Restklassenweise affine Gruppen

Von der Fakultät Mathematik und Physik
der Universität Stuttgart
zur Erlangung der Würde eines
Doktors der Naturwissenschaften (Dr. rer. nat.)
genehmigte Abhandlung

Vorgelegt von

Stefan Kohl

geboren in Sindelfingen

Hauptberichter: Prof. Dr. Wolfgang Kimmerle
Mitberichter: Prof. Dr. Markus Stroppel

Tag der mündlichen Prüfung: 6. Oktober 2005

Institut für Geometrie und Topologie der Universität Stuttgart
2005

Diese Dissertation ist an folgenden Orten publiziert:

- OPUS-Datenbank (Universität Stuttgart):
  `http://elib.uni-stuttgart.de/opus/volltexte/2005/2448/`
- Archivserver Deutsche Bibliothek:
  `http://deposit.ddb.de/cgi-bin/dokserv?idn=977164071`

In diesem Exemplar sind alle dem Autor am 29.12.2005 bekannten Errata korrigiert. Eine im Falle des Bekanntwerdens weiterer Errata jeweils aktualisierte Liste derselben befindet sich auf der Homepage des Autors.

Mathematics Subject Classification (MSC 2000):

20B22	Multiply transitive infinite groups
20E99	Structure and classification of infinite or finite groups
20-04	Group theory: explicit machine computation and programs
11B99	Sequences and sets
11-04	Number theory: explicit machine computation and programs

Schlagworte: $3n + 1$-Vermutung, Collatz-Vermutung, unendliche Permutationsgruppe, mehrfach transitive Permutationsgruppe, hoch transitive Permutationsgruppe, Jordan-Gruppe, restklassenweise affine Abbildung, restklassenweise affine Gruppe, GAP.

Keywords: $3n + 1$ Conjecture, Collatz Conjecture, infinite permutation group, multiply transitive permutation group, highly transitive permutation group, Jordan group, residue class-wise affine mapping, residue class-wise affine group, GAP.

Inhaltsverzeichnis

English Summary

Motivation

This thesis is motivated by the

$3n + 1$ **Conjecture:** Iterated application of the mapping

$$T: \ \mathbb{Z} \longrightarrow \mathbb{Z}, \quad n \ \longmapsto \begin{cases} \frac{n}{2} & \text{if} \ \ n \text{ even,} \\ \frac{3n+1}{2} & \text{if} \ \ n \text{ odd} \end{cases}$$

to any positive integer yields 1 after a finite number of steps, i.e.

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

This conjecture has been made by Lothar Collatz in the 1930s, and is still open today. Conjugating the Collatz mapping T by a permutation σ of $\mathbb{Z}$ which maps positive integers to positive integers and fixes 1 turns the $3n + 1$ Conjecture into the following equivalent assertion:

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

The $3n+1$ Conjecture is true if and only if there is such a permutation σ that T^σ maps all integers $n > 1$ to smaller positive integers. Hence the problem is to find a certain normal form of the Collatz mapping.

Dealing with arbitrary permutations of infinite sets is difficult, both by means of theory and as well by means of computation. One might want to get a better understanding at least of those permutations which look ‘similar’ to the Collatz mapping. The bijective residue class-wise affine mappings form a class of such permutations.

Jeffrey C. Lagarias maintains a comprehensive annotated bibliography [Lag05] on the $3n+1$ Conjecture. In its most recent version at the time of writing these lines, it lists 193 references.

None of the articles which are referenced there describes a group theoretic approach. Also none of them investigates the structure of groups which are generated by bijective residue class-wise affine mappings, i.e. by permutations ‘similar to the Collatz mapping’.

Basic Definitions

Let R denote an infinite euclidean ring, which has at least one prime ideal and all of whose proper residue class rings are finite. Further assume that there is a mapping $|.| : R \to R$, which assigns certain 'standard associates' to the ring elements. In case $R = \mathbb{Z}$, let the standard associate be the absolute value.

We call a mapping $f : R \to R$ *residue class-wise affine*, or in short an *rcwa* mapping, if there is a nonzero element $m \in R$ such that the restrictions of f to the residue classes $r(m) \in R/mR$ are all affine. In different words, this means that for any residue class $r(m)$, there are coefficients $a_{r(m)}, b_{r(m)}, c_{r(m)} \in R$ such that the restriction of the mapping f to the set $r(m) = \{r + km | k \in R\}$ is given by

$$f|_{r(m)} : \; r(m) \to R, \quad n \;\mapsto\; \frac{a_{r(m)} \cdot n + b_{r(m)}}{c_{r(m)}} \;.$$

We call m the *modulus* of f, and use the notation $\mathrm{Mod}(f)$. To make this definition unique, we assume that m is chosen multiplicatively minimal and that $m = |m|$. To ensure uniqueness of the coefficients, we further assume that $\gcd(a_{r(m)}, b_{r(m)}, c_{r(m)}) = 1$ and that $c_{r(m)} = |c_{r(m)}|$.

The residue class-wise affine mappings of R form a monoid (= semigroup with 1) under composition of mappings (Lemma 1.3.4, Part (1)). We denote this monoid by $\mathrm{Rcwa}(R)$, and call its submonoids *residue class-wise affine* monoids.

The bijective residue class-wise affine mappings of R form a proper subgroup of the symmetric group $\mathrm{Sym}(R)$ (Lemma 1.3.4, Part (2)). We denote this group by $\mathrm{RCWA}(R)$, and call its subgroups *residue class-wise affine* groups.

There are two entirely different classes of residue class-wise affine mappings, -groups and -monoids. One of these classes consists of those mappings, groups and monoids, which have a very uncomplicated and easy structure. The other consists of those whose structure is complicated and often very difficult to investigate:

Let $G < \mathrm{Rcwa}(R)$ be a residue class-wise affine monoid. Assume that there is a nonzero element of R which is a multiple of the moduli of all elements of G. Then we say that G is *tame*, and call the standard associate of the multiplicatively minimal such element the *modulus* $\mathrm{Mod}(G)$ of G. Otherwise we say that G is *wild*, and set $\mathrm{Mod}(G) := 0$.

We call a mapping $f \in \mathrm{Rcwa}(R)$ *tame* resp. *wild*, if the cyclic monoid generated by f is tame resp. wild. According to Lemma 1.8.4, Part (2), a tame element of $\mathrm{RCWA}(\mathbb{Z})$ generates a tame cyclic group. However a group generated by two or more tame mappings is in general *not* tame.

Let $m \in R \setminus \{0\}$ and $f \in \mathrm{Rcwa}(R)$. Further let $\Gamma_{f,m}$ be the directed graph whose vertices are the residue classes (mod m), in which there is an edge from $r_1(m)$ to $r_2(m)$ if and only if there is an $n \in r_1(m)$ such that $n^f \in r_2(m)$. Then we call $\Gamma_{f,m}$ the *transition graph* of f with respect to the modulus m. Transition graphs encode a significant amount of information about the underlying residue class-wise affine mappings.

Aim

The aim of this thesis is to investigate the structure of the group $\mathrm{RCWA}(\mathbb{Z})$ of all residue class-wise affine bijections of the ring of integers.

Results

It is shown that the group $\mathrm{RCWA}(\mathbb{Z})$

- is not finitely generated (Theorem 2.1.1),
- has finite subgroups of any isomorphism type (Theorem 2.1.2),
- has a trivial centre (Corollary 2.1.6),
- does not have a nontrivial solvable normal subgroup (Corollary 2.1.6),
- acts highly transitively on $\mathbb{Z}$ (Theorem 2.1.5) and hence has only nontrivial normal subgroups which act highly transitively on $\mathbb{Z}$ as well (Corollary 2.1.6),
- is a group of homoeomorphisms of $\mathbb{Z}$ endowed with a topology by taking the set of all residue classes as a basis (Theorem 2.2.3),
- has, given two of its subgroups, always a subgroup which is isomorphic to their direct product (Corollary 2.3.3),
- acts transitively on the set of nonempty unions of finitely many residue classes of $\mathbb{Z}$ distinct from $\mathbb{Z}$ itself (Theorem 2.4.1),
- contains a monomorphic image of any finite extension $G \trianglerighteq N$ of a subdirect product N of finitely many infinite dihedral groups (Corollary 2.6.5),
- has only finitely many conjugacy classes of elements of given odd order, but infinitely many conjugacy classes of elements of given even order (Conclusion 2.7.2),
- has a normal subgroup which is generated by images of the elements $\nu : n \mapsto n + 1$, $\varsigma : n \mapsto -n$ and $\tau : n \mapsto n + (-1)^n$ under certain explicitly given monomorphisms of the group $\mathrm{RCWA}(\mathbb{Z})$ into itself (Theorem 2.9.4), and
- permits an epimorphism onto the group $\mathbb{Z}^\times$ (Theorem 2.12.8).

Many of the theorems listed above are formulated in a more general context for groups $\mathrm{RCWA}(R)$ over euclidean rings R.

Further the following is shown:

- The homomorphisms from a given group G of odd order to $\mathrm{RCWA}(\mathbb{Z})$ are parametrized up to inner automorphisms of $\mathrm{RCWA}(\mathbb{Z})$ by the nonempty subsets of the set of all equivalence classes of transitive finite-degree permutation representations of G (Theorem 2.6.7).

- Assume that $\mathrm{char}(R) = 0$ and that the exponent of $R^\times$ is finite. Suppose additionally that R has a residue class ring of cardinality 2. Then there are arbitrary large $l \in \mathbb{N}$ such that for any partition $\mathcal{P}$ of R into l residue classes the following holds: Each $1 \neq N \trianglelefteq \mathrm{RCWA}(R)$ has a subgroup which acts on $\mathcal{P}$ as a full symmetric group (Theorem 2.10.6).

- The subgroup $\mathrm{RCWA}^+(\mathbb{Z}) < \mathrm{RCWA}(\mathbb{Z})$ consisting of all class-wise order-preserving elements permits an epimorphism onto the group $(\mathbb{Z}, +)$ (Theorem 2.11.9).

- There is no residue class-wise affine permutation σ of $\mathbb{Z}$ which maps positive integers to positive integers and fixes 1 such that T^σ is monotonous almost everywhere (Theorem 3.11 and Remark 3.12).

Finally, Section 2.13 gives an outlook on open questions concerning the group $\mathrm{RCWA}(\mathbb{Z})$.

Algorithmic Aspects

Any residue class-wise affine mapping can be described by a finite number of ring elements. An immediate consequence of this is that if R is countable, then the group $\mathrm{RCWA}(R)$ and the monoid $\mathrm{Rcwa}(R)$ are countable as well. This fact basically makes residue class-wise affine mappings and -groups accessible to computational investigations.

Quite a number of constructive proofs in this thesis describe algorithms which can be translated more or less directly into GAP [GAP04] code. This has been done in the RCWA package [Koh05] (see `http://www.gap-system.org/Packages/rcwa.html`).

The manual of RCWA has a chapter which lists function names and short descriptions of the corresponding algorithms. In about 20 instances, it refers to theorems or proofs in this thesis.

Almost all of the many examples given in this thesis have been created with the help of the RCWA package. Computational investigations of lots of examples helped to find many of the results which eventually have been proven by purely theoretical means.

Examples

The residue class-wise affine mappings with modulus 1 are the affine mappings. Examples of such mappings are $\nu \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto n+1$ and $\varsigma \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto -n$.

The permutation $\tau \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto n + (-1)^n$ has modulus 2, and is an involution which interchanges the residue classes $0(2)$ and $1(2)$. Obviously, τ is tame.

The Collatz mapping T mentioned above is also a residue class-wise affine mapping with modulus 2. It is surjective, but not injective: The preimage of a given integer n under T is $\{(2n-1)/3, 2n\}$ if $n \equiv 2 \mod 3$, and $\{2n\}$ otherwise. The mapping T is wild. This is basically the reason why the $3n+1$ Conjecture is difficult to prove.

Appendix A describes criteria for distinguishing tame and wild mappings.

In 1932, Lothar Collatz investigated the wild bijective residue class-wise affine mapping

$$\alpha \in \mathrm{RCWA}(\mathbb{Z}) : \quad n \ \longmapsto \begin{cases} \frac{3n}{2} & \text{if} \ \ n \equiv 0 \bmod 2, \\ \frac{3n+1}{4} & \text{if} \ \ n \equiv 1 \bmod 4, \\ \frac{3n-1}{4} & \text{if} \ \ n \equiv 3 \bmod 4. \end{cases}$$

The cycle structure of the permutation α has not been completely determined so far. In Example 2.9.9, this permutation is factored into residue class-wise affine involutions which interchange two residue classes each.

The permutation

$$\xi \in \mathrm{RCWA}(\mathbb{F}_2[x]) : \quad P \ \longmapsto \begin{cases} \frac{(x^2+x+1)P}{x^2+1} & \text{if} \ \ P \equiv 0 \qquad \bmod (x^2+1), \\ \frac{(x^2+x+1)P+x}{x^2+1} & \text{if} \ \ P \equiv 1 \qquad \bmod (x^2+1), \\ \frac{(x^2+x+1)P+x^2}{x^2+1} & \text{if} \ \ P \equiv x \qquad \bmod (x^2+1), \\ \frac{(x^2+x+1)P+(x^2+x)}{x^2+1} & \text{if} \ \ P \equiv (x+1) \bmod (x^2+1) \end{cases}$$

fixes the degree of any polynomial. Therefore it has only finite cycles. However it is easy to show that ξ is wild, thus in particular has infinite order. This implies that there is no upper bound on the cycle lengths. The group $\mathrm{RCWA}(\mathbb{Z})$ has also elements of infinite order which have only finite cycles. For an example see Section B.4.

The permutation

$$\sigma_T \in \mathrm{Sym}(\mathbb{Z} \times \mathbb{Z}) : \quad (x, y) \ \longmapsto \begin{cases} \left(\frac{3x+1}{2}, 2y\right) & \text{if} \ \ x \in 1(2), \\ \left(\frac{x}{2}, y\right) & \text{if} \ \ x \in 0(6) \cup 2(6), \\ \left(\frac{x}{2}, 2y+1\right) & \text{if} \ \ x \in 4(6) \end{cases}$$

acts on the x - coordinate as the Collatz mapping T (cp. Example 3.13).

Further examples are discussed in Appendix B.

Zusammenfassung

Motivation

Diese Arbeit ist motiviert durch die

$3n+1$ **- Vermutung:** Iterierte Anwendung der Abbildung

$$T: \mathbb{Z} \longrightarrow \mathbb{Z}, \quad n \longmapsto \begin{cases} \frac{n}{2} & \text{falls } n \text{ gerade,} \\ \frac{3n+1}{2} & \text{falls } n \text{ ungerade} \end{cases}$$

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. Sie läßt sich vermittels Konjugation der Collatz-Abbildung T mit einer Permutation σ von $\mathbb{Z}$, die natürliche Zahlen auf natürliche Zahlen abbildet und die 1 fixiert, in die folgende äquivalente Behauptung überführen:

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

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

Beliebige Permutationen unendlicher Mengen sind sowohl theoretisch als auch algorithmisch schwer zu handhaben. Naheliegend ist der Wunsch, zumindest Permutationen besser zu verstehen, die von ähnlicher Bauart sind wie die Collatz-Abbildung selbst. Hier bietet sich die Klasse der restklassenweise affinen Permutationen an.

J. C. Lagarias hat eine kommentierte Bibliographie [Lag05] zur $3n+1$ - Vermutung verfaßt, die er laufend aktualisiert. In der zur Zeit der Abfassung dieser Arbeit aktuellen Version vom 10. Juli 2005 umfaßt Lagarias' Bibliographie 193 Referenzen.

