Restklassenweise affine Gruppen

Stefan Kohl

Hochschulöffentlicher Vortrag im Rahmen des Promotionsverfahrens

Universität Stuttgart, 6. Oktober 2005

Motivation (I)

3n+1 - Vermutung: Iterierte Anwendung der Collatz-Abbildung

$$T: \ \mathbb{Z} \longrightarrow \mathbb{Z},$$

$$n \ \longmapsto \ \begin{cases} \frac{n}{2} & \text{falls} \ \ n \text{ gerade,} \\ \frac{3n+1}{2} & \text{falls} \ \ n \text{ ungerade} \end{cases}$$

auf eine beliebige natürliche Zahl führt nach endlich vielen Schritten zur 1, d.h. es gilt

$$\forall n \in \mathbb{N} \ \ \exists k \in \mathbb{N}_0 : \ n^{T^k} = 1.$$

Diese Vermutung wurde um das Jahr 1930 von Lothar Collatz aufgestellt und ist bis heute unbewiesen.

Beispiel: Beginnt man bei $n = 7$, so erhält man die Folge

$$7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1.$$

Motivation (II)

Konjugation der Collatz-Abbildung T mit einer Permutation $\sigma \in (\mathrm{Sym}(\mathbb{Z})_{\{\mathbb{N}\}})_1$ liefert die folgende äquivalente Behauptung:

$$\forall n \in \mathbb{N} \;\; \exists k \in \mathbb{N}_0 : \;\; n^{(T^\sigma)^k} = 1.$$

Die $3n+1$ - Vermutung ist genau dann wahr, wenn es ein σ so gibt, daß T^σ alle $n > 1$ auf kleinere natürliche Zahlen abbildet. Es handelt sich also um ein Normalformenproblem.

Jeffrey C. Lagarias hat eine kommentierte Bibliographie zur $3n+1$ - Vermutung verfaßt, die er laufend aktualisiert. In der derzeit aktuellen Version vom 10. Juli 2005 umfaßt Lagarias' Bibliographie 193 Referenzen.

Keiner der Artikel, die dort zitiert werden, sucht nach einem gruppentheoretischen Zugang oder untersucht die Struktur von bijektiven, 'der Collatz-Abbildung ähnlichen' Abbildungen erzeugter Gruppen.

Motivation (III)

Man weiß bereits einiges über die Struktur unendlicher Permutationsgruppen von beschränktem Transitivitätsgrad.

Eine gute Übersicht über diesbezügliche Resultate gibt der *Springer Lecture Notes* - Band *Notes on Infinite Permutation Groups* von Bhattacharjee et al..

Beträchtlich weniger ist über hoch transitive Permutationsgruppen bekannt, also über solche, die k - fach transitiv für jedes k sind.

Die Gruppe der restklassenweise affinen Bijektionen des Rings der ganzen Zahlen ist eine solche. Überdies besitzt sie eine reichhaltige gruppentheoretische Struktur und ist rechnerischen Untersuchungen zugänglich.

Grundbegriffe (I)

Es sei R ein unendlicher euklidischer Ring, der mindestens ein Primelement enthält, und dessen Restklassenringe alle endlich sind.

'Typisches' Beispiel: $R = \mathbb{Z}$.

Weitere Beispiele:

$$R = \mathbb{Z}_\pi, \quad R = \mathbb{F}_q[x], \quad R = \mathbb{Z}[i].$$

Grundbegriffe (II)

Eine Abbildung $f : R \to R$ heiße *restklassenweise affin* oder kurz *rcwa*-Abbildung, wenn es ein $m \in R \setminus \{0\}$ so gibt, daß die Einschränkungen von f auf die Restklassen $r(m) \in R/mR$ affin sind.

