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

Teil II – Bakkalaureatsprojekt

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

7 Die Sylowgruppen der Polynompermutationsgruppe

In diesem Kaptiel sei p eine Primzahl und für ein $n \in \mathbb{N}$ sei $\mathcal{P}_n$ die zugehörige Gruppe der Polynompermutationen modulo p^n.

Wie in Kaptiel 4 definiert, sei π_n die Projektion von $\mathcal{P}_n$ auf $\mathcal{P}_{n-1}$. Wir verallgemeinern nun dies. Setze $\pi_{n,n-1} := \pi_n$ und für $n > m$

$$\pi_{n,m} := \pi_{n,n-1} \circ \pi_{n-1,n-2} \circ \cdots \circ \pi_{m+1,m}. \tag{7.1}$$

Klarerweise ist diese Abbildung ein Homomorphismus, da π_n einer ist.

Proposition. *Für ein beliebiges $n \in \mathbb{N}$ sei A die Menge der Elemente aus $\mathcal{P}_n$ mit Ableitung modulo p konstant 1 und Z die Menge der Elemente aus $\mathcal{P}_n$, welche als Urbild von $\pi_{n,1}$ einer fixen zyklischen Gruppe der Ordnung p in $\mathcal{P}_1 = \mathcal{S}_p$ auftreten. Dann ist $A \cap Z$ eine p-Sylowgruppe von $\mathcal{P}_n$.*

Beweis. A ist eine Untergruppe von $\mathcal{P}_n$, da für $\alpha, \beta \in A$

$$(\alpha \circ \beta)' = (\alpha(\beta(X)))' = \alpha'(\beta(X)) \cdot \beta'(X) \equiv 1 \cdot 1 \equiv 1 \mod p \tag{7.2}$$

gilt, und für ein $\gamma \in A$ auch $\gamma^{-1} \in A$ ist, da

$$1 = X' = (\mathrm{id})' = \left(\gamma \circ \gamma^{-1}\right)' = \gamma'\left(\gamma^{-1}(X)\right) \cdot \left(\gamma^{-1}\right)'(X) \equiv 1 \cdot \left(\gamma^{-1}\right)'(X) \mod p. \tag{7.3}$$

Z ist ebenfalls eine Untergruppe von $\mathcal{P}_n$, da für $\sigma, \tau \in Z$

$$\pi_{n,1}\left(\sigma \circ \tau^{-1}\right) = \pi_{n,1}(\sigma) \circ (\pi_{n,1}(\tau))^{-1} \in \pi_{n,1}(Z). \tag{7.4}$$

Damit ist auch $A \cap Z$ eine Untergruppe von $\mathcal{P}_n$.

Jedes Element $f \in \mathcal{P}_n$ kann laut [7, Theorem 1] in der Form

$$f(X) = \sum_{i+\alpha_p(j)<n} a_{ij} p^i X^{\underline{j}} \tag{7.5}$$

mit $0 \le i, j$ und $0 \le a_{ij} \le p-1$ dargestellt werden. Dies kann nun weiter in

$$f(X) = g(X) + h(X) + pk(X) \tag{7.6}$$

aufgespalten werden, wobei

$$g(X) = \sum_{j=0}^{p-1} a_{0j} X^{\underline{j}}, \qquad h(X) = \sum_{j=p}^{\alpha_p(j)-1} a_{0j} X^{\underline{j}} \tag{7.7}$$

und $k(X)$ der „Rest“ ist.

Modulo p beleibt von dieser Aufspaltung nur $f(X) \equiv g(X) \mod p$ übrig, es gibt also genau die p Möglichkeiten der zyklischen Gruppe modulo p.

Für vorgegebenes $g(X)$ bestimmt $h(X)$ die Ableitung modulo p, siehe [7]. Es gibt also genau eine Möglichkeit die Koeffizienten von $h(X)$ zu bestimmten, dass die Ableitung modulo p konstant 1 ist.

Damit sind die Elemente genau so bestimmt, wie sie für die Sylowgruppe erforderlich sind, vom Polynom $k(X)$ kommen die restlichen p-Potenzen, welche noch für die p-Sylowgruppe erforderlich sind, siehe ebenfalls wieder [7]. □

Bemerkung. Sei S die p-Sylowgruppe, welche Ableitung modulo p konstant 1 hat und als Funktion modulo p in der zyklischen Untergruppe erzeugt von $(0\,1\,2\,3\,\ldots\,p-1)$ liegt, dann kann jedes $f \in S$ durch

$$f(X) = X + c + pk(X) \tag{7.8}$$

mit passendem $k(X)$ dargestellt werden. Dabei ist f modulo p der Zykel $(0\,1\,2\,3\,\ldots\,p-1)^c$.