Keiner der Artikel, auf die dort verwiesen wird, handelt von einem gruppentheoretischen Zugang oder untersucht die Struktur von Gruppen, die von bijektiven restklassenweise affinen – also der 'Collatz - Abbildung ähnlichen' – Abbildungen erzeugt werden.

Zielsetzung

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

Ergebnisse

Es wird gezeigt, daß die Gruppe RCWA($\mathbb{Z}$)

- nicht endlich erzeugt ist (Satz 2.1.1),
- endliche Untergruppen sämtlicher Isomorphietypen besitzt (Satz 2.1.2),
- ein triviales Zentrum hat (Korollar 2.1.6),
- keinen nichttrivialen auflösbaren Normalteiler besitzt (Korollar 2.1.6),
- hoch transitiv auf $\mathbb{Z}$ operiert (Satz 2.1.5) und deshalb nur nichttriviale Normalteiler hat, die ebenfalls hoch transitiv auf $\mathbb{Z}$ operieren (Korollar 2.1.6),
- zu einer Gruppe von Homöomorphismen wird, wenn man $\mathbb{Z}$ durch Wahl der Menge aller Restklassen als Basis mit einer Topologie versieht (Satz 2.2.3),
- zu je zwei Untergruppen stets eine zu deren direktem Produkt isomorphe Untergruppe hat (Korollar 2.3.3),
- transitiv auf der Menge der nichtleeren, von $\mathbb{Z}$ verschiedenen Vereinigungen endlich vieler Restklassen von $\mathbb{Z}$ operiert (Satz 2.4.1),
- zu jeder endlichen Erweiterung $G \trianglerighteq N$ eines subdirekten Produkts N endlich vieler unendlicher Diedergruppen eine isomorphe Untergruppe hat (Korollar 2.6.5),
- nur endlich viele Konjugiertenklassen von Elementen einer gegebenen ungeraden Ordnung, aber unendlich viele von Elementen einer gegebenen geraden Ordnung besitzt (Folgerung 2.7.2),
- einen Normalteiler hat, 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 angegebenen Monomorphismen der Gruppe RCWA($\mathbb{Z}$) in sich selbst (Satz 2.9.4), und
- die Gruppe $\mathbb{Z}^\times$ als epimorphes Bild besitzt (Satz 2.12.8).

Die bis hierher genannten Aussagen werden zum großen Teil allgemeiner formuliert für Gruppen RCWA(R) über jeweils 'geeigneten' euklidischen Ringen R.

Desweiteren wird gezeigt:

- Die Homomorphismen einer gegebenen endlichen Gruppe G ungerader Ordnung nach $\mathrm{RCWA}(\mathbb{Z})$ werden bis auf innere Automorphismen von $\mathrm{RCWA}(\mathbb{Z})$ parametrisiert durch die nichtleeren Teilmengen der Menge der Äquivalenzklassen transitiver endlicher Permutationsdarstellungen von G (Satz 2.6.7).

- Ist $\mathrm{char}(R) = 0$, ist der Exponent der Einheitengruppe von R endlich, und besitzt R einen Restklassenring der Kardinalität 2, dann gilt für einen Normalteiler $N \neq 1$ von $\mathrm{RCWA}(R)$ die folgende Aussage: Es gibt beliebig große $l \in \mathbb{N}$ so, daß N zu jeder Partition $\mathcal{P}$ von R in l Restklassen eine Untergruppe besitzt, die auf $\mathcal{P}$ als volle symmetrische Gruppe operiert (Satz 2.10.6).

- Die Untergruppe $\mathrm{RCWA}^+(\mathbb{Z}) < \mathrm{RCWA}(\mathbb{Z})$ der klassenweise ordnungserhaltenden restklassenweise affinen Bijektionen besitzt $(\mathbb{Z}, +)$ als epimorphes Bild (Satz 2.11.9).

Darüberhinaus wird

- eine bereits 1932 von Lothar Collatz betrachtete restklassenweise affine Permutation mit bislang unbekannter Zykelstruktur in restklassenweise affine Involutionen faktorisiert, die jeweils zwei Restklassen vertauschen (Beispiel 2.9.9),

- gezeigt, daß es keine restklassenweise affine Permutation σ von $\mathbb{Z}$ gibt, die natürliche Zahlen auf natürliche Zahlen abbildet und die 1 fixiert, sodaß T^σ fast überall monoton ist (Satz 3.11 und Bemerkung 3.12), und

- eine Fortsetzung der Collatz-Abbildung zu einer Permutation von $\mathbb{Z}^2$ konstruiert (Beispiel 3.13).

Ausblick und Beispiele

- Abschnitt 2.13 gibt einen Ausblick auf weitere Fragen zur Gruppe $\mathrm{RCWA}(\mathbb{Z})$, die ebenfalls interessant erscheinen und die im Rahmen dieser Arbeit nicht beantwortet werden konnten.

- Anhang A beschreibt Kriterien, um zu entscheiden, ob eine vorgegebene restklassenweise affine Abbildung *zahm* oder *wild* ist, d.h. ob es eine obere Schranke für die Anzahl der affinen Teilabbildungen ihrer Potenzen gibt oder nicht.

- Anhang B ist eine Sammlung von Beispielen restklassenweise affiner Abbildungen und -Gruppen.

Restklassenweise affine Abbildungen und -Gruppen sind rechnerischen Untersuchungen zugänglich. Siehe hierzu das GAP [GAP04] - Package RCWA [Koh05] des Autors. Dieses Package ist erhältlich unter `http://www.gap-system.org/Packages/rcwa.html`.

Danksagungen

Meinem Doktorvater Herrn Prof. Dr. Wolfgang Kimmerle fühle ich mich zu bestem Dank verpflichtet für die Gewährung wertvollen Freiraums zur selbständigen Arbeit über das von mir gewählte Thema.

Herrn Prof. Dr. Wolfgang Rump möchte ich sehr herzlich danken für einen wesentlichen Beitrag zum Beweis von Satz 2.11.9, für seine kenntnisreichen Hinweise und Kommentare, und nicht zu vergessen dafür, daß er stets klar den Standpunkt vertreten hat, daß restklassenweise affine Gruppen ein lohnendes Forschungsthema zu sein versprechen.

Frau Prof. Dr. Bettina Eick möchte ich ebenso herzlich danken dafür, daß sie mir stets mit gutem Rat zur Seite gestanden hat, für ihre vielen nützlichen und hilfreichen Verbesserungsvorschläge zu meinem GAP - Package RCWA, welches ich im Zuge der Anfertigung dieser Arbeit entwickelt habe, sowie – *last but not least* – für so manche aufmunternden und motivierenden Worte.

Ferner gilt mein Dank den zuvor genannten Personen sowie diversen Kollegen insbesondere aus der GAP Group für viele interessante und anregende Diskussionen.

Dem Institut für Geometrie und Topologie möchte ich danken für die Bereitstellung der nötigen Arbeitsmittel sowie für eine angenehme Arbeitsatmosphäre.

Für finanzielle Unterstützung danken möchte ich dem *Centre for Interdisciplinary Research in Computational Algebra* in St Andrews sowie dem Lehrstuhl D für Mathematik der RWTH Aachen.

Mein ganz besonderer Dank gilt meinen Eltern für die Gewährung des nötigen finanziellen Rückhalts während der gesamten Zeit der Erstellung dieser Arbeit.

KAPITEL 1

Einführung

1.1 Grundlagen

Im folgenden wird eine Klasse von Selbstabbildungen von Ringen definiert.

Die Menge dieser Abbildungen zu einem vorgegebenen Ring mit abzählbar vielen Elementen ist abzählbar, und sie ist rechnerischen Untersuchungen in der Regel relativ gut zugänglich.

Zunächst ist festzulegen, was für ein Ring zugrunde gelegt werden soll:

1.1.1 Definition In dieser Arbeit bezeichne R stets einen unendlichen euklidischen Ring, der mindestens ein Primelement enthält und dessen Restklassenringe alle endlich sind.

Ferner sei eine Abbildung $|.| : R \to R$ erklärt, die jedem Element von R ein gewisses 'standard-assoziiertes' Element zuordnet. Im Falle $R = \mathbb{Z}$ sei dies der Absolutbetrag. Größte gemeinsame Teiler und kleinste gemeinsame Vielfache seien mittels $|.|$ normiert.

Nun zu den angekündigten Abbildungen:

1.1.2 Definition 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

$$f|_{r(m)} : \ r(m) \to R, \quad n \ \mapsto \ \frac{a_{r(m)} \cdot n + b_{r(m)}}{c_{r(m)}} \ .$$

Das Ringelement m wird als *Modul* von f bezeichnet. Um zu gewährleisten, daß der Modul durch die Abbildung eindeutig bestimmt ist, wird stets angenommen, daß m multiplikativ minimal gewählt ist und daß $m = |m|$ gilt. Um der Eindeutigkeit der Koeffizienten willen wird desweiteren angenommen, daß $\mathrm{ggT}(a_{r(m)}, b_{r(m)}, c_{r(m)}) = 1$ sowie $c_{r(m)} = |c_{r(m)}|$ gilt.

Für den Modul von f wird die Notation $\mathrm{Mod}(f)$ verwendet. Ferner sei der

- *Multiplikator* $\mathrm{Mult}(f)$ von f definiert als $\operatorname*{kgV}_{r(m)\in R/mR} a_{r(m)}$, der
- *Divisor* $\mathrm{Div}(f)$ von f definiert als $\operatorname*{kgV}_{r(m)\in R/mR} c_{r(m)}$, und die
- *Primteilermenge* $\mathcal{P}(f)$ von f definiert als die Menge der Primteiler von

$$\mathrm{Mod}(f) \cdot \mathrm{Mult}(f) \cdot \mathrm{Div}(f).$$

1.1.3 Beispiele Im folgenden werden einige Beispiele für rcwa-Abbildungen angegeben:

1. Gewissermaßen der Prototyp einer rcwa-Abbildung ist die bereits in der Zusammenfassung genannte Collatz-Abbildung T. Es ist $\mathrm{Mod}(T) = \mathrm{Div}(T) = 2$, $\mathrm{Mult}(T) = 3$ und $\mathcal{P}(T) = \{2, 3\}$. Die Abbildung T ist surjektiv, aber nicht injektiv – ist $n \equiv 2\ (3)$, so ist $T^{-1}(n) = \{(2n-1)/3, 2n\}$.

2. Ein ebenfalls bereits von Lothar Collatz betrachtetes Beispiel einer bijektiven rcwa-Abbildung ist

$$\alpha \in \mathrm{Sym}(\mathbb{Z}) : \quad n \longmapsto \begin{cases} \frac{3n}{2} & \text{falls } n \equiv 0 \bmod 2, \\ \frac{3n+1}{4} & \text{falls } n \equiv 1 \bmod 4, \\ \frac{3n-1}{4} & \text{falls } n \equiv 3 \bmod 4. \end{cases}$$

   Die Permutation α bildet die Restklasse $0(2)$ bijektiv auf $0(3)$, die Restklasse $1(4)$ bijektiv auf $1(3)$ und die Restklasse $3(4)$ bijektiv auf $2(3)$ ab. Es ist $\mathrm{Mod}(\alpha) = \mathrm{Div}(\alpha) = 4$, $\mathrm{Mult}(\alpha) = 3$ und $\mathcal{P}(\alpha) = \{2, 3\}$. Es gilt $\forall n \in \mathbb{Z}\ (-n)^\alpha = -(n^\alpha)$, oder anders ausgedrückt, α zentralisiert die Involution $\varsigma : n \mapsto -n$. Die einzigen Fixpunkte von α sind -1, 0 und 1. Vermutlich besitzt die Permutation α keine endlichen Zykel außer den Transpositionen $\pm(2\ 3)$, den 5-Zykeln $\pm(4\ 6\ 9\ 7\ 5)$ und den 12-Zykeln $\pm(44\ 66\ 99\ 74\ 111\ 83\ 62\ 93\ 70\ 105\ 79\ 59)$.

3. Die Permutation

$$\xi \in \mathrm{Sym}(\mathbb{F}_2[x]) : \quad P \longmapsto \begin{cases} \frac{(x^2+x+1)P}{x^2+1} & \text{falls } P \equiv 0 \quad \bmod (x^2+1), \\ \frac{(x^2+x+1)P+x}{x^2+1} & \text{falls } P \equiv 1 \quad \bmod (x^2+1), \\ \frac{(x^2+x+1)P+x^2}{x^2+1} & \text{falls } P \equiv x \quad \bmod (x^2+1), \\ \frac{(x^2+x+1)P+(x^2+x)}{x^2+1} & \text{falls } P \equiv (x+1) \bmod (x^2+1) \end{cases}$$

   läßt offensichtlich den Grad eines jeden Polynoms fest, und besitzt folglich nur endliche Zykel. Man kann jedoch leicht zeigen, daß die Menge der Zykellängen keine obere Schranke besitzt. Es ist $\mathrm{Mod}(\xi) = \mathrm{Div}(\xi) = x^2+1$, $\mathrm{Mult}(\xi) = x^2+x+1$ und $\mathcal{P}(\xi) = \{x+1, x^2+x+1\}$.

1.1.4 Definition Folgende Schreibweisen betreffend den Grundring R werden in dieser Arbeit immer wieder verwendet:

1. Der Ring R ist nach Definition ein euklidischer Ring, also bekanntermaßen insbesondere ein Hauptidealring sowie ein ZPE-Ring. Die Menge aller Primelemente von R wird mit $\mathbb{P}(R)$ bezeichnet.

2. Restklassen $r(m) \in R/mR$ werden unter mengentheoretischen Gesichtspunkten betrachtet, und für $n \equiv r \mod m$ wird neben der gängigen Abkürzung $n \equiv r \ (m)$ zwecks Betonung des Mengenaspekts auch $n \in r(m)$ geschrieben.

3. Es bezeichne $\mathfrak{R}(m)$ ein Vertretersystem für die Menge der Restklassen (mod m).

4. Der Quotientenkörper von R wird stets bezeichnet mit K.

Zuweilen ist es hilfreich, eine Partialordnung auf R zu erklären. Dies leistet die folgende Definition:

1.1.5 Definition Ein Element $n_1 \in R$ wird als *größer* (bzw. *kleiner*) als ein anderes Element $n_2 \in R$ bezeichnet, wenn $|R/n_1R|$ größer (bzw. kleiner) als $|R/n_2R|$ ist.

Eine Teilmenge $S \subset R$ heiße *beschränkt*, falls es eine Konstante $c \in \mathbb{N}$ so gibt, daß $\forall n \in S \ \ |R/nR| < c$.

Ist $(n_k) \subset R$ eine Folge von Elementen von R so, daß $\lim_{k\to\infty} |R/n_kR| = \infty$, dann wird dies auch abgekürzt als $\lim_{k\to\infty} n_k = \infty$.

Man überzeugt sich leicht davon, daß diese Definitionen im Falle $R = \mathbb{Z}$ nicht im Widerspruch zu den üblichen Definitionen von '$<$', 'beschränkt', etc. stehen.

Die Abbildung $|.|$ für die in dieser Arbeit außer $\mathbb{Z}$ noch explizit verwendeten Grundringe R sei festgelegt wie folgt:

1.1.6 Definition Für $n \in \mathbb{Z}_{(\pi)}$ sei $|n|$ das größte Produkt von Primzahlen $p \in \pi$, welches n teilt, und zu $P \in \mathbb{F}_q[x]$ (q Primzahlpotenz) erhalte man die Normalform $|P|$ mittels Division durch den Leitkoeffizienten.