Das heißt, es gebe zu jeder Restklasse $r(m)$ Koeffizienten $a_{r(m)}, b_{r(m)}, c_{r(m)} \in R$ so, daß die Einschränkung der Abbildung f auf die Menge $r(m) = \{r + km | k \in R\}$ gegeben ist durch

$$f|_{r(m)} : \; r(m) \to R,$$

$$n \;\mapsto\; \frac{a_{r(m)} \cdot n + b_{r(m)}}{c_{r(m)}} \; .$$

Das Ringelement m werde als *Modul* von f bezeichnet. Um Eindeutigkeit zu erreichen sei m multiplikativ minimal gewählt.

Beispiele

Beispiele für rcwa-Abbildungen von $\mathbb{Z}$:

1. 'Trivialbeispiele'

$$n \mapsto n+1, \quad n \mapsto -n, \quad n \mapsto n+(-1)^n.$$

2. Die Collatz-Abbildung T. Diese ist zwar surjektiv, aber nicht injektiv.

3. Eine auch bereits von Lothar Collatz betrachtete bijektive rcwa-Abbildung ist

$$\alpha: \quad n \ \mapsto \begin{cases} \frac{3n}{2} & \text{falls} \quad n \equiv 0 \bmod 2, \\ \frac{3n+1}{4} & \text{falls} \quad n \equiv 1 \bmod 4, \\ \frac{3n-1}{4} & \text{falls} \quad n \equiv 3 \bmod 4. \end{cases}$$

Die Zykelstruktur dieser Permutation ist bislang noch nicht vollständig bekannt.

Zielsetzung

Es bezeichne RCWA(R) die Gruppe aller bijektiven rcwa-Abbildungen des Rings R.

Vorrangiges Ziel meiner Arbeit war die Untersuchung der Struktur der Gruppe RCWA($\mathbb{Z}$) der restklassenweise affinen Bijektionen des Rings der ganzen Zahlen.

Ergebnisse (I)

Die Gruppe RCWA($\mathbb{Z}$)

- besitzt $\mathbb{Z}^\times$ als epimorphes Bild,
- hat ein triviales Zentrum,
- besitzt keinen nichttrivialen auflösbaren Normalteiler,
- ist nicht endlich erzeugt,
- besitzt endliche Untergruppen sämtlicher Isomorphietypen, und
- hat zu zwei vorgegebenen Untergruppen stets eine zu deren direktem Produkt isomorphe Untergruppe.

Ergebnisse (II)

Die Gruppe RCWA($\mathbb{Z}$)

- hat nur endlich viele Konjugiertenklassen von Elementen einer gegebenen ungeraden Ordnung, aber unendlich viele von Elementen einer gegebenen geraden Ordnung,

- wird zu einer Gruppe von Homöomorphismen, wenn man $\mathbb{Z}$ durch Wahl der Menge aller Restklassen als Basis mit einer Topologie versieht, und

- operiert transitiv auf der Menge aller von $\emptyset$ und $\mathbb{Z}$ verschiedenen Vereinigungen jeweils endlich vieler Restklassen von $\mathbb{Z}$.

Ergebnisse (III)

Die Gruppe RCWA($\mathbb{Z}$)

- operiert hoch transitiv auf $\mathbb{Z}$, und hat deshalb nur nichttriviale Normalteiler, die ebenfalls hoch transitiv auf $\mathbb{Z}$ operieren,

- besitzt nur nichttriviale Normalteiler, die zu jedem $k \in \mathbb{N}$ eine Untergruppe haben, die auf einer geeignet gewählten Partition von $\mathbb{Z}$ in mehr als k Restklassen operiert und auf ihr eine volle symmetrische Gruppe induziert, und

- hat einen Normalteiler, der erzeugt wird von Bildern der Elemente $\nu : n \mapsto n + 1$, $\varsigma : n \mapsto -n$ und $\tau : n \mapsto n + (-1)^n$ unter gewissen konkret angebbaren Monomorphismen der Gruppe RCWA($\mathbb{Z}$) in sich selbst.

Ergebnisse (IV)

Es gilt:

- Eine endliche Erweiterung $G \trianglerighteq N$ eines subdirekten Produkts N endlich vieler unendlicher Diedergruppen besitzt stets ein monomorphes Bild in RCWA($\mathbb{Z}$).

