0j} X^{\underline{j}}, \qquad h(X) = \sum_{j=p}^{2p-1} a_{0j} X^{\underline{j}}, \qquad k(X) = \sum_{j=0}^{p-1} a_{1j} X^{\underline{j}} \tag{4.15}$$

Laut Satz 3.2 ist f_2 genau dann eine Polynompermutation modulo p^2, wenn f_1 eine Permutation auf $\mathbb{Z}/p\mathbb{Z}$ ist und $f'(a) \not\equiv 0 \mod p$ für beliebiges $a \in \mathbb{Z}$ gilt.

Klarerweise gilt $f_1 = g_1$. Da jede Permutation modulo p auch vorkommt, gibt es für $g(X)$ keine Einschränkungen, und somit $p!$ Wahlmöglichkeiten.

Es gilt

$$f'(X) = g'(X) + h'(X) + pk'(X) \equiv g'(X) + h'(X) \mod p \tag{4.16}$$

und

$$h(X) = X^{\underline{p}} \sum_{j=0}^{p-1} a_{0,j+p} (X-p)^{\underline{j}}. \tag{4.17}$$

Für die Ableitung von $h(X)$ ergibt sich

$$\begin{aligned} h'(X) &= (X^{\underline{p}})' \sum_{j=0}^{p-1} a_{0,j+p} (X-p)^{\underline{j}} + X^{\underline{p}} \left(\sum_{j=0}^{p-1} a_{0,j+p} (X-p)^{\underline{j}} \right)' \\ &\equiv (X^{\underline{p}})' \sum_{j=0}^{p-1} a_{0,j+p} (X)^{\underline{j}} \equiv - \sum_{j=0}^{p-1} a_{0,j+p} (X)^{\underline{j}} \mod p, \end{aligned} \tag{4.18}$$

da aus dem *Satz von Wilson* $(X^{\underline{p}})' \equiv -1 \mod p$ folgt. Damit $h'(X)$ eine vorgegebenen Funktion modulo p ist, gibt es also genau eine Möglichkeit $h(X)$ zuwählen. Damit gibt es also zu jedem $g(X)$ genau $(p-1)^p$ Möglichkeiten $h(X)$ so zu wählen, dass die Ableitung von $f(X)$ modulo p nicht verschwindet.

Die Koeffizienten von $k(X)$ können beliebig gewählt werden, also gibt es p^p Möglichkeiten, damit ist $|\mathcal{P}_2| = p!(p-1)^p p^p$ gezeigt. □

Zusammenfassend ergibt sich nun der folgende Satz.

Satz 4.3 (Anzahl der Polynompermutationen)**.** *Es gilt*

$$|\mathcal{P}_1| = p!, |\mathcal{P}_2| = p!(p-1)^p p^p, \tag{4.19}$$

und für $n \geq 3$ gilt

$$|\mathcal{P}_n| = p!(p-1)^p p^p p^{\sum_{k=3}^{n} \beta_p(k)}. \tag{4.20}$$

Korollar. *Für $n \geq 2$ gilt*

$$\frac{|\mathcal{P}_n|}{|\mathcal{F}_n|} = \frac{p!(p-1)^p}{p^{3p}}. \tag{4.21}$$

5 Kranzprodukte

Definition (Kranzprodukt)**.** Sei M ein Monoid und H ein Monoid der auf eine Menge S wirkt. Dann ist das *Kranzprodukt* (englisch. *wreath product*) $M \wr H$ definiert als der Monoid auf $H \times M^S$ mit der Verknüpfung

$$(h, (m_s)_{s\in S}) \cdot (g, (l_s)_{s\in S}) := \left(h \circ g, (m_{g(s)} l_s)_{s\in S}\right). \tag{5.1}$$

Wirkt M auf eine Menge T, dann wird die *Wirkung* von $M \wr H$ auf $S \times T$ mit

$$(h, (m_s)_{s\in S})\,(x, y) := (h(x), m_x(y)) \tag{5.2}$$

definiert.

Die so definierte Multiplikation ist assoziativ und das neutrale Element dieses Monoids ist

$$\mathrm{id}_{M\wr H} = (\mathrm{id}_H, (\mathrm{id}_M)_{s\in S}). \tag{5.3}$$

Für die Anzahl der Elemente gilt

$$|M \wr H| = |M|^{|S|}\,|H|. \tag{5.4}$$

Ist $M = G$ eine Gruppe und $H = P$ eine Permutationsgruppe auf einer endlichen Ziffernmenge S, so bildet $G \wr P$ eine Gruppe, und für das inverse Element gilt

$$(\sigma, (g_s)_{s\in S})^{-1} = \left(\sigma^{-1}, (g^{-1}_{\sigma(s)})_{s\in S}\right). \tag{5.5}$$

Diese und weitere Eigenschaften des Kranzprodukts können zum Beispiel in [6] nachgelesen werden.