Aus naheliegenden Gründen benötigt wird die affine Gruppe von R bzw. K:

1.1.7 Definition Das Monoid der affinen Abbildungen des Rings R wird mit $\mathrm{Aff}(R)$ bezeichnet, und die Gruppe der bijektiven affinen Abbildungen (die *affine Gruppe*) von R wird bezeichnet mit $\mathrm{AFF}(R)$. Letztere wird gebildet von den Abbildungen $n \mapsto un + k$, $u \in R^\times$, $k \in R$. Analog dazu wird die affine Gruppe von K mit $\mathrm{AFF}(K)$ bezeichnet, und ihre Elemente werden auch als *Affinitäten* bezeichnet. Wo keine Mißverständnisse zu befürchten sind, werden affine Abbildungen von R bzw. K mit ihren Einschränkungen auf einzelne Restklassen von R identifiziert, und darüber hinaus auch als *affine Teilabbildungen* von rcwa-Abbildungen angesprochen.

Die folgenden Aussagen zu affinen Abbildungen von K werden wiederholt benötigt:

1.1.8 Lemma *Es sei* $\alpha \in \mathrm{AFF}(K) : n \mapsto (an+b)/c,\ a,b,c \in R,\ \mathrm{ggT}(a,b,c) = 1$. *Ferner seien* $r, m \in R$, *und es bezeichne* $r(m)$ *die Restklasse von* r *modulo* m. *Dann gilt:*

1. $\{r^\alpha, am/c\} \subset R \implies r(m)^\alpha = r^\alpha(am/c)$,
2. $r(m)^\alpha \subseteq R \ \wedge\ \{a,c\} \not\subset R^\times \implies \mathrm{ord}(\alpha) = \infty \ \wedge\ \nexists k \in \mathbb{N}:\ r(m)^{\alpha^k} = r(m)$, *sowie*
3. $\alpha \in \mathrm{AFF}(R) \implies r(m) \cap r(m)^\alpha \in \{\emptyset, r(m)\}$.

Beweis:

1. Für $t \in R$ gilt

$$(r+tm)^\alpha \ = \ \frac{a(r+tm)+b}{c} \ = \ \frac{ar+b}{c} + \frac{atm}{c} \ = \ r^\alpha + t \cdot \frac{am}{c},$$

   woraus sich die Behauptung direkt ergibt.

2. Die Abbildung α^k, $k \in \mathbb{N}$ ist gegeben durch $n \mapsto (a^k n + \tilde{b}_k)/c^k$ für geeignetes $\tilde{b}_k$, also sicher nicht gleich der Identität, wenn a oder c keine Einheit ist. Aus $r(m)^\alpha \subseteq R$ folgt $am/c \in R$, also bildet α^k nach Aussage (1) die Restklasse $r(m)$ auf $r^{\alpha^k}(a^k m/c^k)$ ab. Die letztere Restklasse ist höchstens dann gleich $r(m)$, wenn a und c Einheiten sind.

3. Nach Voraussetzung sind $a, c \in R^\times$. Also bildet α nach Aussage (1) die Restklasse $r(m)$ auf die Restklasse $r^\alpha(m)$ ab, welche offenbar entweder gleich ihrem Urbild oder zu ihm disjunkt ist. □

Eine im gegebenen Zusammenhang wichtige Klasse von Teilmengen des Grundrings R ist die der Vereinigungen endlich vieler Restklassen. Der *Chinesische Restsatz* und die vorausgesetzte Endlichkeit aller Restklassenringe von R liefern die folgende Aussage:

1.1.9 Lemma Die Klasse der (mengentheoretischen) Vereinigungen jeweils endlich vieler Restklassen von R ist abgeschlossen bezüglich der Bildung von Vereinigungen, Schnitt- und Differenzmengen.

Partitionen von R in Restklassen lassen sich Partitionen der 1 in Stammbrüche zuordnen:

1.1.10 Lemma Ist $\mathcal{P} = \{r_1(m_1), \dots, r_l(m_l)\}$ eine Partition von R in endlich viele Restklassen, so ist $1 = 1/|R/m_1R| + \cdots + 1/|R/m_lR|$ eine Partition der 1 in Stammbrüche.

Es sei an dieser Stelle daran erinnert, daß eine *Partition* einer Menge in Teilmengen im Unterschied zu einer *Überdeckung* stets eine Zerlegung in *disjunkte* Teilmengen ist.

1.2 Bilder und Urbilder unter rcwa-Abbildungen

Wie sehen Bilder von rcwa-Abbildungen aus, und was läßt sich über Bilder und Urbilder 'geeigneter' Teilmengen von R unter rcwa-Abbildungen sagen? – Antworten auf diese Fragen gibt folgendes Lemma:

1.2.1 Lemma *Es gilt*

1. *Das Bild einer rcwa-Abbildung ist stets die Vereinigung einer endlichen Anzahl von Restklassen und einer endlichen Teilmenge von R.*

2. *Ist $f \in \mathrm{Rcwa}(R)$ auf keiner Restklasse konstant und ist $M \subseteq R$ eine Vereinigung endlich vieler Restklassen, dann sind Bild und Urbild von M unter f ebenfalls Vereinigungen endlich vieler Restklassen.*

Beweis:

1. Es sei $f \in \mathrm{Rcwa}(R)$ und $m := \mathrm{Mod}(f)$. Die Einschränkung von f auf eine Restklasse $r(m) \in R/mR$ sei gegeben durch $n \mapsto (a_{r(m)}n + b_{r(m)})/c_{r(m)}$. Im Falle $a_{r(m)} = 0$ ist $r(m)^f = \{b_{r(m)}\}$, und für $a_{r(m)} \neq 0$ gilt nach Lemma 1.1.8, Aussage (1)

$$r(m)^f \quad = \quad \frac{a_{r(m)} \cdot r + b_{r(m)}}{c_{r(m)}} \quad \left(\frac{a_{r(m)} \cdot m}{c_{r(m)}}\right).$$

   Die Behauptung folgt, da das Bild von f gleich der Vereinigung der Bilder aller Restklassen (mod m) unter f ist, und es nach Voraussetzung an R nur endlich viele verschiedene gibt.

2. Es genügt, die Behauptung für den Fall zu zeigen, daß M nur eine Restklasse umfaßt. Es sei $m := \mathrm{Mod}(f)$. Der Schnitt $M_{r(m)}$ von M mit einer beliebigen Restklasse $r(m)$ ist entweder ebenfalls eine Restklasse oder leer. Gleiches gilt nach Lemma 1.1.8, Aussage (1) für das Bild von $M_{r(m)}$ unter der Einschränkung von f auf $r(m)$.

   Es sei $\tilde{m} := \mathrm{Mult}(f) \cdot m$. Der Schnitt $\tilde{M}_{\tilde{r}(\tilde{m})}$ von M mit einer Restklasse $\tilde{r}(\tilde{m})$ ist entweder ebenfalls eine Restklasse oder leer. Wegen Lemma 1.1.8, Aussage (1) wird jede Restklasse (mod m) unter f auf eine Vereinigung von Restklassen (mod $\tilde{m}$) abgebildet. Daher ist das Urbild der Menge $\tilde{M}_{\tilde{r}(\tilde{m})}$ unter f gleich der Vereinigung ihrer Urbilder unter keiner, einer oder mehrerer affiner Teilabbildungen von f, also leer oder eine Vereinigung endlich vieler Restklassen.

   Die Behauptung folgt wegen der Endlichkeit von R/mR und $R/\tilde{m}R$ nun daraus, daß das Bild (Urbild) von M unter f gleich der Vereinigung der Bilder (Urbilder) der Restklassen $M_{r(m)}$ ($\tilde{M}_{\tilde{r}(\tilde{m})}$) unter f ist. □

1.2.2 Beispiel Es sollen Bild und Urbild der Restklasse 0(5) unter der Collatz-Abbildung T bestimmt werden. In der Terminologie aus dem Beweis von Lemma 1.2.1, Aussage (2) ist $M = 0(5)$, $M_{0(2)} = M \cap 0(2) = 0(10)$ und $M_{1(2)} = M \cap 1(2) = 5(10)$. Es folgt ${M_{0(2)}}^T = 0(10)/2 = 0(5)$ und ${M_{1(2)}}^T = (3 \cdot 5(10) + 1)/2 = 8(15)$, und somit $M^T = {M_{0(2)}}^T \cup {M_{1(2)}}^T = 0(5) \cup 8(15)$.

Die Bestimmung des Urbildes ist schon ein wenig mühsamer: schneidet man M jeweils mit einer der Restklassen (mod $\tilde{m} = \mathrm{Mult}(T) \cdot \mathrm{Mod}(T) = 6$), so erhält man die Mengen $\tilde{M}_{0(6)} = 0(30)$, $\tilde{M}_{1(6)} = 25(30)$, $\tilde{M}_{2(6)} = 20(30)$, $\tilde{M}_{3(6)} = 15(30)$, $\tilde{M}_{4(6)} = 10(30)$ und $\tilde{M}_{5(6)} = 5(30)$. Deren Urbilder kann man nun wieder Teilabbildung für Teilabbildung bestimmen (Vorsicht: T ist nicht injektiv – man muß für $\tilde{r} \equiv 2$ (3) beide Teilabbildungen berücksichtigen). Es ergeben sich auf diese Weise die Urbildmengen $2 \cdot 0(30) = 0(60)$, $2 \cdot 25(30) = 50(60)$, $2 \cdot 20(30) \cup (2 \cdot 20(30) - 1)/3 = 40(60) \cup 13(20)$, $2 \cdot 15(30) = 30(60)$, $2 \cdot 10(30) = 20(60)$ und $2 \cdot 5(30) \cup (2 \cdot 5(30) - 1)/3 = 10(60) \cup 3(20)$. Das volle Urbild der Restklasse 0(5) unter T ist schließlich deren Vereinigung, also $0(10) \cup 3(10)$.

Es wird sich im weiteren Verlauf der Arbeit häufig als nützlich erweisen, eine der folgenden Eigenschaften des Grundrings R vorauszusetzen:

1.2.3 Definition Der Ring R besitze die

- *schwache Restklassenteilbarkeitseigenschaft*, sofern er einen Restklassenring der Kardinalität 2 besitzt, und die
- *starke Restklassenteilbarkeitseigenschaft*, wenn er sogar Restklassenringe jeder von 0 verschiedenen endlichen Kardinalität besitzt.

Diese Bezeichnungen bedürfen natürlich einer Rechtfertigung:

1.2.4 Bemerkung Der Ring R besitzt genau dann die schwache Restklassenteilbarkeitseigenschaft, wenn sich jede Restklasse von R als disjunkte Vereinigung zweier anderer Restklassen schreiben läßt.

Besitzt R die schwache Restklassenteilbarkeitseigenschaft, so folgt induktiv, daß sich eine disjunkte Vereinigung von k Restklassen von R auch als disjunkte Vereinigung einer beliebigen Anzahl $\tilde{k} > k$ von Restklassen von R schreiben läßt.

Die starke Restklassenteilbarkeitseigenschaft ist äquivalent zu der Bedingung, daß sich jede Restklasse in eine beliebige Anzahl disjunkter anderer Restklassen gleichen Moduls zerlegen läßt.

1.2.5 Beispiele Die Ringe $\mathbb{Z}$, $\mathbb{Z}_{(\pi)}$ mit $2 \in \pi$, der Ring der Gauß'schen ganzen Zahlen und $\mathbb{F}_2[x]$ zum Beispiel besitzen die schwache Restklassenteilbarkeitseigenschaft. Zum Beispiel läßt sich in $\mathbb{F}_2[x]$ eine Restklasse $a(m)$ schreiben als Vereinigung von $a(x \cdot m)$ und $a + m(x \cdot m)$. Die Ringe $\mathbb{Z}_{(\pi)}$ mit $2 \notin \pi$ und $\mathbb{F}_q[x]$ mit $q \neq 2$ besitzen diese Eigenschaft hingegen nicht. Der Ring $\mathbb{Z}$ besitzt sogar die starke Restklassenteilbarkeitseigenschaft.

1.3 Komposita und Inverse von rcwa-Abbildungen

Das Thema dieser Arbeit sind restklassenweise affine *Gruppen*.

Aber bilden die bijektiven restklassenweise affinen Abbildungen des Rings R überhaupt eine Gruppe? – Dies soll in diesem Abschnitt geklärt werden.

Außerdem soll untersucht werden, wie Modul, Multiplikator und Divisor des Produkts zweier rcwa-Abbildungen von Modul, Multiplikator und Divisor der Faktoren abhängen, und welchen Einfluß die Inversion einer bijektiven rcwa-Abbildung auf diese Größen hat.

1.3.1 Lemma *(Komposita und Inverse von rcwa-Abbildungen.)*

a) Sind f und g rcwa-Abbildungen eines Rings R, so ist $f \cdot g$ (f wird zuerst angewandt) ebenfalls eine rcwa-Abbildung von R, und es gilt

1. $\mathrm{Div}(f) | \mathrm{Mod}(f)$,
2. $\mathrm{Mod}(f \cdot g) | \mathrm{Mod}(f) \cdot \mathrm{Mod}(g)$ *sowie* $\mathrm{Mod}(f \cdot g) | \mathrm{Div}(f) \cdot \mathrm{kgV}(\mathrm{Mod}(f), \mathrm{Mod}(g))$,
3. $\forall k \in \mathbb{N} \ \ \mathrm{Mod}(f^k) | \mathrm{Div}(f)^{k-1} \cdot \mathrm{Mod}(f)$,
4. $\mathrm{Mult}(f \cdot g) | \mathrm{Mult}(f) \cdot \mathrm{Mult}(g)$,
5. $\mathrm{Div}(f \cdot g) | \mathrm{Div}(f) \cdot \mathrm{Div}(g)$, *und*
6. $\mathcal{P}(f \cdot g) \subseteq \mathcal{P}(f) \cup \mathcal{P}(g)$.

b) Ist σ eine bijektive rcwa-Abbildung von R, so auch σ^{-1}. Ist ferner die Einschränkung von σ auf eine Restklasse $r(m)$ gegeben durch $n \mapsto (a_{r(m)} \cdot n + b_{r(m)})/c_{r(m)}$, dann gilt

1. $\mathrm{Mod}(\sigma^{-1}) | (\mathrm{Mult}(\sigma) \cdot \mathrm{Mod}(\sigma)) / \mathrm{ggT}_{r(m) \in R/mR} \, c_{r(m)}$,
2. $\mathrm{Mult}(\sigma) | \mathrm{Mod}(\sigma^{-1})$,
3. $\mathrm{Mult}(\sigma^{-1}) = \mathrm{Div}(\sigma)$,
4. $\mathrm{Div}(\sigma^{-1}) = \mathrm{Mult}(\sigma)$, *und*
5. $\mathcal{P}(\sigma^{-1}) = \mathcal{P}(\sigma)$.

c) Sind f, σ, σ_1 und σ_2 rcwa-Abbildungen von R und sind σ, σ_1 und σ_2 bijektiv, so gilt

1. $\mathrm{Mod}(f^\sigma) | \mathrm{Mult}(\sigma) \cdot \mathrm{Mod}(\sigma)^2 \cdot \mathrm{Mod}(f)$, *und*
2. $\mathrm{Mod}([\sigma_1, \sigma_2]) | \mathrm{Mult}(\sigma_1) \cdot \mathrm{Mult}(\sigma_2) \cdot \mathrm{Mod}(\sigma_1)^2 \cdot \mathrm{Mod}(\sigma_2)^2$.