- Die Homomorphismen einer vorgegebenen endlichen Gruppe G ungerader Ordnung nach RCWA($\mathbb{Z}$) werden bis auf innere Automorphismen von RCWA($\mathbb{Z}$) parametrisiert durch die nichtleeren Teilmengen der Menge der Äquivalenzklassen von transitiven endlichen Permutationsdarstellungen von G.

Ergebnisse (V)

Eine affine Abbildung $n \mapsto (an+b)/c$ von $\mathbb{Q}$ ist genau dann ordnungserhaltend, wenn $a > 0$.

Eine rcwa-Abbildung von $\mathbb{Z}$ heiße *klassenweise ordnungserhaltend*, wenn alle ihre affinen Teilabbildungen ordnungserhaltend sind.

Es gilt: Die Untergruppe

$$\mathrm{RCWA}^{+}(\mathbb{Z}) < \mathrm{RCWA}(\mathbb{Z})$$

der klassenweise ordnungserhaltenden bijektiven restklassenweise affinen Abbildungen besitzt $(\mathbb{Z}, +)$ als epimorphes Bild.

-

Die genannten Aussagen lassen sich zum großen Teil allgemeiner formulieren für Gruppen $\mathrm{RCWA}(R)$ über jeweils geeigneten euklidischen Ringen R.

Methoden (I)

Es wurden explizit Epimorphismen

$$\text{sgn}: \quad \text{RCWA}(\mathbb{Z}) \to \mathbb{Z}^\times$$

('Signatur') sowie

$$\det: \quad \text{RCWA}^+(\mathbb{Z}) \to (\mathbb{Z}, +)$$

('Determinante') konstruiert.

In der in der Definition einer rcwa-Abbildung verwendeten Notation gilt für eine Permutation $\sigma \in \text{RCWA}(\mathbb{Z})$

$$\det(\sigma) \;=\; \frac{1}{m} \sum_{r(m) \in \mathbb{Z}/m\mathbb{Z}} \frac{b_{r(m)}}{|a_{r(m)}|}$$

sowie

$$\text{sgn}(\sigma) \;=\; (-1)^{\det(\sigma) + \sum\limits_{r(m):a_{r(m)}<0} \frac{m-2r}{m}}.$$

Methoden (II)

Zur Ideenfindung haben umfangreiche rechnerische Untersuchungen mit meinem GAP-Package RCWA beigetragen.

Im Beweis, daß es sich wirklich um Epimorphismen handelt, werden Restklassen $[r/m]$ mit fixierten Repräsentanten und vorzeichenbehaftetem Modul eingeführt.

Ferner wird eine Invariante δ derartiger Restklassen definiert wie folgt:

$$\delta\left(\left[\frac{r}{m}\right]\right) \;:=\; \frac{r}{m} \;-\; \frac{1}{2}.$$

Diese Definition wird additiv fortgesetzt auf Partitionen $\mathcal{P}$ von $\mathbb{Z}$ in endlich viele Restklassen $[r/m]$:

$$\delta\left(\mathcal{P}\right) \;:=\; \sum_{[r/m]\in\mathcal{P}} \delta\left(\left[\frac{r}{m}\right]\right).$$

Methoden (III)

Es wird gezeigt, daß der Wert $\delta(\mathcal{P}) \mod 1$ für jede Partition $\mathcal{P}$ gleich ist. Ferner wird gezeigt, daß für $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ gilt:

$$\delta(\mathcal{P}^\sigma) \;=\; \delta(\mathcal{P}) + \det(\sigma).$$

Dies liefert die Ganzzahligkeit der Determinante sowie die Additivität der Determinantenabbildung.

Beispiele:

- Es ist $\det(n \mapsto n+1) = 1$.