Lemma. *Sei $n = 2$ und S die p-Sylowgruppe in $\mathcal{P}_2$, welche modulo p Ableitung konstant 1 und als Funktion modulo p in der zyklischen Untergruppe erzeugt von $(0\,1\,2\,3\,\ldots\,p-1)$ liegt. Dann ist die Kardinalität des Normalisators von S gleich $p^{p+1}(p-1)^2$.*

Beweis. Der Zykel $(0\,1\,2\,3\,\ldots\,p-1)$ entspricht dem Polynom $f = X + 1$, die zugehörige zyklische Untergruppe besteht somit aus allen $X + c$ mit $0 \leq c \leq p-1$.

Wir suchen nun jene Elemente h, für welche $h \circ f \circ h^{-1}$ wieder in S liegt. Da die Ableitung von f konstant 1 modulo p ist, gilt

$$\left(h \circ f \circ h^{-1}\right)' \equiv h'\left(h^{-1}(X) + 1\right) \cdot \left(h^{-1}\right)'(X) \stackrel{!}{\equiv} 1 \mod p. \tag{7.9}$$

Sei $h = aX + c$, dann ist $h^{-1} = bX + d$ mit $b \equiv a^{-1}$ und $d \equiv -a^{-1}c$ jeweils modulo p, denn

$$(aX + c) \circ (bX + d) = abX + ad + c \equiv X \mod p. \tag{7.10}$$

Alle Einheiten vom Polynomring ${}^{\mathbb{Z}}/_{p\mathbb{Z}}[X]$, welche die konstanten Polynome ungleich 0 sind, erfüllen also Gleichung (7.9), da

$$h'(X) \equiv a \mod p \qquad \text{und} \qquad \left(h^{-1}\right)'(X) \equiv a^{-1} \mod p. \tag{7.11}$$

Somit gibt es für die Wahl der Ableitung modulo p genau diese $p-1$ Möglichkeiten.

Jetzt müssen wir noch die Anzahl der möglichen Konjugationen von $(0\,1\,2\,3\,\ldots\,p-1)$ bestimmen, damit wir wieder eine Potenz von diesem Zykel $(0\,1\,2\,3\,\ldots\,p-1)^k, 1 \leq k \leq p-1$ bekommen. Es gibt genau $p-1$ Möglichkeiten, da wir auf $p-1$ verschiedene Zykel abbilden können, und weiters kann ohne Beschränkung der Allgemeinheit 0 auf jedes Element in diesem p-Zykel abgebildet werden, also p Möglichkeiten. Da modulo p alle Permutationen vorkommen, gibt es diese Konjugationen auch, und das sind auch alle.

Laut [7, p. 837, Lemma] gibt es zu jeder vorgegebenen Funktion modulo p und vorgegebener Ableitung modulo p genau p^p Elemente aus $\mathcal{P}_2$, welche diese Funktion und Ableitung modulo p erfüllen.

Insgesamt ergibt sich somit für die Kardinalität des Normalisators $(p-1)^2 p p^p$. □

Satz 7.1 (Anzahl der p-Sylowgruppen)**.** *Die Anzahl der p-Sylowgruppen ist $(p-2)!$ falls $n = 1$ und $(p-2)!(p-1)^{p-1}$ falls $n \geq 2$.*

Beweis. Falls $n = 1$ ist, so ist die Kardinalität einer p-Sylowgruppe p. Die einzigen Elemente, von welchen die Ordnung p teilt, sind die p-Zyklen und natürlich die Identität. Von den p-Zyklen gibt es $(p-1)!$ Stück, da modulo p alle Permutationen vorkommen

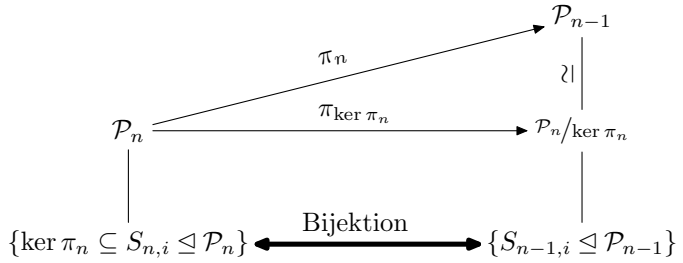

Abbildung 7.1: Anzahl der p-Sylowgruppen für $n \geq 3$

und ich $p-1$ Elemente in einem p-Zyklus beliebig anordnen kann (ein Element kann fix an einer Stelle bleiben). Da nun aber in jeder Gruppe der Ordnung p genau $p-1$ p-Zyklen drinnen sind, können diese auf $(p-2)!$ Untergruppen der Ordnung p aufgeteilt werden.