Beweis:

a) Es seien f und g rcwa-Abbildungen des Rings R. Ferner sei $m_f := \mathrm{Mod}(f)$ und $m_g := \mathrm{Mod}(g)$.

Das Kompositum je einer affinen Teilabbildung von f und g ist stets wieder affin. Welche beiden affinen Teilabbildungen bei der Auswertung von $n^{f \cdot g}$ hintereinander angewandt werden, hängt nur von n mod $(m_f \cdot \mathrm{Div}(f) \cdot m_g)$ ab. Ferner ist das Produkt $m_f \cdot \mathrm{Div}(f) \cdot m_g$ ungleich 0, da R nach Voraussetzung nullteilerfrei ist. Folglich ist das Kompositum $f \cdot g$ ebenfalls eine rcwa-Abbildung.

Es seien $a, b, c \in R$. Nach Lemma 1.1.8, Aussage (1) ist das Bild einer Restklasse $r(m_f) \in R/m_fR$ unter der Abbildung $n \mapsto a \cdot n + b$ die Restklasse $a \cdot r + b(a \cdot m_f)$. Diese ist höchstens dann Teilmenge von $0(c)$, wenn $c|a \cdot m_f$. Sind a und c teilerfremd, so erfordert dies $c|m_f$. Es gilt also (1).

Es sei $m_{fg} := \mathrm{Mod}(f \cdot g)$. Es ist zu zeigen, daß sowohl $m_{fg}|(m_f \cdot m_g)$ als auch $m_{fg}|\,\mathrm{Div}(f) \cdot \mathrm{kgV}(m_f, m_g)$ (2). Ein Element $m \in R$ ist Vielfaches von m_{fg}, wenn $m_f|m$, und wenn nur von n mod m abhängt, in welcher Restklasse (mod m_g) das Bild von n unter f liegt. Welche affine Teilabbildung von f auf n angewandt wird, hängt definitionsgemäß nur von n mod m_f ab, und in welcher Restklasse (mod m_g) das Bild von n unter einer festen affinen Teilabbildung von f liegt, wird bestimmt durch n mod $(\mathrm{Div}(f) \cdot m_g)$. Somit gilt $m_{fg}|\,\mathrm{kgV}(m_f, \mathrm{Div}(f) \cdot m_g)$, und mithin die zweite der behaupteten Teilbarkeitsbeziehungen. Wegen $\mathrm{Div}(f)|m_f$ (Aussage (1)) gilt auch die erste. Im Fall $g = f$ ergibt sich aus $m_{fg}|\,\mathrm{Div}(f) \cdot \mathrm{kgV}(m_f, m_g)$ induktiv sofort Aussage (3).

Die Abbildungen f und g seien gegeben durch

$$n^f = \frac{a_{r(m_f)} \cdot n + b_{r(m_f)}}{c_{r(m_f)}} \quad \text{für } n \in r(m_f), \text{ wobei } r(m_f) \in R/m_fR, \quad \text{und}$$

$$n^g = \frac{\tilde{a}_{r(m_g)} \cdot n + \tilde{b}_{r(m_g)}}{\tilde{c}_{r(m_g)}} \quad \text{für } n \in r(m_g), \text{ wobei } r(m_g) \in R/m_gR.$$

Es gilt

$$n^{f \cdot g} = \frac{a_{r_1(m_f)}\tilde{a}_{r_2(m_g)}n + (\tilde{a}_{r_2(m_g)}b_{r_1(m_f)} + \tilde{b}_{r_2(m_g)}c_{r_1(m_f)})}{c_{r_1(m_f)}\tilde{c}_{r_2(m_g)}}$$

für $r_1(m_f) \in R/m_fR$ und $r_2(m_g) \in R/m_gR$ abhängig von n mod m_{fg}, woran sich die Aussagen $\mathrm{Mult}(f \cdot g)|\,\mathrm{Mult}(f) \cdot \mathrm{Mult}(g)$ (4) und $\mathrm{Div}(f \cdot g)|\,\mathrm{Div}(f) \cdot \mathrm{Div}(g)$ (5) direkt ablesen lassen. Die Aussage (6) zur Primteilermenge von $f \cdot g$ ergibt sich jetzt sofort aus deren Definition.

b) Es sei σ eine bijektive rcwa-Abbildung von R und $m := \mathrm{Mod}(\sigma)$.

Die Inverse von σ setzt sich aus den Umkehrabbildungen der Einschränkungen $\sigma|_{r(m)}$ von σ auf die Restklassen (mod m) zusammen. Deren Definitionsbereiche sind die Bilder der Restklassen $r(m) \in R/mR$ unter σ. Diese sind wegen (a.1) nach Lemma 1.1.8, Aussage (1) ebenfalls Restklassen. Die Abbildung σ^{-1} ist folglich wie behauptet restklassenweise affin.

Der Modul von σ^{-1} teilt offenbar das kleinste gemeinsame Vielfache der Moduln der Restklassen $r(m)^\sigma$. Ist

$$\sigma|_{r(m)}: \quad n \longmapsto \frac{a_{r(m)} \cdot n + b_{r(m)}}{c_{r(m)}},$$

dann gilt nach Lemma 1.1.8, Aussage (1)

$$r(m)^\sigma \quad = \quad \frac{a_{r(m)} r + b_{r(m)}}{c_{r(m)}} \left(\frac{a_{r(m)} \cdot m}{c_{r(m)}} \right).$$

Es folgt Aussage (1). Ferner ist

$$\sigma^{-1}|_{r(m)^\sigma}: \quad n \longmapsto \frac{c_{r(m)} \cdot n - b_{r(m)}}{a_{r(m)}}.$$

Daran läßt sich direkt ablesen, daß Multiplikator und Divisor durch Inversenbildung miteinander vertauscht werden (Aussagen (3) und (4)). Aussage (2) ist unmittelbare Konsequenz aus (4) und (a.1). Es folgt ebenfalls sofort, daß $\mathcal{P}(\sigma^{-1}) \subseteq \mathcal{P}(\sigma)$. Da die Überlegungen allesamt gültig bleiben, wenn man die Rollen von σ und σ^{-1} vertauscht, folgt die in (5) behauptete Gleichheit.

c) Es seien σ, σ_1 und σ_2 bijektive rcwa-Abbildungen des Rings R, und es sei f irgendeine rcwa-Abbildung von R. Mittels (a.2) und (b.1) erhält man die Teilerkette

$$\mathrm{Mod}(f^\sigma) \mid \mathrm{Mod}(\sigma^{-1}) \cdot \mathrm{Mod}(f) \cdot \mathrm{Mod}(\sigma) \mid \mathrm{Mult}(\sigma) \cdot \mathrm{Mod}(\sigma)^2 \cdot \mathrm{Mod}(f),$$

also Aussage (1). Ebenso schließt man via

$$\begin{aligned} \mathrm{Mod}([\sigma_1, \sigma_2]) &\mid \mathrm{Mod}(\sigma_1^{-1}) \cdot \mathrm{Mod}(\sigma_2^{-1}) \cdot \mathrm{Mod}(\sigma_1) \cdot \mathrm{Mod}(\sigma_2) \\ &\mid \mathrm{Mult}(\sigma_1) \cdot \mathrm{Mult}(\sigma_2) \cdot \mathrm{Mod}(\sigma_1)^2 \cdot \mathrm{Mod}(\sigma_2)^2 \end{aligned}$$

auf Aussage (2). □

1.3.2 Beispiele Ist T die Collatz-Abbildung und α wie in Beispiele 1.1.3, dann ist

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

Der Leser kann die Gültigkeit der Aussagen von Lemma 1.3.1 in diesen Beispielen anhand folgender Tabelle sofort verifizieren:

f	α	α^{-1}	T	$\alpha^{-1} \cdot T$
$\mathrm{Mod}(f)$	4	3	2	3
$\mathrm{Mult}(f)$	3	4	3	2
$\mathrm{Div}(f)$	4	3	2	3
$\mathcal{P}(f)$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$

1.3.3 Definition Es bezeichne

- $\mathrm{Rcwa}(R)$ die Menge aller rcwa-Abbildungen des Rings R, und
- $\mathrm{RCWA}(R)$ die Menge aller bijektiven rcwa-Abbildungen des Rings R.

1.3.4 Lemma *Es gilt:*

1. *Die Menge* $\mathrm{Rcwa}(R)$ *bildet bezüglich Komposition von Abbildungen ein Monoid.*
2. *Die Menge* $\mathrm{RCWA}(R)$ *bildet bezüglich Komposition von Abbildungen eine echte Untergruppe von* $\mathrm{Sym}(R)$.
3. *Die Kardinalitäten der Mengen R,* $\mathrm{Rcwa}(R)$ *und* $\mathrm{RCWA}(R)$ *sind gleich.*

Beweis:

1. Da die Identität eine rcwa-Abbildung ist, folgt die Aussage direkt aus Lemma 1.3.1a.
2. Die Untergruppeneigenschaft ist eine triviale Konsequenz aus Lemma 1.3.1. Echt ist die Untergruppe bereits aus Kardinalitätsgründen: Die Mengen R und $\mathrm{RCWA}(R)$ haben nach Aussage (3) dieselbe Kardinalität, diejenige von $\mathrm{Sym}(R)$ ist jedoch bekanntlich größer.
3. Zu jedem $y \in R$ ist durch $x \mapsto x + y$ eine bijektive rcwa-Abbildung gegeben. Die Mengen $\mathrm{Rcwa}(R)$ und $\mathrm{RCWA}(R)$ haben somit keine kleinere Kardinalität als R. Da jede rcwa-Abbildung von R durch endlich viele Koeffizienten aus R bestimmt wird und vorausgesetzt wurde, daß R unendlich ist, besitzen sie auch keine größere. □

1.4 Rcwa-Gruppen und -Monoide

1.4.1 Definition Ein Untermonoid von $\mathrm{Rcwa}(R)$ werde bezeichnet als *restklassenweise affines* Monoid über R. Entsprechend heiße eine Untergruppe von $\mathrm{RCWA}(R)$ *restklassenweise affine* Gruppe über R. Abkürzend werden auch die Begriffe *rcwa-Monoid* bzw. *rcwa-Gruppe* verwendet.

Es sei an dieser Stelle daran erinnert, daß jede Gruppe insbesondere auch ein Monoid, also eine Halbgruppe mit Einselement ist. Der Ausdruck *Monoid* wird im folgenden daher stets als Oberbegriff verwendet.

Die Begriffe *Modul*, *Multiplikator*, *Divisor* und *Primteilermenge* lassen sich in natürlicher Weise auf rcwa-Gruppen und -Monoide übertragen:

1.4.2 Definition Es seien *Modul*, *Multiplikator* und *Divisor* eines rcwa-Monoids definiert als das kleinste gemeinsame Vielfache der Moduln, Multiplikatoren bzw. Divisoren seiner Elemente. Gibt es kein endliches kleinstes gemeinsames Vielfaches, so nimmt man in ersterem Fall an seiner Statt den Wert 0 und in den letzteren beiden Fällen den Wert ∞. Die *Primteilermenge* $\mathcal{P}(G)$ eines rcwa-Monoids G sei die Vereinigung der Primteilermengen seiner Elemente.

1.4.3 Lemma *Für rcwa-Monoide* $G, H \leqslant \mathrm{Rcwa}(R)$ *und* $\sigma \in \mathrm{RCWA}(R)$ *gilt*

1. *G ist rcwa-Gruppe* $\Rightarrow \mathrm{Mult}(G) \,|\, \mathrm{Mod}(G)$,
2. $\mathrm{Div}(G) \,|\, \mathrm{Mod}(G)$,
3. $H \leqslant G \Rightarrow \mathrm{Mod}(H) \,|\, \mathrm{Mod}(G)$,
4. $H \leqslant G \Rightarrow \mathcal{P}(H) \subseteq \mathcal{P}(G)$,
5. *G ist rcwa-Gruppe* $\Rightarrow \mathrm{Mult}(G) = \mathrm{Div}(G)$,
6. *G ist rcwa-Gruppe* $\Rightarrow \mathcal{P}(G)$ *ist die Menge der Primteiler von* $\mathrm{Mod}(G)$, *und*
7. $\mathrm{Mod}(G^\sigma) \,|\, \mathrm{Mult}(\sigma) \cdot \mathrm{Mod}(\sigma)^2 \cdot \mathrm{Mod}(G)$.

Es sei hierbei $0|0$ *und* $\infty|0$.

Beweis: Aussage (2) folgt direkt aus Lemma 1.3.1a, Aussage (1) und der Definition des Divisors und des Moduls eines rcwa-Monoids. Aussage (1) erhält man, wenn man noch Lemma 1.3.1b, Aussage (2) hinzuzieht. Die Aussagen (3) und (4) ergeben sich unmittelber aus der Definition des Moduls bzw. der Primteilermenge eines rcwa-Monoids. Aussage (5) folgt aus Lemma 1.3.1b, Aussage (3) und (4), und Aussage (6) aus (1) und (2) sowie der Definition der Primteilermenge einer rcwa-Gruppe. Aussage (7) schließlich ist unmittelbare Konsequenz von Lemma 1.3.1c, Aussage (1). □

1.5 Rcwa-Darstellungen von Gruppen

Es sei $\mathbb{K}$ eine Kategorie. Unter einer $\mathbb{K}$-Darstellung einer Gruppe G versteht man allgemein einen Homomorphismus

$$\varphi: \ G \ \longrightarrow \ \mathrm{Aut}_{\mathbb{K}}(X)$$

für ein Objekt X von $\mathbb{K}$. In der Darstellungstheorie ist $\mathbb{K}$ in der Regel die Kategorie der endlichdimensionalen Vektorräume über einem Körper oder die der endlichdimensionalen Moduln über einem Ring. Der folgende Darstellungsbegriff fügt sich ebenfalls nahtlos in die kategorientheoretische Definition:

1.5.1 Definition Es sei G eine Gruppe. Ein Homomorphismus $\varphi : G \rightarrow \mathrm{RCWA}(R)$ heiße eine *restklassenweise affine Darstellung*, oder kurz *rcwa-Darstellung*, von G über R. rcwa-Darstellungen über $\mathbb{Z}$ werden auch als *ganzzahlig* bezeichnet.

1.5.2 Beispiele Diese Definition soll durch ein paar Beispiele illustriert werden:

1. Nachrechnen zeigt, daß eine treue rcwa-Darstellung der 3-Sylowgruppe

$$G = \langle (1,2,3)(4,6,5)(7,8,9), (1,4,7)(2,5,8)(3,6,9) \rangle$$

von S_9 gegeben ist durch

$$\begin{aligned} \varphi: \ G \ &\longrightarrow \ \mathrm{RCWA}(\mathbb{Z}), \\ (1,2,3)(4,6,5)(7,8,9) \ &\longmapsto \ \left(s_1 : \ n \mapsto \begin{cases} n & \text{falls} \ \ n \in 0(3) \cup 2(3), \\ n+6 & \text{falls} \ \ n \in 1(9), \\ n-3 & \text{falls} \ \ n \in 4(9) \cup 7(9). \end{cases} \right), \\ (1,4,7)(2,5,8)(3,6,9) \ &\longmapsto \ \left(s_2 : \ n \mapsto \begin{cases} n & \text{falls} \ \ n \in 0(9) \cup 6(9), \\ 3n+18 & \text{falls} \ \ n \in 1(9), \\ n+2 & \text{falls} \ \ n \in 2(9) \cup 5(9), \\ \frac{n+3}{3} & \text{falls} \ \ n \in 3(9), \\ 3n-9 & \text{falls} \ \ n \in 4(9) \cup 7(9), \\ n-7 & \text{falls} \ \ n \in 8(9). \end{cases} \right). \end{aligned}$$

Es ist $\mathrm{Mod}(G^\varphi) = 27$, $\mathrm{Mult}(G^\varphi) = \mathrm{Div}(G^\varphi) = 3$, und $\mathcal{P}(G^\varphi) = \{3\}$.