- Es bezeichne α die eingangs erwähnte Collatz'sche Permutation. Dann ist

$$\det(\alpha) \;=\; \frac{1}{4}\left(0 + \frac{1}{3} + 0 - \frac{1}{3}\right) \;=\; 0.$$

Methoden (IV)

Im Beweis, daß die Signaturabbildung ein Epimorphismus ist, wird eine Invariante ϱ eingeführt wie folgt:

$$\varrho\left(\left[\frac{r}{m}\right]\right) := \begin{cases} \exp\left(\frac{1}{2}\,\delta\left(\left[\frac{r}{m}\right]\right)\right) & \text{falls} \quad m > 0, \\ \exp\left(-\frac{1}{2}\,\delta\left(\left[\frac{r}{m}\right]\right)\right) & \text{falls} \quad m < 0. \end{cases}$$

Hierbei sei $\exp : z \mapsto e^{2\pi i z}$.

Diese Definition wird multiplikativ fortgesetzt auf Partitionen $\mathcal{P}$ von $\mathbb{Z}$ in endlich viele Restklassen $[r/m]$:

$$\varrho\,(\mathcal{P}) \;:=\; \prod_{[r/m]\in\mathcal{P}} \varrho\left(\left[\frac{r}{m}\right]\right).$$

Es wird gezeigt, daß $\varrho\,(\mathcal{P})$ bis auf etwaige Multiplikation mit -1 unabhängig von der Wahl von $\mathcal{P}$ ist.

Methoden (V)

Ferner wird gezeigt, daß für $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ gilt:

$$\varrho\left(\mathcal{P}^{\sigma}\right) \;=\; \varrho\left(\mathcal{P}\right) \cdot \mathrm{sgn}(\sigma).$$

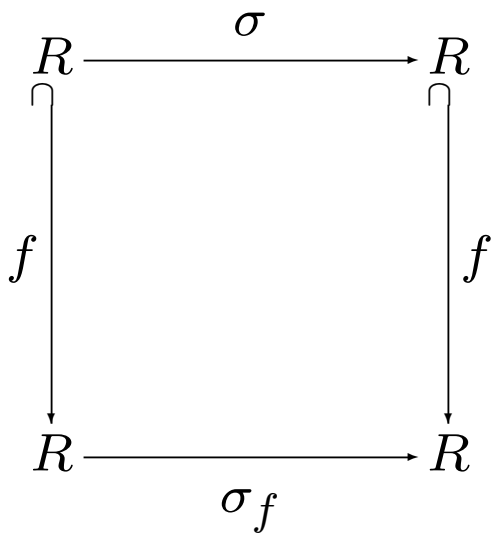
Dies liefert die Multiplikativität der Signaturabbildung, sowie zusammen mit der vorhergehenden Aussage $\mathrm{sgn}(\sigma) \in \{-1, 1\}$.

Methoden (VI)

Es sei $f : R \to R$ eine injektive rcwa-Abbildung. Der *zu f assoziierte Einschränkungsmonomorphismus*

$$\pi_f : \mathrm{RCWA}(R) \to \mathrm{RCWA}(R), \quad \sigma \mapsto \sigma_f$$

sei so definiert, daß das Diagramm



stets kommutiert, und σ_f das Komplement des Bildes von f punktweise fixiert.

Methoden (VII)

Es sei $r(m) \subset \mathbb{Z}$ eine Restklasse, und es sei $\nu : n \mapsto n+1$ und $\varsigma : n \mapsto -n$. Ferner sei $\nu_{r(m)} := \nu^{\pi_{n \mapsto mn+r}}$ und $\varsigma_{r(m)} := \varsigma^{\pi_{n \mapsto mn+r}}$. Die Abbildungen $\nu_{r(m)}$ und $\varsigma_{r(m)}$ erzeugen eine unendliche Diedergruppe, die auf der Restklasse $r(m)$ operiert.