Falls $n = 2$ ist, so wissen wir aufgrund des vorherigen Lemmas, dass der Normalisator N einer Sylowgruppe $p^{p+1}(p-1)^2$ Elemente umfasst. Da der Index dieses Normalisators der p-Sylowgruppe gleich der Anzahl der p-Sylowgruppen ist (siehe [6, Kapitel I, Satz 7.5b]), ergibt sich dafür

$$[\mathcal{P}_2 : N] = \frac{p!(p-1)^p p^p}{(p-1)^2 p^{p+1}} = (p-2)!(p-1)^{p-1}. \tag{7.12}$$

Für $n \geq 3$ ändert sich die Anzahl der p-Sylowgruppen nicht mehr. Denn für $n \geq 3$ ist der Kern K_n der Projektion von $\mathcal{P}_n$ auf $\mathcal{P}_{n-1}$ eine p-Gruppe (siehe [7, Theorem 2]) und ja sowieso ein Normalteiler. Somit ist dieser in jeder p-Sylowgruppe von $\mathcal{P}_n$ drinnen.

Aufgrund des Transfersatzes werden nun die Untergruppen von $\mathcal{P}_n$, welche K_n enthalten bijektiv auf die Untergruppen von $\mathcal{P}_{n-1} \simeq {}^{\mathcal{P}_n}\!/_{K_n}$ abgebildet und, da der Kern für $n \geq 3$ eine p-Gruppe ist, auch die p-Sylowgruppen, siehe auch Abbildung 7.1. □

8 Die Struktur der Polynompermutationsgruppe

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

8.1 Die Einbettung der Polynompermutationsgruppe in $\mathcal{S}_p \wr \cdots \wr \mathcal{S}_p$

Notation. Sei $\sum_{k\geq 0} a_k X^k \in \mathbb{Z}[X]$. Definiere

$$[X^m] \sum_{k\geq 0} a_k X^k := a_m. \tag{8.1}$$

Sei $\alpha \in \mathbb{Z}$. Dann gibt es $a_0, \ldots, a_L$, $0 \leq a_k \leq p-1$ sodass $\alpha = \pm \sum a_k p^k$. Definiere

$$[p^m](\alpha) := a_m. \tag{8.2}$$

Falls $\alpha \in {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}$ gilt alles analog, mit $L = n-1$.

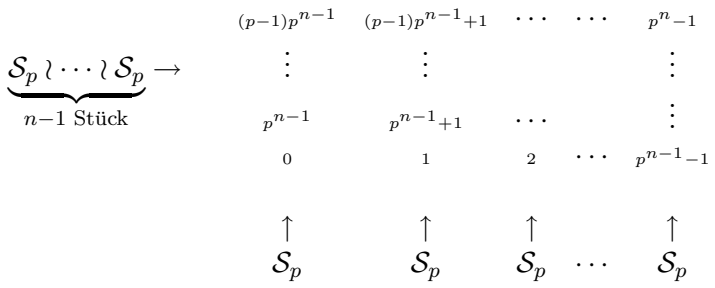

Abbildung 8.1: Einbettung von $\mathcal{P}_n \subseteq \mathcal{S}_p \wr \cdots \wr \mathcal{S}_p$

Satz 8.1 (Einbettung der Polynompermutationsgruppe)**.** *Sei $n \in \mathbb{N}$. Dann gilt*

$$\mathcal{P}_n \subseteq \underbrace{\mathcal{S}_p \wr \cdots \wr \mathcal{S}_p}_{n \text{ Stück}}, \tag{8.3}$$

d.h. die Gruppe der Polynompermutationen kann in ein Kranzprodukt aus symmetrischen Gruppen $\mathcal{S}_p$ eingebettet werden.