2. Definiert man $\nu_{1(4)}, \nu_{3(4)} \in \mathrm{RCWA}(\mathbb{Z})$ durch

$$n \mapsto \begin{cases} n+4 & \text{falls} \ \ n \in 1(4), \\ n & \text{sonst}, \end{cases} \quad \text{bzw.} \quad n \mapsto \begin{cases} n+4 & \text{falls} \ \ n \in 3(4), \\ n & \text{sonst} \end{cases}$$

und übernimmt die Abbildung α aus Beispiele 1.1.3, dann ist die rcwa-Darstellung

$$\varphi: \ \mathrm{S}_{10} \to \mathrm{RCWA}(\mathbb{Z}), \quad (1\ 2\ 3\ 4\ 6\ 8) \mapsto [\alpha, \nu_{1(4)}\alpha], \quad (3\ 5\ 7\ 6\ 9\ 10) \mapsto [\alpha, \nu_{3(4)}\alpha],$$

wie man mit RCWA leicht nachrechnet, treu.

Es ist $\mathrm{Mod}([\alpha, \nu_{1(4)}\alpha]) = \mathrm{Mod}([\alpha, \nu_{3(4)}\alpha]) = 18$. Der Kommutator $[\alpha, \nu_{1(4)}\alpha]$ ist gegeben durch

$$n \longmapsto \begin{cases} n & \text{falls } n \in 0(9) \cup 2(9) \cup 3(9) \cup 8(9), \\ n+3 & \text{falls } n \in 4(9) \cup 7(9), \\ 2n-5 & \text{falls } n \in 1(9), \\ 2n-4 & \text{falls } n \in 5(9), \\ \frac{n+2}{2} & \text{falls } n \in 6(18), \\ \frac{n-5}{2} & \text{falls } n \in 15(18). \end{cases}$$

Es ist $\mathrm{Mod}(\mathrm{S}_{10}^{\varphi}) = 18$, $\mathrm{Mult}(\mathrm{S}_{10}^{\varphi}) = \mathrm{Div}(\mathrm{S}_{10}^{\varphi}) = 2$, und $\mathcal{P}(\mathrm{S}_{10}^{\varphi}) = \{2, 3\}$.

3. Es sei $F := \langle g_i, \ i \in \mathbb{N} \rangle$ die freie abelsche Gruppe von abzählbar unendlichem Rang. Dann ist

$$\varphi: \ F \ \to \ \mathrm{RCWA}(\mathbb{Z}), \quad g_i \ \mapsto \ \left(h_i: \ \mathbb{Z} \to \mathbb{Z}, \ n \mapsto \begin{cases} n + 2^i & \text{falls } \ n \equiv 2^{i-1} \ (2^i), \\ n & \text{sonst} \end{cases} \right)$$

eine treue rcwa-Darstellung von F. Es ist $\mathrm{Mod}(F^{\varphi}) = 0$, $\mathrm{Mult}(F^{\varphi}) = \mathrm{Div}(F^{\varphi}) = 1$, und $\mathcal{P}(F^{\varphi}) = \{2\}$.

1.6 Transitionsgraphen von rcwa-Abbildungen

Es wird sich im weiteren Verlauf als sehr nützlich erweisen, rcwa-Abbildungen auf folgende Weise gerichtete Graphen zuzuordnen:

1.6.1 Definition Es sei $f \in \mathrm{Rcwa}(R)$ und $m \in R \backslash \{0\}$. Der *Transitionsgraph* $\Gamma_{f,m}$ *von* f *zum Modul* m sei definiert wie folgt:

- Die Knoten sind die Restklassen (mod m).
- Es geht genau dann eine Kante von $r_1(m)$ nach $r_2(m)$, wenn es ein $n \in r_1(m)$ mit $n^f \in r_2(m)$ gibt.

Damit ist $\Gamma_{f,m}$ ein gerichteter, i.a. nicht schlingenfreier Graph. Im Falle $m = \mathrm{Mod}(f)$ wird $\Gamma_{f,m}$ auch abgekürzt als Γ_f.

Die folgenden elementaren Eigenschaften erschließt man direkt aus der Definition:

1.6.2 Lemma Es sei $f \in \mathrm{Rcwa}(R)$, $\sigma \in \mathrm{RCWA}(R)$ und $m, m_1, m_2 \in R$. Dann gilt:

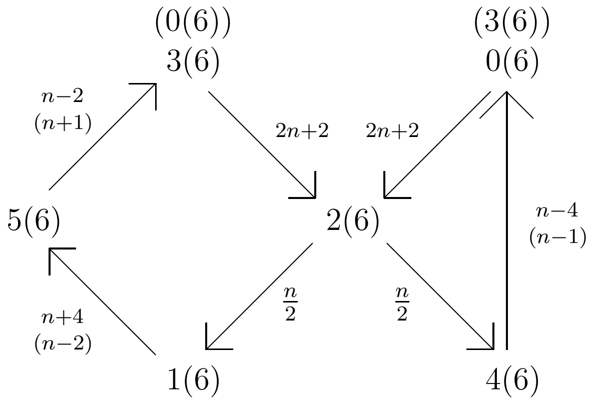
1. Jeder Knoten des Graphen $\Gamma_{f,m}$ besitzt eine herausgehende Kante. Ist f surjektiv, so besitzt außerdem jeder Knoten von $\Gamma_{f,m}$ auch eine hineingehende Kante.

2. Der Graph Γ_{f,m_1} ist der Quotient von $\Gamma_{f,m_1 \cdot m_2}$ nach der durch Kongruenz (mod m_1) induzierten Äquivalenzrelation auf der Knotenmenge.

3. Der Graph $\Gamma_{\sigma^{-1},m}$ entsteht aus $\Gamma_{\sigma,m}$ durch Umkehren aller Kanten.

1.6.3 Beispiel Der untenstehende Graph ist u.a. Transitionsgraph einer rcwa-Abbildung g der Ordnung 7 und einer rcwa-Abbildung h der Ordnung 12 (jeweils zum Modul 6).

Die Knoten und die zugehörigen affinen Teilabbildungen von h sind, sofern sie sich von denen von g unterscheiden, in Klammern angegeben. Aus satztechnischen Gründen seien hier und in allen weiteren Darstellungen von Transitionsgraphen affine Abbildungen $n \mapsto (an + b)/c$ abgekürzt mit $(an + b)/c$.



Dieser Graph besitzt je einen Zyklus der Länge 3 und einen der Länge 4. Bei iterierter Anwendung der Abbildung g werden beide Zyklen stets hintereinander 'durchlaufen', bei derjenigen von h hingegen wird, abhängig vom Startwert, entweder nur der eine oder nur der andere Zyklus 'durchlaufen'. Die Ordnung von g ist daher $3 + 4 = 7$, und h hat Ordnung $\mathrm{kgV}(3, 4) = 12$. Ferner sieht man insbesondere, daß es möglich ist, einen 7-Zykel in eine rcwa-Abbildung mit Modul 6 'hineinzutwisten'.

Wesentlich kompliziertere Beispiele für Transitionsgraphen von rcwa-Abbildungen finden sich in Anhang B.

Man kann nicht nur Transitionsgraphen zu gegebenen Abbildungen bestimmen.

Wenn man eine Abbildung mit bestimmten Eigenschaften konstruieren möchte, ist es häufig auch sehr hilfreich, einen solchen Graphen vorzugeben und anschließend dessen Kanten bzw. Knoten affine Abbildungen zuzuordnen:

1.6.4 Beispiel Es soll eine Permutation $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ der Ordnung 257 mit Modul 32 konstruiert werden.

Hierzu sei $\Gamma_{\sigma,32}$ ein gerichteter Graph mit 32 Knoten $0(32), \dots, 31(32)$, 15 Zyklen der Länge 16 und einem Zyklus der Länge 17. Es sollen 15 Knoten von $\Gamma_{\sigma,32}$ zu allen Zyklen gleichermaßen, 15 Knoten ausschließlich zu je einem der Zyklen der Länge 16 und 2 Knoten ausschließlich zu dem Zyklus der Länge 17 gehören.

Die Permutation σ gewinnt man, indem man den Kanten bzw. Knoten dieses Graphen affine Abbildungen zuordnet. Diese seien so gewählt, daß ein Zykel der Permutation σ stets alle Zyklen von $\Gamma_{\sigma,32}$ hintereinander durchläuft. Die Länge eines solchen Zykels ist dann $15 \cdot 16 + 17 = 257$. Man kann auf diese Weise zum Beispiel die folgende Abbildung konstruieren:

$$\sigma \in \mathrm{RCWA}(\mathbb{Z}), \quad n \longmapsto \begin{cases} 16n+2 & \text{falls } n \in 0(32), \\ 16n+18 & \text{falls } n \in 1(2) \setminus -1(32), \\ n-31 & \text{falls } n \in -1(32), \\ \frac{n}{16} & \text{falls } n \in 16(32), \\ n+16 & \text{falls } n \in 2(32) \cup 4(32) \cup 6(32) \cup \dots \cup 14(32), \\ n-14 & \text{falls } n \in 18(32) \cup 20(32) \cup 22(32) \cup \dots \cup 30(32). \end{cases}$$

Man sieht also, daß die Ordnung eines Elements $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ auch eine Primzahl sein kann, die beträchtlich größer ist als $\mathrm{Mod}(\sigma)$.

1.7 Ganze, ausbalancierte und klassenweise ordnungserhaltende Abbildungen

1.7.1 Definition Eine rcwa-Abbildung $f \in \mathrm{Rcwa}(R)$ heiße

- *ganz*, falls $\mathrm{Div}(f) = 1$,
- *ausbalanciert*, falls die Mengen der Primteiler von $\mathrm{Mult}(f)$ und $\mathrm{Div}(f)$ gleich sind, und
- *klassenweise ordnungserhaltend*, wenn R angeordnet ist und alle affinen Teilabbildungen von f ordnungserhaltend sind.

Ein rcwa-Monoid heiße ganz, ausbalanciert bzw. klassenweise ordnungserhaltend, sofern alle seine Elemente die jeweilige Eigenschaft besitzen. Die von den bijektiven klassenweise ordnungserhaltenden Abbildungen gebildete Untergruppe von $\mathrm{RCWA}(R)$ werde bezeichnet mit $\mathrm{RCWA}^+(R)$.

1.7.2 Bemerkung Ganze rcwa-Abbildungen sind solche, die 'keine Brüche beinhalten'. Sie besitzen mithin eine besonders übersichtliche Struktur. Einfache Dichteargumente zeigen, daß eine surjektive ganze rcwa-Abbildung sogar bijektiv ist, und daß der Multiplikator einer bijektiven ganzen rcwa-Abbildung ebenfalls gleich 1 ist. Die bijektiven ganzen rcwa-Abbildungen bilden mithin wegen Lemma 1.3.1, Aussage (a.4), (a.5), (b.3) und (b.4) eine Untergruppe von $\mathrm{RCWA}(R)$. Potenzieren einer ganzen rcwa-Abbildung vergrößert nach Lemma 1.3.1a, Aussage (3) den Modul nicht.

Ausbalanciertheit ist eine wesentlich schwächere Eigenschaft als Ganzheit. Es wird sich herausstellen, daß sie unter anderem eine notwendige Bedingung dafür ist, daß die Menge der Moduln der Potenzen einer gegebenen rcwa-Abbildung beschränkt ist.

Eine rcwa-Abbildung von $\mathbb{Z}$ ist genau dann klassenweise ordnungserhaltend, wenn ihre affinen Teilabbildungen ordnungserhaltend, also von der Form $n \mapsto (an+b)/c$ mit $a > 0$ sind.

1.7.3 Bemerkung Die Gruppe $\mathrm{RCWA}^+(\mathbb{Z})$ ist kein Normalteiler von $\mathrm{RCWA}(\mathbb{Z})$:

Zum Beispiel ist die Abbildung $\nu^{\varsigma_{0(2)}}$ mit $\nu : n \mapsto n+1$ und $\varsigma_{0(2)} : n \mapsto (-1)^{n+1} \cdot n$ gegeben durch $n \mapsto -n + (-1)^n$. Sie ist also im Gegensatz zu ν selbst nicht klassenweise ordnungserhaltend.

1.8 Ein Zahmheitsbegriff für rcwa-Abbildungen und -Monoide

Manche rcwa-Abbildungen, -Gruppen, -Monoide und -Darstellungen besitzen eine wesentlich übersichtlichere Struktur als andere:

1.8.1 Definition Folgende Objekte werden als *zahm* bezeichnet:

1. Ein rcwa-Monoid mit von Null verschiedenem Modul.
2. Eine rcwa-Abbildung, die ein zahmes zyklisches Monoid erzeugt.
3. Eine rcwa-Darstellung, deren Bild zahm ist.

Ein rcwa-Monoid, eine rcwa-Abbildung bzw. eine rcwa-Darstellung heiße *wild*, wenn es / sie nicht zahm ist.

1.8.2 Bemerkung Eine rcwa-Abbildung $f \in \mathrm{Rcwa}(R)$ ist genau dann zahm, wenn die Menge $\{\mathrm{Mod}(f^k) | k \in \mathbb{N}\}$ der Moduln ihrer Potenzen beschränkt ist. Ganze rcwa-Abbildungen und endlich erzeugte ganze rcwa-Monoide sind stets zahm.

Zahmheit ist eine Klasseninvariante:

1.8.3 Lemma *Es sei $\sigma \in \mathrm{RCWA}(R)$. Dann gilt*

1. *$f \in \mathrm{Rcwa}(R)$ zahm $\Rightarrow f^\sigma$ zahm,*
2. *$G < \mathrm{Rcwa}(R)$ zahm $\Rightarrow G^\sigma$ zahm, sowie*
3. *$G < \mathrm{RCWA}(R)$ zahm $\Rightarrow G^\sigma$ zahm.*

Beweis: Aussage (2) folgt aus Lemma 1.4.3, Aussage (7). Aussage (3) ist ein Spezialfall von (2), und Aussage (1) folgt aus (2), da eine rcwa-Abbildung nach Definition genau dann zahm ist, wenn sie ein zahmes zyklisches Monoid erzeugt. □

Eine zahme bijektive rcwa-Abbildung erzeugt stets sogar eine zahme zyklische Gruppe:

1.8.4 Lemma *Es gelten folgende Aussagen:*

1. *Der Multiplikator einer bijektiven rcwa-Abbildung wird beschränkt durch eine Funktion von deren Modul.*
2. *Bijektive zahme rcwa-Abbildungen erzeugen stets zahme zyklische rcwa-Gruppen.*

Beweis:

1. Es sei $\sigma \in \mathrm{RCWA}(R)$ und $m := \mathrm{Mod}(\sigma)$. Aufgrund der Bijektivität von σ bilden die Bilder der Restklassen $r(m) \in R/mR$ unter σ eine Partition von R. Diese Partition besteht nach Lemma 1.1.8, Aussage (1) aus einzelnen Restklassen und besitzt die Gestalt
$$R \;=\; \dot{\bigcup_{r(m) \in R/mR}} \; r^\sigma \left(\frac{a_{r(m)} \cdot m}{c_{r(m)}} \right),$$
wobei für die Koeffizienten die Notation aus Definition 1.1.2 verwendet wird. Nach Lemma 1.3.1a, Aussage (1) gilt $\forall r(m) \in R/mR \;\; c_{r(m)} | m$. Der Multiplikator von σ teilt also das kleinste gemeinsame Vielfache der Moduln der Restklassen in dieser Partition. Nach Lemma 1.1.10 gibt es eine Partition
$$1 \;=\; \sum_{r(m) \in R/mR} \frac{1}{|R/a_{r(m)}R| \cdot |R/mR| / |R/c_{r(m)}R|}$$
der 1 in Stammbrüche. Wie man aus der elementaren Zahlentheorie weiß, bedingt jedoch eine obere Schranke für die Anzahl der Summanden auch eine solche für deren Nenner. Hieraus folgt die Behauptung.