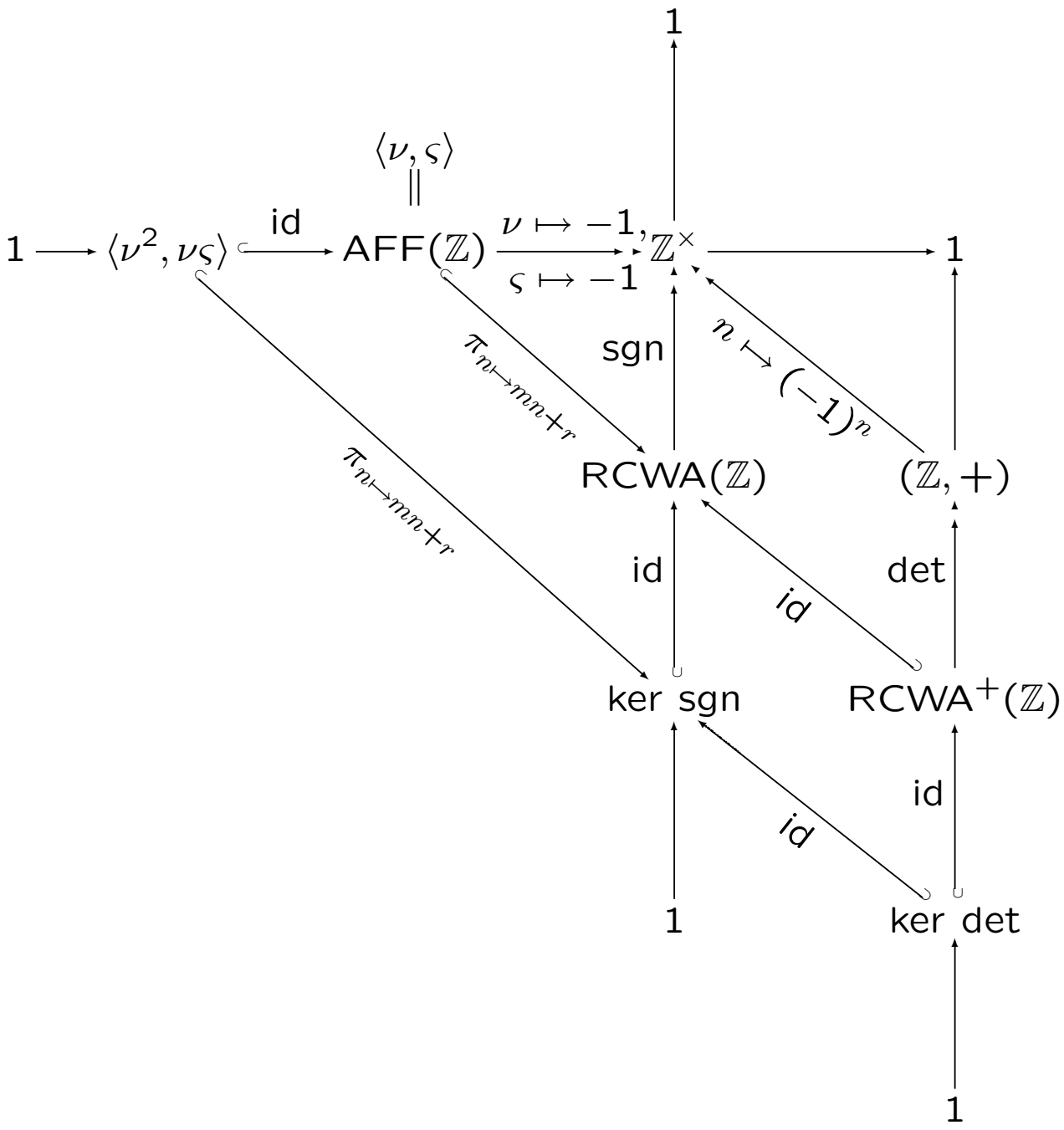
Es seien $r_1(m_1), r_2(m_2) \subset \mathbb{Z}$ Restklassen, und es sei $\tau : n \mapsto n + (-1)^n$. Ferner sei

$$\mu = \mu_{r_1(m_1),r_2(m_2)} \in \mathrm{Rcwa}(\mathbb{Z}),$$

$$n \mapsto \begin{cases} \dfrac{m_1 n + 2r_1}{2} & \text{falls } \ n \in 0(2), \\ \dfrac{m_2 n + (2r_2 - m_2)}{2} & \text{falls } \ n \in 1(2) \end{cases}$$

Dann ist $\tau_{r_1(m_1),r_2(m_2)} := \tau^{\pi_\mu}$ eine Involution, die die Restklassen $r_1(m_1)$ und $r_2(m_2)$ vertauscht ('Klassentransposition').