Bemerkung. Die Idee hinter dieser Einbettung ist wie folgt. Wenn ich von $\mathcal{P}_{n-1}$ auf $\mathcal{P}_n$ gehe, betrachte ich das Kranzprodukt aus den symmetrischen Gruppen $\mathcal{S}_p \wr (\mathcal{S}_p \wr \cdots \wr \mathcal{S}_p)$. Die $n-1$ Faktoren können als Polynompermutation modulo p^{n-1} aufgefasst werden, also das was bei der Projektion einer Polynompermutation modulo p^n auf $\mathcal{P}_{n-1}$ übrig bleibt. Jede „Stelle“ dieser Permutation wird nun modulo p^n wieder permutiert, also der Koeffizient von p^{n-1} in einer p-adischen Darstellung gewählt. Diesen Teil übernimmt das verbleibende $\mathcal{S}_p$, siehe Abbildung 8.1.

Beweis. Wir definieren rekursiv eine Familie von Abbildung $\{\iota_n\}_{n\in\mathbb{N}}$,

$$\iota_n : \mathcal{P}_n \longrightarrow \underbrace{\mathcal{S}_p \wr \cdots \wr \mathcal{S}_p}_{n \text{ Stück}} \tag{8.4}$$

mit

$$\iota_1 := \mathrm{id}_{\mathcal{S}_p} \tag{8.5}$$

und

$$\iota_n(f_n) := \Big(\iota_{n-1}(f_{n-1}), (\psi_{n,j})_{j\in\mathbb{Z}/p^{n-1}\mathbb{Z}}\Big) \quad \text{für } n \geq 2, \tag{8.6}$$

mit $\psi_{n,j} \in \mathcal{S}_p$, wobei

$$\psi_{n,j}(k) = \left[p^{n-1}\right] f_n(kp^{n-1} + j) \quad \text{für } k \in \{0, 1, \ldots, p-1\}. \tag{8.7}$$

Um zu zeigen, dass diese Abbildung das macht was sie soll, starten wir eine Induktion nach n. Für $n = 1$ ist nichts zu zeigen, denn laut Kapitel 3 ist $\mathcal{P}_1 = \mathcal{S}_p$, und somit erfüllt ι_1 trivialerweise alle Eigenschaften.

Damit weiter zum Induktionsschritt.

1. ι_n ist eine wohldefinierte Abbildung.

   Seien $f, g \in \mathbb{Z}[X]$ mit $f_n = g_n$. Aus Satz 3.2 folgt $f_{n-1} = g_{n-1}$ und damit $\iota_{n-1}(f_{n-1}) = \iota_{n-1}(g_{n-1})$ laut Induktionsvoraussetzung.

   Seien $\widehat{\psi}_{n,j}$ die zu f gehörenden Abbildungen und $\tilde{\psi}_{n,j}$ die zu g gehörenden. Weil $f_n = g_n$ gilt $f_n(a) \equiv g_n(a) \mod p^n$ für alle $a \in \mathbb{Z}/p^n\mathbb{Z}$, damit auch speziell für $a = kp^{n-1} + j$. Die Koeffizienten von p^{n-1} befinden sich somit in der gleichen Äquivalenzklasse modulo p und damit gilt die Gleichheit von $\widehat{\psi}_{n,j} = \tilde{\psi}_{n,j}$.

2. ι_n ist ein Homomorphismus.

   Seien $f, g \in \mathbb{Z}[X]$.

$$\begin{aligned}
\iota_n(f_n) \cdot \iota_n(g_n) &= \left(\iota_{n-1}(f_{n-1}), (\widehat{\psi}_{n,j})_{j\in\mathbb{Z}/p^{n-1}\mathbb{Z}}\right) \cdot \left(\iota_{n-1}(g_{n-1}), (\tilde{\psi}_{n,j})_{j\in\mathbb{Z}/p^{n-1}\mathbb{Z}}\right) \\
&= \left(\iota_{n-1}(f_{n-1}) \cdot \iota_{n-1}(g_{n-1}), (\widehat{\psi}_{n,\iota_n(g_{n-1}(j))} \circ \tilde{\psi}_{n,j})_{j\in\mathbb{Z}/p^n\mathbb{Z}}\right) \\
&= \left(\iota_{n-1}(f_{n-1} \circ g_{n-1}), \psi_{n,j})_{j\in\mathbb{Z}/p^n\mathbb{Z}}\right) \\
&= \iota_n(f_n \circ g_n),
\end{aligned} \tag{8.8}$$