2. Aus Aussage (1) und Lemma 1.3.1b, Aussage (1) folgt die Existenz einer oberen Schranke für den Modul der Inversen einer bijektiven rcwa-Abbildung vorgegebenen Moduls. Hieraus folgt die Behauptung. □

1.8.5 Beispiele Die Begriffe *zahm* und *wild* sollen illustriert werden anhand von ein paar Beispielen:

1. Die Collatz-Abbildung T ist wild, genauer: es ist $\forall k \in \mathbb{N}\ \mathrm{Mod}(T^k) = 2^k$. Dies ist ein wesentlicher Grund für die Schwierigkeit, die $3n+1$ - Vermutung zu beweisen. Denn wäre T zahm, so gäbe es eine obere Schranke für die Anzahl der affinen Teilabbildungen der Potenzen T^k, und die Verifikation der $3n+1$ - Vermutung wäre lediglich eine Frage des Nachrechnens.

2. Die Gruppen G^φ und S_{10}^φ aus Beispiele 1.5.2, Teil (1) und (2) sind endlich, also erst recht zahm.

   Dagegen ist die Darstellung aus Beispiele 1.5.2, Teil (3) wild, obgleich sämtliche Elemente ihres Bildes zahm sind.

3. Die durch

$$n \longmapsto \begin{cases} \frac{3n}{5} & \text{falls } n \in 0(5), \\ \frac{9n+1}{5} & \text{falls } n \in 1(5), \\ \frac{3n-1}{5} & \text{falls } n \in 2(5), \\ \frac{9n-2}{5} & \text{falls } n \in 3(5), \\ \frac{9n+4}{5} & \text{falls } n \in 4(5) \end{cases} \quad \text{bzw.} \quad n \longmapsto \begin{cases} \frac{5n}{3} & \text{falls } n \in 0(3), \\ \frac{5n+1}{3} & \text{falls } n \in 1(3), \\ \frac{5n-1}{9} & \text{falls } n \in 2(9), \\ \frac{5n+2}{9} & \text{falls } n \in 5(9), \\ \frac{5n-4}{9} & \text{falls } n \in 8(9) \end{cases}$$

   gegebenen Abbildungen $\beta, \beta^{-1} \in \mathrm{RCWA}(\mathbb{Z})$ sind zueinander invers. Ist $5^k||n$ für ein $k \in \mathbb{N}$, so ist offenbar $\forall l \in \{0, \dots, k\}\ 5^{k-l}||n^{\beta^l}$. Der Wert $n^{\beta^{k-1}}$ mod 5 wird also nicht bereits durch n mod 5^{k-1} bestimmt. Mittels Lemma 1.3.1a, Aussage (2) kann man folgern, daß $\mathrm{Mod}(\beta^k) = \mathrm{Mod}(\beta)^k = 5^k$, und schließen, daß β wild ist. Wegen Lemma 1.8.4, Aussage (2) ist damit auch β^{-1} wild.

4. Es sei $F := \langle f_1, f_2 \rangle$ die freie Gruppe vom Rang 2. Ferner sei α wie in Beispiele 1.1.3 und β wie oben. Dann ist durch

$$\varphi: \ F \ \rightarrow \ \mathrm{RCWA}(\mathbb{Z}), \ f_1 \ \mapsto \ \alpha, \ f_2 \ \mapsto \ \beta,$$

   eine wilde Darstellung von F gegeben.

5. Man kann zeigen, daß die Abbildungen g und h aus Beispiel 1.6.3 eine zahme unendliche Gruppe erzeugen. Der Modul dieser Gruppe ist 12.

KAPITEL 2

Restklassenweise affine Gruppen

2.1 Reichhaltigkeitsaussagen

In diesem Abschnitt werden folgende Reichhaltigkeitsaussagen gezeigt:

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

- ist nicht endlich erzeugt,
- enthält zu jeder endlichen Gruppe eine isomorphe Untergruppe, und
- operiert hoch transitiv auf $\mathbb{Z}$.

Soweit ohne wesentlichen Mehraufwand möglich, werden diese Aussagen desweiteren auf Gruppen $\mathrm{RCWA}(R)$ über geeigneten anderen Grundringen R verallgemeinert.

2.1.1 Satz *Enthält der Ring R unendlich viele Primelemente, so ist* $\mathrm{RCWA}(R)$ *nicht endlich erzeugt.*

Beweis: Zu jedem Primelement $p \in R$ besitzt die Gruppe $\mathrm{RCWA}(R)$ ein Element mit Primteilermenge $\{p\}$, zum Beispiel

$$\nu_{0(p)} \in \mathrm{RCWA}(R): \quad n \longmapsto \begin{cases} n+p & \text{falls } \; p|n, \\ n & \text{sonst.} \end{cases}$$

Ferner ist die Primteilermenge einer rcwa-Abbildung stets endlich. Die Behauptung folgt sofort aus Lemma 1.3.1, Aussage (a.6) und (b.5). □

Jede endliche Gruppe läßt sich in RCWA($\mathbb{Z}$) einbetten:

2.1.2 Satz Es sei $R = \mathbb{Z}$ oder $R = \mathbb{Z}_{(\pi)}$ für eine endliche Primzahlmenge π. Dann besitzt jede endliche symmetrische Gruppe S_m eine treue R-rcwa-Darstellung. Zu gegebenem $m \in \mathbb{N}$, $m > 1$ ist eine solche gegeben durch

$$\varphi_m : \ \mathrm{S}_m \ \longrightarrow \ \mathrm{RCWA}(R), \ \ (1\ 2) \ \longmapsto \left(\tau : R \to R, \ n \mapsto \begin{cases} n+1 & \text{falls} \ \ n \equiv 0 \ (\tilde{m}), \\ n-1 & \text{falls} \ \ n \equiv 1 \ (\tilde{m}), \\ n & \text{sonst.} \end{cases} \right),$$

$$(1\ 2\ \ldots\ m) \ \longmapsto \left(\sigma : R \to R, \ n \mapsto \begin{cases} n+1 & \text{falls} \ \ n \equiv 0, 1, \ldots, m-2 \ (\tilde{m}), \\ n-(m-1) & \text{falls} \ \ n \equiv m-1 \ (\tilde{m}), \\ n & \text{sonst.} \end{cases} \right),$$

wobei im Falle $R = \mathbb{Z}$ schlicht $\tilde{m} := m$ sei, und im Falle $R = \mathbb{Z}_{(\pi)}$ für $\tilde{m}$ die kleinste natürliche Zahl $\geqslant m$ gewählt werde, deren Primteiler alle in π liegen.

Es verbleibt zu zeigen, daß die Gruppe RCWA(R) hoch transitiv auf R operiert. Hierzu werden zwei elementare Hilfsaussagen benötigt. Zunächst eine einfache Aussage zu affinen Abbildungen von Restklassen auf Restklassen:

2.1.3 Lemma *Es seien $r(m)$ und $\tilde{r}(\tilde{m})$ Restklassen von R. Dann besitzt der Quotientenkörper K von R Affinitäten, die $r(m)$ bijektiv auf $\tilde{r}(\tilde{m})$ abbilden. Diese sind von der Form $f = f_1 \cdot f_2(u,k)$ mit*

$$f_1 \in \mathrm{AFF}(K) : \ \ n \ \longmapsto \ \frac{\tilde{m}n + (m\tilde{r} - \tilde{m}r)}{m}$$

und

$$f_2(u,k) \in \mathrm{AFF}(R) : \ \ n \ \longmapsto \ un + \tilde{r}(1-u) + k\tilde{m}$$

für ein $u \in R^\times$ und ein $k \in R$. Alle Affinitäten, die die Restklasse $\tilde{r}(\tilde{m})$ bijektiv auf sich abbilden, sind darstellbar in der Form $f_2(u,k)$ für geeignete u, k.

Beweis: Nach Lemma 1.1.8, Aussage (1) ist $r(m)^{f_1} = \tilde{r}(\tilde{m})$. Es verbleibt zu zeigen, daß die Abbildungen $f_2(u,k)$ die Restklasse $\tilde{r}(\tilde{m})$ bijektiv auf sich abbilden, und daß es keine weiteren Affinitäten von K gibt, die dies tun. Hierzu sei

$$\alpha : \tilde{r}(\tilde{m}) \to R, \quad n \mapsto (an+b)/c \quad (a, b, c \in R)$$

eine affine Abbildung. Es gilt $\{\tilde{r}^\alpha, a\tilde{m}/c\} \subset R$, und es kann o.E. angenommen werden, daß $\mathrm{ggT}(a,b,c) = 1$ und daß $c = |c|$. Nach Lemma 1.1.8, Aussage (1) ist das Bild von α die Restklasse $(a\tilde{r}+b)/c$ mod $a\tilde{m}/c$. Bild und Definitionsbereich von α sind also genau dann gleich, wenn $a/c \in R^\times$, und wenn es ferner ein $k \in R$ so gibt, daß $b = \tilde{r}(c-a) + k\tilde{m}$. Die Normierung $c = |c|$ liefert $c = 1$, und die Behauptung folgt, da Affinitäten nach Definition injektiv sind. □

Die in Lemma 2.1.3 beschriebenen affinen Abbildungen lassen sich zu rcwa-Abbildungen zusammensetzen – dies liefert die folgende 'Partitionentransitivitätsaussage':

2.1.4 Lemma Es sei M eine Vereinigung endlich vieler Restklassen von R, und es sei $k \in \mathbb{N}$. Ferner seien $R = r_1(m_1) \cup \cdots \cup r_k(m_k)$ und $M = \tilde{r}_1(\tilde{m}) \cup \cdots \cup \tilde{r}_k(\tilde{m})$ Partitionen von R bzw. M in jeweils k Restklassen, und es seien $n_i \in r_i(m_i)$ bzw. $\tilde{n}_i \in \tilde{r}_i(\tilde{m}_i)$ beliebige Repräsentanten. Dann gibt es wegen Lemma 2.1.3 auf den Restklassen $r_1(m_1), \dots, r_k(m_k)$ definierte affine Abbildungen, die sich zu einer injektiven Abbildung $f \in \mathrm{Rcwa}(R)$ mit der Eigenschaft

$$\forall i \in \{1, \dots, k\} \ \left(r_i(m_i)^f = \tilde{r}_i(\tilde{m}_i) \wedge n_i^f = \tilde{n}_i \right)$$

zusammensetzen lassen. Konstruktionsgemäß gilt $\mathrm{Mod}(f) | \,\mathrm{kgV}(m_1, \dots, m_k)$. Besitzt der Ring R die schwache Restklassenteilbarkeitseigenschaft, dann kann man die Restklassen $r_i(m_i), \tilde{r}_i(\tilde{m}_i)$ wegen Bemerkung 1.2.4 durch beliebige Vereinigungen jeweils endlich vieler Restklassen ersetzen.

Jetzt läßt sich leicht die versprochene Transitivitätsaussage zeigen:

2.1.5 Satz *Die Gruppe* $\mathrm{RCWA}(R)$ *operiert hoch transitiv auf* R.

Beweis: Sei $k \in \mathbb{N}$ beliebig. Es ist zu zeigen, daß es zu je zwei k-Tupeln $(n_1, \dots, n_k)$ und $(\tilde{n}_1, \dots, \tilde{n}_k)$ paarweise verschiedener Elemente von R stets ein $\sigma \in \mathrm{RCWA}(R)$ so gibt, daß $(n_1^\sigma, \dots, n_k^\sigma) = (\tilde{n}_1, \dots, \tilde{n}_k)$. Es sei $a \in R \backslash (R^\times \cup \{0\})$. Ferner sei $e \in \mathbb{N}$ so groß gewählt, daß keine zwei n_i, n_j und keine zwei $\tilde{n}_i, \tilde{n}_j$ in derselben Restklasse (mod a^e) liegen. Legt man nun $n_{k+1}, \dots, n_{|R/a^eR|}$ und $\tilde{n}_{k+1}, \dots, \tilde{n}_{|R/a^eR|}$ so fest, daß die Mengen $\{n_1, \dots, n_{|R/a^eR|}\}$ und $\{\tilde{n}_1, \dots, \tilde{n}_{|R/a^eR|}\}$ zu Vertretersystemen für die Restklassen (mod a^e) werden, so folgt die Behauptung mit Lemma 2.1.4, angewandt auf die Partitionen

$$R \ = \ \bigcup_{i=1}^{|R/a^eR|} n_i(a^e) \ = \ \bigcup_{i=1}^{|R/a^eR|} \tilde{n}_i(a^e)$$

mit der Festlegung $\forall i \in \{1, \dots, |R/a^eR|\} \ n_i^\sigma = \tilde{n}_i$. □

Satz 2.1.5 hat erhebliche Konsequenzen im Hinblick auf die Reichhaltigkeit eventueller nichttrivialer Normalteiler von $\mathrm{RCWA}(R)$:

2.1.6 Korollar Mittels [DM96], Korollar 7.2A läßt sich folgern, daß ein etwaiger nichttrivialer Normalteiler von $\mathrm{RCWA}(R)$ ebenfalls hoch transitiv auf R operiert. Da eine abelsche Gruppe nur maximal einfach transitiv operieren kann, folgt ebenfalls sofort, daß das Zentrum von $\mathrm{RCWA}(R)$ trivial ist. Da eine hoch transitiv operierende Gruppe stets eine Untergruppe besitzt, die auf einer 5-elementigen Menge als A_5 operiert, besitzt $\mathrm{RCWA}(R)$ nicht einmal einen auflösbaren nichttrivialen Normalteiler.

2.2 Die Fürstenberg - Topologie

Die Gruppe $\mathrm{RCWA}(R)$ läßt sich als Gruppe von Homöomorphismen auffassen, wenn man den Grundring R auf geeignete Weise mit einer Topologie versieht. Lemma 1.1.9 liefert hierzu einen guten Ausgangspunkt:

2.2.1 Definition Die durch Wahl der Menge der Restklassen als Basis auf R induzierte Topologie werde bezeichnet als *Fürstenberg-Topologie*. Im folgenden werde der Ring R stets auch als topologischer Raum mit dieser Topologie betrachtet.

2.2.2 Bemerkung Im Fall $R = \mathbb{Z}$ ist dies die Topologie, die Harry Fürstenberg in seinem topologischen Beweis [Für55] für die Existenz unendlich vieler Primzahlen verwendet hat.

2.2.3 Satz Es gilt:

1. Der topologische Raum R ist Hausdorffsch.
2. Restklassen sind sowohl offen als auch abgeschlossen.
3. Rcwa-Abbildungen sind stetig.
4. Urbilder von Vereinigungen endlich vieler Restklassen von R unter rcwa-Abbildungen sind ebenfalls Vereinigungen endlich vieler Restklassen.
5. Die Gruppe $\mathrm{RCWA}(R)$ ist eine Gruppe von Homöomorphismen.