Strukturübersicht



Methoden (VIII)

Es sei $\mathcal{P} = \{r_1(m_1), \ldots, r_k(m_k)\}$ eine Partition von $\mathbb{Z}$ in endlich viele Restklassen. Dann erzeugen die Klassentranspositionen $\tau_{r_i(m_i),r_j(m_j)}$ eine zur symmetrischen Gruppe S_k isomorphe Gruppe, die treu auf $\mathcal{P}$ operiert.

Nimmt man die Abbildungen $\nu_{r_i(m_i)}$ und $\varsigma_{r_i(m_i)}$ zur Menge der Erzeugenden hinzu, so erhält man eine zum Kranzprodukt $\mathsf{D}_\infty \wr \mathsf{S}_k$ isomorphe Gruppe.

Es wurde gezeigt, daß alle Untergruppen von RCWA($\mathbb{Z}$), für die Menge der Moduln derer Elemente es eine obere Schranke gibt, auch Untergruppen einer solchen Gruppe sind, vorausgesetzt, man wählt jeweils k genügend groß und $\mathcal{P}$ geeignet.

Es wurde ebenfalls gezeigt, daß die von allen diesen Untergruppen erzeugte Untergruppe von RCWA($\mathbb{Z}$) ein Normalteiler ist.

Beispiele (I)

Es sei

$$g: \quad n \mapsto \begin{cases} 2n+2 & \text{falls} \quad n \in 0(3), \\ n+4 & \text{falls} \quad n \in 1(6), \\ \frac{n}{2} & \text{falls} \quad n \in 2(6), \\ n-4 & \text{falls} \quad n \in 4(6), \\ n-2 & \text{falls} \quad n \in 5(6) \end{cases}$$

und

$$h: \quad n \mapsto \begin{cases} 2n+2 & \text{falls} \quad n \in 0(3), \\ n-2 & \text{falls} \quad n \in 1(6), \\ \frac{n}{2} & \text{falls} \quad n \in 2(6), \\ n-1 & \text{falls} \quad n \in 4(6), \\ n+1 & \text{falls} \quad n \in 5(6). \end{cases}$$

Dann ist $\text{ord}(g) = 7$ und $\text{ord}(h) = 12$.

Beispiele (II)

Die Gruppe $G := \langle g, h \rangle$ operiert auf der Partition

$$\begin{aligned}\mathcal{P} := \{\ & 0(12),\ 1(12),\ 3(12),\ 4(12),\ 5(12),\\ & 6(12),\ 7(12),\ 9(12), 10(12), 11(12),\\ & 2(24),\ 8(24), 14(24), 20(24)\ \}\end{aligned}$$

von $\mathbb{Z}$. Die von G auf $\mathcal{P}$ induzierte Permutationsgruppe ist isomorph zu

$$\begin{aligned}H\ := \Big\langle & (1,11,2,5,3,12,4)\\ & (6,13,7,10,8,14,9),\\ & (1,11,2,10)(3,12,4)\\ & (5,6,13,7)(8,14,9)\Big\rangle.\end{aligned}$$

Die Ordnung von H ist 322560, und H' ist eine perfekte Gruppe der Ordnung 161280. Der Kern der Operation von G auf $\mathcal{P}$ ist eine freie abelsche Gruppe vom Rang 6.