   weil $\iota_{n-1}(f_{n-1}) \cdot \iota_{n-1}(g_{n-1}) = \iota_{n-1}(f_{n-1} \circ g_{n-1})$ laut Induktionsvoraussetzung und

$$\begin{aligned}
\widehat{\psi}_{n,\iota_n(g_{n-1}(j))} \circ \tilde{\psi}_{n,j}(k) &= \left[p^{n-1}\right] f_n(kp^{n-1} + g_{n-1}(j)) \circ \left[p^{n-1}\right] g_n(kp^{n-1} + j) \\
&= \left[p^{n-1}\right] f_n\left(\left(\left[p^{n-1}\right] g_n(kp^{n-1} + j)\right) p^{n-1} + g_{n-1}(j)\right)\right) \\
&\overset{(*)}{=} \left[p^{n-1}\right] f_n\left(g_n(kp^{n-1} + j)\right) \\
&= \left[p^{n-1}\right] (f_n \circ g_n)(kp^{n-1} + j) \\
&= \psi_{n,j}(k).
\end{aligned} \tag{8.9}$$

   Die Gleichheit bei $(*)$ gilt wegen der eindeutigen Darstellung

$$g_n(a) = \left([p^{n-1}]g_n(a)\right) p^{n-1} + g_{n-1}(a) \tag{8.10}$$

   von ganzen Zahlen als Potenzen von p und wegen Satz 3.2.

3. ι_n ist injektiv.

   Seien $f, g \in \mathbb{Z}[X]$ und sei $\iota_n(f_n) = \iota_n(g_n)$. Damit (einsetzen in die Definition) gilt $\iota_{n-1}(f_{n-1}) = \iota_{n-1}(g_{n-1})$ und somit, mittels Induktionsvoraussetzung $f_{n-1} = g_{n-1}$. Weiters gilt $\widehat{\psi}_{n,j} = \tilde{\psi}_{n,j}$. Damit sind die Koeffizienten von p^{n-1} bei f_n und g_n gleich, wodurch sich die Gleichheit $f_n = g_n$ ergibt.

□

8.2 Die Struktur der p-Sylowgruppen

Für den Binomialkoffizienten werden wir im Folgenden die Konvention $\binom{n}{k} = 0$, falls $k < 0$ ist, verwenden. Weiters gilt $\binom{n}{k} = 0$ für $n < k$, das folgt direkt aus der Definition.

Lemma. *Sei p eine Primzahl. Für die $p \times p$-Matrix*

$$T_p \equiv \left(i^{\underline{j}}\right)_{0 \le i,j \le p-1} \mod p \tag{8.11}$$

gilt

$$T_p^{-1} \equiv \left([i \ge j]\,(-1)^{i+j+1} \binom{p-1}{i-j} (p-1-i+j)^{\underline{p-1-i}} \right)_{0 \le i,j \le p-1} \mod p. \tag{8.12}$$

Beweis. Da $i^{\underline{j}} = 0$ für $j > i$, ist T_p eine untere Dreiecksmatrix, somit ist dies auch die inverse Matrix. Wir betrachten nun die ein einzelenen Einträge von $(a_{ij})_{0 \le i,j \le p-1} = T_p \cdot T_p^{-1}$. Für $i = j$ gilt

$$\begin{aligned} a_{ii} &\equiv \sum_{k=i}^{i} k^{\underline{k}} (-1)^{2k+1} \binom{p-1}{0} (p-1)^{\underline{p-1-k}} \\ &\equiv -i^{\underline{i}} (p-1)^{\underline{p-1-i}} = -(p-1)^{\underline{p-1}} \equiv 1 \mod p. \end{aligned} \tag{8.13}$$

Für $i > j$ gilt

$$\begin{aligned} a_{ij} &\equiv \sum_{k=j}^{i} i^{\underline{k}} (-1)^{k+j+1} \binom{p-1}{k-j} (p-1-k+j)^{\underline{p-1-k}} \\ &\overset{l=k-j}{=} \sum_{l=0}^{i-j} i^{\underline{l+j}} (-1)^{l+2j+1} \binom{p-1}{l} (p-1-l)^{\underline{p-1-j-l}} \\ &= -i^{\underline{j}} \sum_{l=0}^{i-j} (i-j)^{\underline{l}} (-1)^{l} \frac{(p-1)^{\underline{p-1-j}}}{l!} \\ &= -i^{\underline{j}} (p-1)^{\underline{p-1-j}} \sum_{l=0}^{i-j} \binom{i-j}{l} (-1)^{l} \\ &= -i^{\underline{j}} (p-1)^{\underline{p-1-j}} \cdot 0^{i-j} = 0 \mod p. \end{aligned} \tag{8.14}$$