Beweis: Wählt man zu zwei verschiedenen Punkten $n_1, n_2 \in R$ ein $m \in R \setminus \{0\}$ so, daß $m \nmid (n_1 - n_2)$, dann sind die Restklassen $n_1(m)$ und $n_2(m)$ disjunkte offene Umgebungen von n_1 bzw. n_2. Folglich gilt Aussage (1). Wegen der vorausgesetzten Endlichkeit aller Restklassenringe von R gilt Aussage (2). Die Aussagen (3) und (4) erhält man analog zu Lemma 1.2.1, Aussage (2), wenn man zusätzlich berücksichtigt, daß das Urbild einer Menge unter einer konstanten affinen Teilabbildung einer rcwa-Abbildung f entweder leer oder eine Restklasse (mod $\mathrm{Mod}(f)$) ist. Aussage (5) folgt aus Lemma 1.2.1, Aussage (2) und Lemma 1.3.4, Aussage (2). □

2.3 Einschränkungsmonomorphismen

Im folgenden wird dargelegt, daß die Gruppen $\mathrm{RCWA}(R)$ echte Untergruppen besitzen, die zu ganz $\mathrm{RCWA}(R)$ isomorph sind. Es wird sich für weitere Untersuchungen als sehr zweckmäßig erweisen, Isomorphismen von $\mathrm{RCWA}(R)$ auf derartige Untergruppen zu betrachten:

2.3.1 Definition Sind f und g rcwa-Abbildungen von R und ist f injektiv, dann sei g_f die eindeutig bestimmte, $R \setminus \operatorname{im} f$ punktweise festlassende rcwa-Abbildung so, daß das folgende Diagramm kommutiert:

$$\begin{tikzcd}
R \arrow[r, "g"] \arrow[d, hook, "f"'] & R \arrow[d, hook, "f"] \\
R \arrow[r, "g_f"'] & R
\end{tikzcd}$$

Die Abbildung $\pi_f : \mathrm{Rcwa}(R) \to \mathrm{Rcwa}(R),\ g \mapsto g_f$ werde bezeichnet als der *zu f assoziierte Einschränkungsmonomorphismus*. Wo keine Verwechselungen zu befürchten sind, wird der Einschränkungsmonomorphismus π_f mit seiner Einschränkung auf $\mathrm{RCWA}(R)$ identifiziert.

2.3.2 Satz *Die Einschränkungsmonomorphismen π_f sind wohldefinierte Abbildungen, und es handelt sich tatsächlich um Monomorphismen. Außerdem sind die Abbildungen $\pi_f : \mathrm{RCWA}(R) \to \mathrm{RCWA}(R)^{\pi_f}$ Permutationsisomorphismen.*

Beweis: Aufgrund der Forderung nach Injektivität von f sind Einschränkungsmonomorphismen wohldefinierte injektive Abbildungen. Bis hierher braucht man noch nicht einmal zu wissen, daß man es mit rcwa-Abbildungen zu tun hat. Ferner sind mit f auch Bilder von rcwa-Abbildungen unter dem zu f assoziierten Einschränkungsmonomorphismus stets wieder rcwa-Abbildungen. Daß Einschränkungsmonomorphismen Homomorphismen sind, ist gleichfalls leicht zu sehen – für beliebige $g_1, g_2 \in \mathrm{Rcwa}(R)$ kommutieren gemäß Definition alle drei Rechtecke in folgendem Diagramm:

$$\begin{tikzcd}
R \arrow[r, "g_1^{\pi_f}"] & R \arrow[r, "g_2^{\pi_f}"] & R \\
R \arrow[u, hook, "f"] \arrow[r, "g_1"] \arrow[d, hook, "f"'] & R \arrow[u, hook, "f"] \arrow[r, "g_2"] & R \arrow[u, hook, "f"] \arrow[d, hook, "f"] \\
R \arrow[rr, "(g_1g_2)^{\pi_f}"] & & R
\end{tikzcd}$$

Es folgt $(g_1g_2)^{\pi_f} = g_1^{\pi_f} g_2^{\pi_f}$. Die Beziehung $(g^{-1})^{\pi_f} = (g^{\pi_f})^{-1}$ für bijektives g erhält man direkt aus der Definition, indem man den horizontalen Pfeilen in umgekehrter Richtung folgt. Weil die Abbildung f als Abbildung von R auf $\operatorname{im} f$ bijektiv ist, bewirkt der Einschränkungsmonomorphismus π_f lediglich eine 'Umnumerierung' $n \mapsto n^f$ der Punkte, es handelt sich also außerdem um einen Permutationsisomorphismus. $\square$

2.3.3 Korollar Aus Satz 2.3.2 und Satz 2.1.5 kann man schließen, daß $\mathrm{RCWA}(R)$ zu jedem möglichen Bild $\mathrm{im}\, f$ einer injektiven rcwa-Abbildung f eine zu ganz $\mathrm{RCWA}(R)$ permutationsisomorphe Untergruppe besitzt, die hoch transitiv auf $\mathrm{im}\, f$ operiert und $R \setminus \mathrm{im}\, f$ punktweise fixiert. Es folgt, daß die Klasse der Gruppen, die treue R-rcwa-Darstellungen besitzen, abgeschlossen ist bezüglich der Bildung direkter Produkte – denn sind $G, H \leqslant \mathrm{RCWA}(R)$, ist $a \in R \setminus (R^\times \cup \{0\})$ und sind $b_1, b_2 \in R$ inkongruent $(\mathrm{mod}\ a)$, so ist

$$G \times H \ \cong\ \langle G^{\pi_{n \mapsto an+b_1}}, H^{\pi_{n \mapsto an+b_2}} \rangle \ \leqslant\ \mathrm{RCWA}(R).$$

Es besitze R die schwache Restklassenteilbarkeitseigenschaft. Ferner seien M_1 und M_2 nichtleere, von R verschiedene Vereinigungen jeweils endlich vieler Restklassen von R. Dann kann man mittels Lemma 2.1.4 schließen, daß es injektive rcwa-Abbildungen f_1 und f_2 von R so gibt, daß $\mathrm{im}\, f_1 = M_1$ und $\mathrm{im}\, f_2 = M_2$. Ein kleiner Vorgriff auf Satz 2.4.1 liefert ferner die Existenz einer Permutation $\sigma \in \mathrm{RCWA}(R)$ so, daß $M_1^\sigma = M_2$. Es folgt $(\mathrm{im}\, \pi_{f_1})^\sigma = \mathrm{im}\, \pi_{f_2}$. Insbesondere sind also sämtliche Bilder von zu injektiven, aber nicht surjektiven rcwa-Abbildungen assoziierten Einschränkungsmonomorphismen zueinander konjugiert in $\mathrm{RCWA}(R)$.

2.4 Klassentransitivitätsaussagen

In Satz 2.1.5 wurde bereits gezeigt, daß die Gruppe $\mathrm{RCWA}(R)$ hoch transitiv auf dem zugrundeliegenden Ring R operiert. Ebenso leicht ist es möglich, eine Transitivitätsaussage für die Operation von $\mathrm{RCWA}(R)$ auf der Menge der Vereinigungen von Restklassen zu erhalten. Natürlich kann man hier ohne Disjunktheitsvoraussetzungen nur einfache Transitivität erwarten:

2.4.1 Satz *Besitzt der Ring R die schwache Restklassenteilbarkeitseigenschaft, so operiert die Gruppe $\mathrm{RCWA}(R)$ transitiv auf der Menge der von $\emptyset$ und R verschiedenen Vereinigungen endlich vieler Restklassen von R.*

Beweis: Es seien $\emptyset \neq M_1, M_2 \subsetneq R$ Vereinigungen endlich vieler Restklassen. Zu zeigen ist: $\exists \sigma \in \mathrm{RCWA}(R) : M_1^\sigma = M_2$. Weil R die schwache Restklassenteilbarkeitseigenschaft besitzt und weil nach Lemma 1.1.9 Komplemente von Vereinigungen endlich vieler Restklassen ebenfalls Vereinigungen endlich vieler Restklassen sind, liefert Lemma 2.1.4 angewandt auf die Partitionen $R = M_1 \cup (R \setminus M_1) = M_2 \cup (R \setminus M_2)$ die gewünschte Existenzaussage. □

2.4.2 Beispiel Es soll eine Abbildung $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ konstruiert werden, welche die Restklasse $1(2)$ auf die Vereinigung der Restklassen $2(5)$ und $3(5)$ abbildet.

Hierzu wird $1(2)$ als Vereinigung von $1(4)$ und $3(4)$, und das Komplement $\mathbb{Z} \setminus 1(2)$ als Vereinigung von $0(6)$, $2(6)$ und $4(6)$ geschrieben.

Nach Lemma 2.1.3 konstruiert man affine Abbildungen, die $1(4)$ auf $2(5)$, $3(4)$ auf $3(5)$, $0(6)$ auf $0(5)$, $2(6)$ auf $1(5)$ bzw. $4(6)$ auf $4(5)$ abbilden, und setzt diese zur gewünschten Abbildung σ vom Modul $\mathrm{kgV}(4,6) = 12$ zusammen – es ist dann

$$\sigma \in \mathrm{RCWA}(\mathbb{Z}), \quad n \longmapsto \begin{cases} \frac{5n+3}{4} & \text{falls } n \in 1(4), \\ \frac{5n-3}{4} & \text{falls } n \in 3(4), \\ \frac{5n}{6} & \text{falls } n \in 0(6), \\ \frac{5n-4}{6} & \text{falls } n \in 2(6), \\ \frac{5n+4}{6} & \text{falls } n \in 4(6). \end{cases}$$

In Satz 2.4.1 die schwache Restklassenteilbarkeitseigenschaft vorauszusetzen ist essentiell:

2.4.3 Bemerkung Besitzt der Ring R nicht die schwache Restklassenteilbarkeitseigenschaft, so operiert die Gruppe $\mathrm{RCWA}(R)$ i.a. nicht transitiv auf der Menge der von $\emptyset$ und R verschiedenen Vereinigungen endlich vieler Restklassen von R. Im Fall $R = \mathbb{Z}_{(3)}$ beispielsweise läßt sich eine Vereinigung einer geraden Anzahl von Restklassen nicht als Vereinigung einer ungeraden Anzahl von Restklassen schreiben und umgekehrt. Hier ist die Parität der Anzahl der Restklassen außerdem unter rcwa-Abbildungen invariant, die Operation von $\mathrm{RCWA}(\mathbb{Z}_{(3)})$ auf der Menge der Vereinigungen von Restklassen folglich intransitiv.

Anstatt auf der Menge der Vereinigungen von Restklassen kann man $\mathrm{RCWA}(R)$ auch auf deren Elementen – also eben auf Vereinigungen von Restklassen – operieren lassen. An dieser Stelle ist es zweckmäßig, den Begriff der *Jordan-Menge* ins Spiel zu bringen. Da dieser nicht notwendigerweise jedem Leser geläufig sein dürfte, sei hier die gängige Definition angegeben (vgl. z.B. [DM96], Kapitel 7, Abschnitt 4):

2.4.4 Definition Es sei G eine Gruppe, die auf einer Menge M operiert. Man nennt M_J eine *Jordan-Menge* und ihr Komplement $M_C := M \setminus M_J$ ein *Jordan-Komplement*, falls die Operation des punktweisen Stabilisators $G_{(M_C)}$ auf M_J transitiv und $|M_J| > 1$ ist. Ist M_C endlich und operiert G mindestens $|M_C| + 1$-fach transitiv auf M, so nennt man M_J und M_C *unecht*. In diesem Fall ist M_C bereits aus Kardinalitätsgründen ein Jordan-Komplement. Man nennt M_J und M_C *echt*, wenn M_C unendlich ist, oder G nicht $|M_C|+1$-fach transitiv auf M operiert. Die Gruppe G bezeichnet man als *Jordan-Gruppe*, falls sie transitiv auf M operiert und mindestens ein echtes Jordan-Komplement besitzt. Operiert der punktweise Stabilisator eines Jordan-Komplements k-fach transitiv bzw. hoch transitiv auf der zugehörigen Jordan-Menge, so bezeichnet man letztere ebenfalls als k-fach transitiv bzw. hoch transitiv.

2.4.5 Bemerkung Besitzt R die schwache Restklassenteilbarkeitseigenschaft, dann ist $\mathrm{RCWA}(R)$ nach Korollar 2.3.3 eine Jordan-Gruppe, und alle nichtleeren Vereinigungen $M \subsetneq R$ endlich vieler Restklassen sind sowohl hoch transitive Jordan-Mengen als auch Jordan-Komplemente.

2.4.6 Satz *Besitzt der Ring R die schwache Restklassenteilbarkeiteigenschaft, so sind die Jordan-Mengen für* $\mathrm{RCWA}(R)$ *in R genau die offenen und die Jordan-Komplemente genau die abgeschlossenen Mengen. Alle Jordan-Mengen sind hoch transitiv.*

Beweis: Nach Satz 2.2.3, Aussage (5) ist $\mathrm{RCWA}(R)$ eine Gruppe von Homöomorphismen von R. Ferner besitzt die Fürstenberg-Topologie auf R nach Satz 2.2.3, Aussage (2) eine Basis aus Mengen, die sowohl offen als auch abgeschlossen sind, und $\mathrm{RCWA}(R)$ operiert nach Satz 2.1.5 transitiv auf R. Daher kann man [BMMN98], Abschnitt 11.1.2 entnehmen, daß die Jordan-Mengen bzw. -Komplemente für $\mathrm{RCWA}(R)$ in R höchstens die offenen bzw. abgeschlossenen Mengen sind. Es verbleibt also zu zeigen, daß alle offenen Mengen auch tatsächlich hoch transitive Jordan-Mengen sind.

Nach Bemerkung 2.4.5 sind Vereinigungen endlich vieler Restklassen hoch transitive Jordan-Mengen. Es sei nun $M \subset R$ offen. Man kann o.E. annehmen, daß $M = \cup_{i=1}^{\infty} r_i(m_i)$. Dies läßt sich umschreiben zu $M = \cup_{i=1}^{\infty}(r_i(m_i) \cup r_{i+1}(m_{i+1}))$. Die Menge M ist also Vereinigung einer zusammenhängenden Familie hoch transitiver Jordan-Mengen, und als solche nach [BMMN98], Korollar 10.10 gleichfalls eine hoch transitive Jordan-Menge. $\square$

Ben Green und Terence Tao haben in [GT04] gezeigt, daß die Menge der Primzahlen arithmetische Progressionen beliebiger Länge enthält. Dies motiviert die folgenden Betrachtungen.