Beispiele (III)

Die von den Permutationen

$$\alpha: \quad n \;\mapsto\; \begin{cases} \frac{3n}{2} & \text{falls} \quad n \in 0(2), \\ \frac{3n+1}{4} & \text{falls} \quad n \in 1(4), \\ \frac{3n-1}{4} & \text{falls} \quad n \in 3(4) \end{cases}$$

und

$$\beta: \quad n \;\mapsto\; \begin{cases} \frac{3n}{5} & \text{falls} \quad n \in 0(5), \\ \frac{9n+1}{5} & \text{falls} \quad n \in 1(5), \\ \frac{3n-1}{5} & \text{falls} \quad n \in 2(5), \\ \frac{9n-2}{5} & \text{falls} \quad n \in 3(5), \\ \frac{9n+4}{5} & \text{falls} \quad n \in 4(5) \end{cases}$$

erzeugte Gruppe operiert (mindestens!) vierfach transitiv auf der Menge der natürlichen Zahlen ($\neq 0$).

(Beweis rechnerisch mit RCWA .)

Beispiele (IV)

Die von den Permutationen

$$\nu : \ n \ \mapsto \ n+1$$

und

$$\tau_{1(2),0(4)} : \ n \ \mapsto \ \begin{cases} 2n-2 & \text{falls} \ \ n \in 1(2), \\ \frac{n+2}{2} & \text{falls} \ \ n \in 0(4), \\ n & \text{falls} \ \ n \in 2(4) \end{cases}$$

erzeugte Gruppe operiert 3-fach transitiv, aber nicht 4-fach transitiv auf $\mathbb{Z}$.

(Beweis rechnerisch mit RCWA .)

Beispiele (V)

Es sei p eine ungerade Primzahl, und

$$\begin{aligned}\sigma_p \;:=\; & \tau_{0(8),1(2p)} \cdot \tau_{4(8),2p-1(2p)} \\ & \cdot\tau_{0(4),1(2p)} \cdot \tau_{2(4),2p-1(2p)} \\ & \cdot\tau_{2(2p),1(4p)} \cdot \tau_{4(2p),2p+1(4p)}\cdot\end{aligned}$$

Dann ist σ_p gegeben durch

$$n \mapsto \begin{cases} n/2 & \text{falls} \quad n \in 0(4) \setminus M_1, \\ n+1 & \text{falls} \quad n \in 1(2p), \\ (pn+2p-2)/2 & \text{falls} \quad n \in 2(4), \\ n & \text{falls} \quad n \in 1(2) \setminus M_2, \\ n-3 & \text{falls} \quad n \in 4(4p), \\ n+2p-7 & \text{falls} \quad n \in 8(4p), \\ n-2p+5 & \text{falls} \quad n \in 2p-1(2p) \end{cases}$$

mit $M_1 = 4(4p) \cup 8(4p)$
und $M_2 = 1(2p) \cup 2p-1(2p)$.

Beispiele (V')

Die eingangs genannte Collatz'sche Permutation α läßt sich in Klassentranspositionen faktorisieren. Man benötigt allerdings 'ziemlich viele' Faktoren.

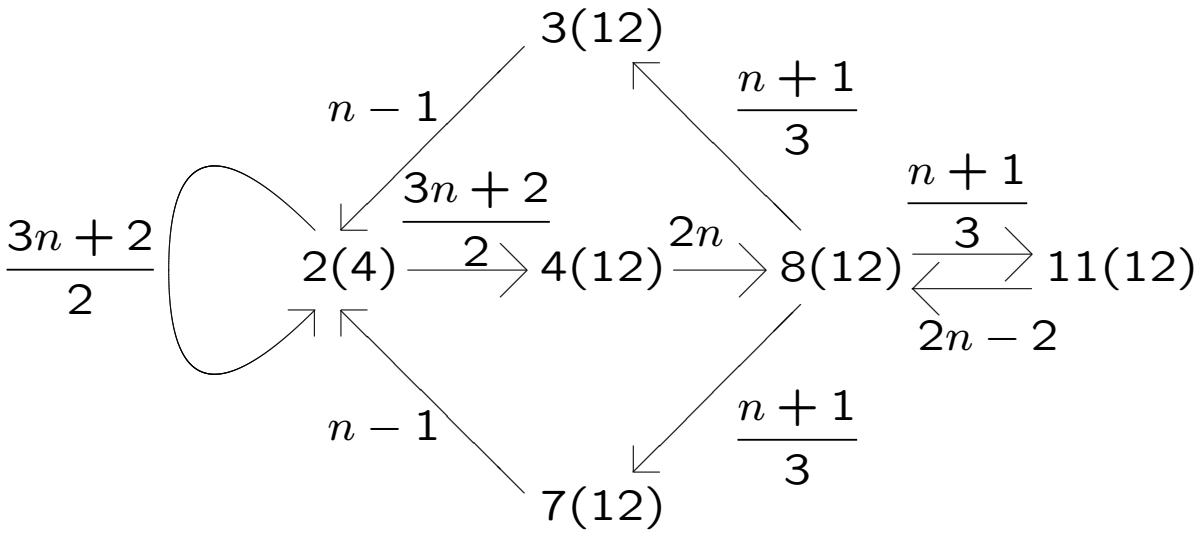
Ein in RCWA implementiertes Verfahren, eine solche Faktorisierung einer gegebenen rcwa-Abbildung zu bestimmen, stützt sich wesentlich auf die Abbildungen σ_p sowie deren Bilder unter Einschränkungsmonomorphismen.