Somit ist $(a_{ij})_{0 \le i,j \le p-1}$ die Einheitsmatrix modulo p. □

Lemma. *Sei p eine Primzahl und*

$$f(i,k) = (-1)^{i+k+1} [k \le i] \binom{p-1}{i-k} (p-1-i+k)^{\underline{p-1-i}}. \tag{8.15}$$

Dann gilt

$$\sum_{0 \le i,k \le p-1} X^{\underline{i}} f(i,k) y_{k+d} \equiv \sum_{0 \le i,k \le p-1} (X+d)^{\underline{i}} f(i,k) y_k \mod p \tag{8.16}$$

für beliebige $y_j \in \mathbb{Z}/p\mathbb{Z}$, mit $y_{j+p} = y_j$.

Beweis. Mit

$$(X+d)^{\underline{i}} = \sum_{0\le j} [j \le i] \binom{i}{j} X^{\underline{j}} d^{\underline{i-j}} \tag{8.17}$$

und anschließendem Koeffizientenvergleich in $X^{\underline{m}} y_n$ bleibt zu zeigen, dass $\forall d, m, n$

$$f(m, n-d) \equiv \sum_{0\le i\le p-1} f(i,n)\,[m \le i] \binom{i}{m} d^{\underline{i-m}} \mod p \tag{8.18}$$

gilt.

Wir machen nun eine Induktion nach d. Für $d = 0$ gilt

$$f(m,n) \equiv \sum_{0\le i\le p-1} f(i,n)\,[m \le i] \binom{i}{m} \underbrace{0^{\underline{i-m}}}_{[i=m]} \equiv f(m,n)\,[m=m] \binom{m}{m} \mod p \tag{8.19}$$

Vor unserem Induktionsschritt werden wir noch die folgenden Umformungen von Gleichung (8.15) und (8.18) durchführen.

$$f(i,k) = (-1)^{i+k+1}\,[k \le i]\,\frac{(p-1)^{\underline{p-1-k+1}}}{(i-k)!} \tag{8.20}$$

Dies setzen wir nun in (8.18) ein, kürzen gemeinsame Faktoren raus, schreiben die Binomialkoeffizienten mit fallenden Faktoriellen an und machen das Ganze nennerfrei.

$$\begin{aligned}(-1)^{m+n-d+1}\,[n-d \le m]\,\frac{(p-1)^{\underline{p-1-n+d+1}}}{(m-n+d)!} \equiv \\ \equiv \sum_{0\le i\le p-1} (-1)^{i+n+1}\,[n \le i]\,\frac{(p-1)^{\underline{p-1-n+1}}}{(i-n)!}\,[m \le i] \binom{i}{m} d^{\underline{i-m}} \mod p\end{aligned} \tag{8.21a}$$

$$\begin{aligned}(-1)^{m-d}\,[n-d \le m]\,\frac{(n-1)^{\underline{d}}}{(m-n+d)!} \equiv \\ \equiv \sum_{0\le i\le p-1} (-1)^{i}\,[n \le i]\,\frac{1}{(i-n)!}\,[m \le i]\,\frac{i^{\underline{m}}}{m!} d^{\underline{i-m}} \mod p\end{aligned} \tag{8.21b}$$

$$\begin{aligned}(-1)^{m-d}\,[n-d \le m]\,\underbrace{(p-1)^{\underline{p-1}}}_{\equiv -1 \mod p} m^{\underline{n-d}} (n-1)^{\underline{d}} \equiv \\ \equiv \sum_{0\le i\le p-1} \underbrace{(-1)^{i}\,[n \le i]\,(p-1)^{\underline{p-1+n-i}}}_{=:A(n,i)}\,[m \le i]\,i^{\underline{m}} d^{\underline{i-m}} \mod p\end{aligned} \tag{8.21c}$$

Und nun geht es endlich an den Induktionsschritt $d \to d+1$.