6 Die Struktur der Polynomfunktionshalbgruppe

In diesem Kapitel sei p wieder eine beliebige, aber fixe Primzahl und $n \in \mathbb{N}$. Wie in Kapitel 2 definiert, sei φ_n die Abbildung von $\mathbb{Z}[X]$ nach $\mathcal{F}_n$, wobei $\mathcal{F}_n$ wieder die Menge der Funktionen von $\mathbb{Z}/p^n\mathbb{Z}$ in sich selbst ist, welche als Polynome dargestellt werden können.

Wir werden nun die Struktur des Kerns von φ_n beschreiben. Der nachfolgende Satz ist in [3, Satz 27] zu finden

Satz 6.1. *Sei $n \le p$ und $f \in \mathbb{Z}[X]$ mit $f(X) \equiv 0 \mod p^n$. Dann ist f von der Form*

$$\sum_{k=0}^{n} p^{n-k} \left(X^p - X\right)^k f_k(X), \tag{6.1}$$

wobei $f_0, \ldots, f_n \in \mathbb{Z}[X]$

Bemerkung. Anders ausgedrück besagt der Satz, dass für $n \leq p$

$$\ker \varphi_n = (X^p - X, p)^n \tag{6.2}$$

gilt.

Beweis. Für $n = 1$ folgt aus $f(X) \equiv 0 \mod p$, dass f von der Gestalt

$$X(X-1)\dots(X-p+1)f_1(X) + pf_0(X) \tag{6.3}$$

ist. Da $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ein endlicher Körper ist, gilt

$$X^p - X \equiv \prod_{\alpha \in \mathbb{F}_p} (X - \alpha) \equiv 0 \mod p, \tag{6.4}$$

und somit gilt

$$pf_0(X) + (X^p - X)f_1(X) \equiv 0 \mod p. \tag{6.5}$$

Für den Induktionsschritt von n auf $n+1 \leq p$ sei

$$f(X) \equiv 0 \mod p^{n+1}. \tag{6.6}$$

Da diese Relation auch modulo p^n gilt, ist f von der Form (6.1). Nach Fermat gibt es ein $y \in \mathbb{Z}$, sodass $X^p - X = py$. Setze $Z = y - z$. Mittels binomischem Lehrsatz ergibt sich

$$(X + pz)^p \equiv X^p = X + pz + pZ \mod p^2, \tag{6.7}$$

also

$$((X + pz)^p - (X + pz))^k = (pZ + tp^2)^k \equiv p^k Z^k \mod p^{n+1}. \tag{6.8}$$

Damit

$$0 \equiv f(X + pz) \equiv \sum_{k=0}^{n} p^{n-k} p^k Z^k f_k(X + pz) \mod p^{n+1}, \tag{6.9}$$

und daher gilt für beliebiges $Z \in \mathbb{Z}$

$$\sum_{k=k}^{n} f_k(X) Z^k \equiv 0 \mod p. \tag{6.10}$$

Der Grad in Z dieser Kongruenz ist $\leq n < p$, und daher gibt es p Lösungen. Analog wie in der Induktionsbasis muss damit jedes $f_k(X)$ die Form

$$pu(X) + (X^p - X)v(X) \tag{6.11}$$

haben, was eingesetzt in (6.1) modulo p^{n+1} unsere Induktion vervollständigt. □

Die nachfolgende Beschreibung des Kerns von φ_n für allgemeine n, ist aus [1]. Dort findet sich auch eine Darstellung des Kerns als $\mathbb{Z}$-Modul und die zugehörigen Beweise für diese Aussagen.

Satz 6.2 (Bandini)**.** *Sei*

$$H_2(X) := (X^p - X)^p - p^{p-1}(X^p - X) \tag{6.12}$$

Polynom in $\mathbb{Z}[X]$ *und*

$$I := (X^p - X, p) \tag{6.13}$$

Ideal in $\mathbb{Z}[X]$*.*

1. *Es gilt*

$$\ker \varphi_{p+1} = \left(I^{p+1}, H_2\right) \tag{6.14}$$

2. *Für* $n \in \mathbb{N}$ *gilt*

$$\ker \varphi_n \subseteq (I^n, H_2)\,. \tag{6.15}$$

Ohne Beweis. □

Literatur

[1] Bandini, A. Functions $f : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ induced by polynomials of $\mathbb{Z}[X]$. *Annali di Matematica 181*, 4 (2002), 95–104.

[2] Carlitz, L. Functions and polynomials mod p^n. *Acta Arithmetica IX* (1964), 67–78.

[3] Dickson, L. E. *Einführung in die Zahlentheorie.* B. G. Teubner, 1931.

[4] Graham, R. L., Knuth, D. E., and Patashnik, O. *Concrete Mathematics*, second edition ed. Addison-Wesley, 2005.

[5] Hardy, G. H., and Wright, E. M. *An Introduction to the theory of numbers*, fifth ed. Clarendon Press Oxford, 1984.

[6] Huppert, B. *Endliche Gruppen I*, vol. 134 of *Die Grundlagen der mathematischen Wissenschaften in Einzeldarstellung.* Springer-Verlag, 1967.

[7] Keller, G., and Olson, F. R. Counting polynomial functions mod p^n. *Duke J. Math 35* (1968), 835–838.

[8] McDonald, B. R. *Finite Rings with Identity.* Marcel Dekker, Inc., 1974.