Deren 'Schlüsseleigenschaft' ist, daß in den Zählern nur der Faktor p, in den Nennern hingegen nur der Faktor 2 vorkommt. Man kann sie daher dazu verwenden, gewissermaßen 'Übergewichte' einzelner Primfaktoren der Koeffizienten in Zähler und Nenner der affinen Teilabbildungen auszugleichen.

Beispiele (VI)

Es sei $\kappa := \tau_{2(4),3(4)} \cdot \tau_{3(4),8(12)} \cdot \tau_{4(6),8(12)}$.

Die Permutation κ besitzt nur endliche Zykel, hat aber dennoch unendliche Ordnung. Der folgende Graph visualisiert die durch sie induzierten Übergänge zwischen den einzelnen Restklassen (mod 12):



Beispiele (VII)

Die von den Permutationen $\tau : n \mapsto n+(-1)^n$ und

$$\tau_r := \prod_{k=1}^{\infty} \tau_{2^{k-1}-1(2^k+1),2^k+2^{k-1}-1(2^k+1)}^{1-\delta_{r,k} \bmod 3}$$

($r \in \{0,1,2\}$) erzeugte Gruppe ist isomorph zur Grigorchuk-Gruppe.

Die Erzeugenden τ, τ_0, τ_1 bzw. τ_2 entsprechen a, b, c bzw. d in der Notation von

R. I. Grigorchuk.
Bernside's Problem on Periodic Groups.
Functional Anal. Appl. 14:41–43, 1980.

Offene Fragen

- Ist RCWA($\mathbb{Z}$) $\rhd$ ker sgn $\rhd$ 1 eine Kompositionsreihe?

- Wird RCWA($\mathbb{Z}$) von den Abbildungen $\nu_{r(m)}$, $\varsigma_{r(m)}$ und $\tau_{r_1(m_1),r_2(m_2)}$ erzeugt?

- Sind endlich erzeugte Untergruppen von RCWA($\mathbb{Z}$) stets endlich präsentiert?

- Welche Transitivitätsgrade kann die Operation einer endlich erzeugten Untergruppe von RCWA($\mathbb{Z}$) auf $\mathbb{Z}$ haben?

- Besitzt RCWA($\mathbb{Z}$) nichttriviale äußere Automorphismen?

- Enthaltenseins- / Konjugiertheitsproblem in endl.-erz. Untergruppen von RCWA($\mathbb{Z}$).

Referenzen

RCWA -
[R]esidue [C]lass-[W]ise [A]ffine Groups.
GAP package, 2005.
`www.gap-system.org/Packages/rcwa.html`

Meenaxi Bhattacharjee, Dugald Macpherson, Rögnvaldur G. Möller, and Peter M. Neumann. *Notes on Infinite Permutation Groups*. Number 1698 in Lecture Notes in Mathematics. Springer-Verlag, 1998.

Jeffrey C. Lagarias.
The 3x+1 problem:
An annotated bibliography, 2004.
`arxiv.org/abs/math.NT/0309224`