$$\begin{aligned}
&\sum_{0\le i\le p-1} A(n,i)\,[m\le i]\,i^{\underline{m}}d+1^{\underline{i-m}} = \\
&\qquad = \sum_{0\le i\le p-1} A(n,i)\,[m\le i]\,i^{\underline{m}}\left(d^{\underline{i-m}} + (i-m)d^{\underline{i-m-1}}\right) \\
&\qquad = \sum_{0\le i\le p-1} A(n,i)\,[m\le i]\,i^{\underline{m}}d^{\underline{i-m}} \\
&\qquad\quad + \sum_{0\le i\le p-1} A(n,i)\underbrace{[m\le i]\,i^{\underline{m+1}}}_{=[m+1\le i]i^{\underline{m+1}}}d^{\underline{i-(m+1)}} \\
&\qquad \equiv (-1)^{m-d+1}\,[n-d\le m]\,m^{\underline{n-d}}(n-1)^{\underline{d}} \\
&\qquad\quad + (-1)^{m+1-d+1}\,[n-d\le m+1]\,m+1^{\underline{n-d}}(n-1)^{\underline{d}} \\
&\qquad = (-1)^{m-d+1}\,[n-d\le m+1]\,m^{\underline{n-d-1}}(n-1)^{\underline{d}} \\
&\qquad\quad \cdot \underbrace{\left([n-d\le m]\,(m-n+d+1)-(m+1)\right)}_{=-[n-d\le m](n-d)} \\
&\qquad = (-1)^{m+1-(d+1)}\,[n-(d+1)\le m]\,m^{\underline{n-(d+1)}}(n-1)^{\underline{d+1}},
\end{aligned} \tag{8.22}$$

und somit ist die Aussage bewiesen. □

Für ein $m \in \mathbb{N}$ sei mit $\mathcal{C}_m$ die zyklische Gruppe mit m Elementen notiert, also $\mathcal{C}_m \simeq (\mathbb{Z}/m\mathbb{Z}, +)$. Wir werden im Folgenden $\mathcal{C}_m = \{0, 1, 2, \ldots, m-1\}$ mit „+“ modulo m verwenden.

Proposition. *Sei p eine Primzahl. Für jede p-Sylowgruppe S von $\mathcal{P}_1$ gilt*

$$S \simeq \mathcal{C}_p, \tag{8.23}$$

und für jede p-Sylowgruppe S von $\mathcal{P}_2$ gilt

$$S \simeq \mathcal{C}_p \wr \mathcal{C}_p. \tag{8.24}$$

Bemerkung. Betrachten wir eine p-Sylowgruppe von $\mathcal{P}_2$, so ist eine zyklische Gruppe des Kranzprodukts (8.24) für den modulo p genommenen Teil verantwortlich. Die restlichen zyklischen Gruppen übernehmen dann modulo p^2 wieder je eine „Stelle“ und permutieren dabei den Koeffizienten von p in der p-adischen Darstellung der Zahlen, siehe Abbildung 8.2.

Beweis. Die Aussage für $\mathcal{P}_1$ ist trivialerweise erfüllt, da die p-Sylowgruppe genau p Elemente hat und somit, da p prim ist, eine zyklische Gruppe mit p Elementen.

In $\mathcal{P}_2$ betrachten wir ohne Beschränkung der Allgemeinheit die p-Sylowgruppe S mit Ableitung konstant 1 modulo p und welche als Funktion modulo p die Gestalt $(0\,1\,2\,3\,\ldots\,p-1)^k, 0 \le k \le p-1$ hat. Die anderen Sylowgruppen ergeben sich dann klarerweise mittels Konjugation.

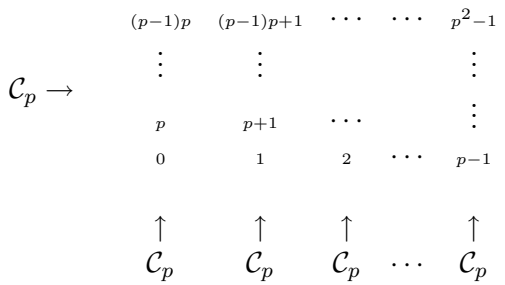

Abbildung 8.2: Isomorphie der p-Sylowgruppe $S \simeq \mathcal{C}_p \wr \mathcal{C}_p$ in $\mathcal{P}_2$

Wir definieren uns eine Abbildung

$$\lambda : S \longrightarrow \mathcal{C}_p \wr \mathcal{C}_p; \quad X + c + p \sum_{0 \le i \le p-1} a_i X^{\underline{i}} \longmapsto \left(c, (y_k)_{0 \le k \le p-1}\right) \tag{8.25}$$

mit

$$y_k \equiv \sum_{0 \le j \le k} a_i k^{\underline{i}} \mod p. \tag{8.26}$$

1. λ ist eine wohldefinierte Abbildung.

   Sei $f \equiv g \mod p^2$. Aufgrund der eindeutigen Darstellung (siehe Satz 4.1) sind alle Koeffizienten gleich. Da es sich bei (8.26) um eine reguläre Transformation handelt (siehe Lemma am Anfang dieses Kapitels) folgt unmittelbar, dass $\lambda(f) = \lambda(g)$ ist.

2. λ ist ein Homomorphismus.

   Sei

   $$f = X + c + pA, \quad \text{mit } A = \sum_{0 \le i \le p-1} a_i X^{\underline{i}}, \quad 0 \le c, a_0, \ldots, a_{p-1} \le p-1 \tag{8.27a}$$

   und

   $$g = X + d + pB, \quad \text{mit } B = \sum_{0 \le i \le p-1} b_i X^{\underline{i}}, \quad 0 \le d, b_0, \ldots, b_{p-1} \le p-1. \tag{8.27b}$$

   Laut dem Lemma am Anfang diese Kapitels ist (8.26) eine reguläre Transformation und es ergibt sich

   $$a_i \equiv \sum_{0 \le k \le p-1} \underbrace{(-1)^{i+k+1} \, [k \le i] \binom{p-1}{i-k} (p-1-i+k)^{\underline{p-1-i}} y_k}_{=:q(i,k)} \mod p \tag{8.28}$$

Setzt man dies in die Komposition $f \circ g$ ein, so ergibt sich

$$\begin{aligned} f \circ g &= X + d + pB + c + p \sum_{0 \le i \le p-1} a_i (X + d + pB)^{\underline{i}} \\ &\equiv X + c + d + pB + p \sum_{0 \le i \le p-1} a_i (X + d)^{\underline{i}} \\ &\equiv X + c + d + pB + p \sum_{0 \le i,k \le p-1} q(i,k) y_k (X + d)^{\underline{i}} \\ &\equiv X + c + d + pB + p \sum_{0 \le i,k \le p-1} q(i,k) y_{k+d} X^{\underline{i}} \mod p^2, \end{aligned} \tag{8.29}$$

wobei wir im letzten Schritt das vorherige Lemma verwendet haben.

Einsetzen von (8.28) in B ergibt

$$B = \sum_{0 \le i \le p-1} b_i X^{\underline{i}} = \sum_{0 \le i,k \le p-1} q(i,k) z_k X^{\underline{i}}. \tag{8.30}$$

Ordnen wir nun nach $X^{\underline{i}}$ so ergibt sich

$$f \circ g \equiv X + (c + d) + p \sum_{0 \le i,k \le p-1} q(i,k)(y_{k+d} + z_k) X^{\underline{i}} \mod p^2 \tag{8.31}$$

Jetzt wenden wir auf beiden Seite unsere Abbildung λ an und erhalten

$$\begin{aligned} \lambda(f \circ g) &= \lambda \left(X + (c + d) + p \sum_{0 \le i,k \le p-1} q(i,k)(y_{k+d} + z_k) X^{\underline{i}} \right) \\ &= \left(c + d, (y_{k+d} + z_k)_{0 \le k \le p-1} \right) \\ &= \left(c, (y_k)_{0 \le k \le p-1} \right) \cdot \left(d, (z_k)_{0 \le k \le p-1} \right) \\ &= \lambda(f) \cdot \lambda(g), \end{aligned} \tag{8.32}$$

wobei $y_{k+p} = y_k$ und $z_{k+p} = z_k$ beziehungsweise wir denken uns die Indizes modulo p.

3. λ ist bijektiv.

   Wir betrachten den Kern von λ. Sei $\left(c, (y_k)_{0 \le k \le p-1} \right) = \mathrm{id}_{\mathcal{C}_p \wr \mathcal{C}_p}$, also $c = 0$ und $\forall k : y_k = 0$. Aufgrund von (8.28) und da $0 \le a_i \le p - 1$ erhalte ich $a_i = 0$ für jedes i. Somit ist das zugehörige $f = X$, also die Identität in $\mathcal{P}_2$, also ist λ injektiv.

   Surjektiv gilt dann aus Kardinalitätsgründen, und somit ist die Abbildung bijektiv.

□

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.