2.4.7 Definition Die Elemente der Bahnen $\{1, 2, \ldots, l\}^{\mathrm{Aff}(\mathbb{Z})}$, $l \in \mathbb{N}$ werden als *arithmetische Progressionen der Länge l* bezeichnet. Dementsprechend sagt man, eine Menge $M \subseteq \mathbb{Z}$ *enthalte arithmetische Progressionen beliebiger Länge*, falls

$$\forall l \in \mathbb{N}\ \exists n \in \mathbb{Z}, m \in \mathbb{N}: \ \{n, n+m, n+2m, \ldots, n+(l-1)m\} \subset M.$$

2.4.8 Satz *Die Eigenschaft einer Menge ganzer Zahlen, arithmetische Progressionen beliebiger Länge zu enthalten, ist invariant unter der Operation von* $\mathrm{RCWA}(\mathbb{Z})$. *Das heißt, ist $M \subseteq \mathbb{Z}$ und $\sigma \in$* $\mathrm{RCWA}(\mathbb{Z})$, *so besitzt M^σ diese Eigenschaft genau dann, wenn auch M sie besitzt.*

Beweis: Es sei $M \subseteq \mathbb{Z}$ eine Menge, die arithmetische Progressionen beliebiger Länge enthält, und es sei $\sigma \in \mathrm{RCWA}(\mathbb{Z})$. Ferner sei $l \in \mathbb{N}$. Es genügt zu zeigen, daß M^σ eine arithmetische Progression der Länge l enthält. Setzt man $m := \mathrm{Mod}(\sigma)$, dann enthält M nach Voraussetzung eine solche der Länge $m \cdot l$. Diese werde bezeichnet mit A. Es gibt nun eine Restklasse $r(m) \in \mathbb{Z}/m\mathbb{Z}$ so, daß $|A \cap r(m)| \geqslant l$. Dieser Schnitt ist ebenfalls eine arithmetische Progression, wie auch sein Bild $(A \cap r(m))^{\sigma|_{r(m)}} \subseteq M^\sigma$ unter der affinen Abbildung $\sigma|_{r(m)}$. $\square$

Eine weitere Invariante ist die folgende:

2.4.9 Satz *Die Eigenschaft einer Menge $M \subseteq \mathbb{Z} \setminus \{0\}$, daß die Reihe $\sum_{n \in M} \frac{1}{|n|}$ divergiert, ist in demselben Sinne wie in Satz 2.4.8 invariant unter der Operation des Punktstabilisators* $\mathrm{RCWA}(\mathbb{Z})_0$.

Beweis: Die Behauptung gilt, da zu gegebenem $\sigma \in \mathrm{RCWA}(\mathbb{Z})_0$ die Quotienten $|n|/|n^\sigma|$ und $|n^\sigma|/|n|$ für $n \in \mathbb{Z} \setminus \{0\}$ definiert und beschränkt sind. $\square$

2.4.10 Bemerkung G. Szekeres hat die Vermutung aufgestellt, sogar jede Menge $M \subseteq \mathbb{Z} \setminus \{0\}$ so, daß die Reihe $\sum_{n \in M} \frac{1}{|n|}$ divergiert, enthalte arithmetische Progressionen beliebiger Länge (vgl. [ET36]). Diese Vermutung ist bis dato unbewiesen (vgl. [GT04]). Satz 2.4.9 reduziert dieses Problem auf Bahnenvertreter unter der Operation von $\mathrm{RCWA}(\mathbb{Z})_0$.

2.5 Zahme Gruppen und respektierte Partitionen

Im folgenden wird begonnen mit Betrachtungen zur Operation geeigneter rcwa-Gruppen auf Partitionen von R in einzelne Restklassen. Diese werden im nächsten Abschnitt zur weitgehenden Klärung der Struktur zahmer Gruppen führen.

Zunächst zu einer Aussage zu den Bahnen gewisser Restklassen unter der Operation von zahmen Gruppen, welche hierbei gute Dienste leisten wird:

2.5.1 Lemma *Es sei $G < \mathrm{RCWA}(R)$ zahm und $\mathrm{Mod}(G)|m$. Dann ist die Bahn einer Restklasse $r(m)$ unter der Operation von G eine Menge von endlich vielen disjunkten einzelnen Restklassen.*

Beweis: Die Wahl von m bedingt, daß die Einschränkung eines Elementes $g \in G$ auf $r(m)$ stets affin ist. Hieraus folgt die Affinität der Elemente von G auf allen Elementen der Bahn Ω von $r(m)$ unter der Operation von G: Es seien $\tilde{r}(\tilde{m}) \in \Omega$ und $g \in G$ beliebig. Es ist zu zeigen, daß $g|_{\tilde{r}(\tilde{m})}$ affin ist. Nach Voraussetzung gibt es ein $h \in G$ so, daß $r(m)^h = \tilde{r}(\tilde{m})$. Wie bereits bekannt, sind die Abbildungen $h|_{r(m)}$ und $(hg)|_{r(m)}$ affin. Damit sind aber auch die Abbildungen $h^{-1}|_{\tilde{r}(\tilde{m})}$ und $h^{-1}|_{\tilde{r}(\tilde{m})} \cdot (hg)|_{r(m)} = (h^{-1}hg)|_{\tilde{r}(\tilde{m})} = g|_{\tilde{r}(\tilde{m})}$ affin, da $\mathrm{AFF}(K)$ eine Gruppe ist. Zumal das Bild einer Restklasse unter einer Affinität nach Lemma 1.1.8, Aussage (1) wieder eine Restklasse ist, sofern es ganz in R liegt, enthält Ω nur einzelne Restklassen. Wegen Lemma 1.4.3, Aussage (1) gilt $\mathrm{Mult}(G)|m$, d.h. $\forall g \in G \ \ \mathrm{Mult}(g)|m$, die Moduln der Restklassen in Ω sind nach Lemma 1.1.8, Aussage (1) also Teiler von m^2. Ein Abzählen der in Frage kommenden Restklassen liefert $|\Omega| \leqslant \sum_{t|m^2} |R/tR| < \infty$. Angenommen, die Bahn Ω enthielte zwei Restklassen, die sich nichttrivial schneiden, d.h. es gäbe ein $\tilde{r}(\tilde{m}) \in \Omega$ und ein $g \in G$ so, daß $\tilde{r}(\tilde{m})^g \cap \tilde{r}(\tilde{m}) \notin \{\emptyset, \tilde{r}(\tilde{m})\}$. Ist hierbei $g|_{\tilde{r}(\tilde{m})}$ gegeben durch $n \mapsto (an + b)/c$ für geeignete $a, b, c \in R$, dann folgt nach Lemma 1.1.8, Aussage (3), daß mindestens einer der Koeffizienten a, c keine Einheit ist. Dies steht nach Lemma 1.1.8, Aussage (2) im Widerspruch zur Endlichkeit von Ω. $\square$

2.5.2 Definition Eine rcwa-Gruppe $G < \mathrm{RCWA}(R)$ *respektiere* eine Partition $\mathcal{P}$ von R in endlich viele Restklassen, wenn G auf $\mathcal{P}$ in natürlicher Weise als Permutationsgruppe operiert, und die Einschränkung eines Elements von G auf eine der Restklassen in $\mathcal{P}$ stets affin ist. Eine Abbildung $\sigma \in \mathrm{RCWA}(R)$ *respektiere* die Partition $\mathcal{P}$, wenn die zyklische Gruppe $\langle\sigma\rangle$ diese respektiert.

In der beschriebenen Situation wird die von σ auf $\mathcal{P}$ induzierte Permutation bzw. die von G auf $\mathcal{P}$ induzierte Permutationsgruppe bezeichnet mit $\sigma_\mathcal{P}$ bzw. $G_\mathcal{P}$.

Das Symbol $\mathrm{Sym}(\mathcal{P})$ stehe für eine beliebige rcwa-Gruppe, die die Partition $\mathcal{P}$ respektiert und auf ihr als volle symmetrische Gruppe operiert. Der Ausdruck $\mathrm{Sym}(\mathcal{P}) < G$ bedeute dementsprechend, daß G eine Untergruppe besitzt, die die Partition $\mathcal{P}$ respektiert und auf ihr als volle symmetrische Gruppe operiert.

Es sei M eine Menge von Mengen. Dann wird die Vereinigung der Elemente von M mit $\cup M$ bezeichnet. Analog dazu wird der Schnitt der Elemente von M mit $\cap M$ bezeichnet.

2.5.3 Beispiel Es seien $g, h \in \mathrm{RCWA}(\mathbb{Z})$ die Abbildungen der Ordnungen 7 bzw. 12 aus Beispiel 1.6.3. Diese sind gegeben durch

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

Die Gruppe $G := \langle g, h\rangle$ respektiert die 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 $\mathbb{Z}$, und es ist

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

Die Ordnung von $G_\mathcal{P}$ ist $322560 = 2^{10} \cdot 3^2 \cdot 5 \cdot 7$, und die Kommutatoruntergruppe $G'_\mathcal{P}$ ist perfekt und hat den Index 2. Der Kern der Operation von G auf $\mathcal{P}$ ist eine freie abelsche Gruppe vom Rang 6. Die Berechnungen für dieses und alle weiteren Beispiele wurden durchgeführt mit GAP [GAP04] und RCWA [Koh05].

2.5.4 Lemma *Eine zahme rcwa-Gruppe $G < \mathrm{RCWA}(R)$ ist genau dann ganz, wenn sie die Partition $R/\mathrm{Mod}(G)R$ von R respektiert.*

Beweis: Es sei $m := \mathrm{Mod}(G) \neq 0$ und $g \in G$ beliebig. Es ist lediglich zu zeigen, daß die Abbildung g genau dann ganz ist, wenn sie die Restklassen (mod m) permutiert – die Affinitätsbedingung ist nach Wahl von m ohnehin erfüllt. Dies folgt jedoch, da das Bild einer Restklasse (mod m) unter einer Affinität $\alpha \in \mathrm{AFF}(K)$ nach Lemma 1.1.8, Aussage (1) genau dann auch eine Restklasse (mod m) ist, wenn bereits $\alpha \in \mathrm{AFF}(R)$. □

2.5.5 Beispiel Es sei $m \in \mathbb{N}$ und φ_m wie in Satz 2.1.2. Dann respektiert die Gruppe $G := \mathrm{S}_m{}^{\varphi_m}$ nach Lemma 2.5.4 die Partition

$$\mathbb{Z}/m\mathbb{Z} \;=\; \{0(m), 1(m), 2(m), \ldots, m-1(m)\}.$$

Ferner gilt $G_{\mathbb{Z}/m\mathbb{Z}} \cong \mathrm{S}_m$, die Operation von G auf $\mathbb{Z}/m\mathbb{Z}$ ist also treu.

2.5.6 Lemma *Sind $G, H < \mathrm{RCWA}(R)$ rcwa-Gruppen, ist $\mathcal{P}$ eine von G und H respektierte Partition von R und ist $\sigma \in \mathrm{RCWA}(R)$ auf jedem Element von $\mathcal{P}$ affin, dann gilt:*

1. *Das Erzeugnis $\langle G, H\rangle < \mathrm{RCWA}(R)$ respektiert $\mathcal{P}$ ebenfalls.*
2. *Die Gruppe G^σ respektiert die Partition $\mathcal{P}^\sigma$, und die Gruppen $G_\mathcal{P}$ und $G^\sigma_{\mathcal{P}^\sigma}$ sind zueinander permutationsisomorph.*

Beweis:

1. Alle Elemente von G und alle Elemente von H permutieren nach Voraussetzung die Restklassen in der Partition $\mathcal{P}$, und wirken ferner auf allen Restklassen in $\mathcal{P}$ als affine Abbildungen. Damit gilt dasselbe aber auch für beliebige Produkte von Elementen von G mit Elementen von H, oder anders ausgedrückt, für beliebige Elemente der von G und H erzeugten Untergruppe von $\mathrm{RCWA}(R)$.
2. Nach Voraussetzung ist $\sigma \in \mathrm{RCWA}(R)$ auf jedem Element von $\mathcal{P}$ affin. Folglich ist $\mathcal{P}^\sigma$ nach Lemma 1.1.8, Aussage (1) ebenfalls eine Partition von R in einzelne Restklassen. Diese wird von G^σ permutiert, und aufgrund der genannten Affinitätsvoraussetzung sogar respektiert. Die Abbildung σ induziert einen Permutationsisomorphismus von $G_\mathcal{P}$ auf $G^\sigma_{\mathcal{P}^\sigma}$. □

2.5.7 Beispiel Es sei G wie in Beispiel 2.5.5. Die Abbildung $\nu : n \mapsto n+1$ hat unendliche Ordnung, und $\varsigma : n \mapsto -n$ ist nicht klassenweise ordnungserhaltend. Da die Gruppe G endlich und klassenweise ordnungserhaltend ist, enthält sie weder ν noch ς. Die Gruppe $H := \langle \nu, \varsigma\rangle$ respektiert ebenfalls die Partition $\mathbb{Z}/m\mathbb{Z}$. Nach Lemma 2.5.6, Aussage (1) gilt gleiches auch für das Erzeugnis $\langle G, H\rangle$ dieser beiden Gruppen.

Der folgende Satz wird von zentraler Bedeutung sein für eine vollständige Klassifikation jener Gruppen, die treue zahme R-rcwa-Darstellungen besitzen:

2.5.8 Satz *Eine Gruppe $G < \mathrm{RCWA}(R)$ ist genau dann zahm, wenn sie eine Partition von R in endlich viele Restklassen respektiert.*

Beweis: Es sei zunächst G zahm. Es sei $m := \mathrm{Mod}(G)$, und die Restklassen (mod m) seien bezeichnet mit $r_i(m)$, $i = 1, \dots, |R/mR|$. Die gesuchte Partition $\mathcal{P}$ von R konstruiert man nach folgendem Algorithmus:

1. Setze $i := 1$ und $\mathcal{P} := \emptyset$.
2. Falls $r_i(m) \nsubseteq \cup\mathcal{P}$, setze $D := r_i(m) \setminus \cup\mathcal{P}$, andernfalls fahre fort bei Schritt 4.
3. Die Menge D ist nach Lemma 1.1.9 eine Vereinigung endlich vieler Restklassen. Setze jetzt $\tilde{m} := \mathrm{kgV}(m, \mathrm{Mod}(D))$, und nehme an, es sei $D = \tilde{r}_1(\tilde{m}) \cup \dots \cup \tilde{r}_k(\tilde{m})$. Für $j = 1, \dots, k$ setze $\mathcal{P} := \mathcal{P} \cup \tilde{r}_j(\tilde{m})^G$ – die Bahnen der Restklassen $\tilde{r}_j(\tilde{m})$ unter der Operation von G sind nach Lemma 2.5.1 endliche Mengen disjunkter einzelner Restklassen.
4. Falls $i < |R/mR|$, setze $i := i + 1$ und fahre fort bei Schritt 2. Andernfalls fertig.

Die Endlichkeit von $\mathcal{P}$ folgt daraus, daß höchstens $|R/mR| < \infty$ Differenzmengen D zu bilden sind, und daß diese Vereinigungen endlich vieler Restklassen sind, deren Bahnen wiederum jeweils endlich sind.

Die Umkehrung ist trivial, denn offenbar teilt der Modul der Gruppe das kleinste gemeinsame Vielfache der Moduln der Restklassen in der respektierten Partition. $\square$

2.5.9 Bemerkung Eine zahme Gruppe $G < \mathrm{RCWA}(R)$ respektiert nach Satz 2.5.8 eine Partition $\mathcal{P}$ von R. Ist die Operation von G auf R transitiv, so ist $\mathcal{P}$ ein Blocksystem für G. Daher operiert G imprimitiv, also maximal einfach transitiv auf R. Nach Korollar 2.1.6 kann eine nichttriviale zahme Gruppe also kein Normalteiler von $\mathrm{RCWA}(R)$ sein.

2.5.10 Korollar *Eine Abbildung $\sigma \in \mathrm{RCWA}(R)$ ist genau dann zahm, wenn es ein $k \in \mathbb{N}$ so gibt, daß σ^k ganz ist.*

Beweis: Ist $\sigma \in \mathrm{RCWA}(R)$ zahm, so respektiert die zyklische Gruppe $\langle\sigma\rangle$ nach Satz 2.5.8 eine Partition $\mathcal{P}$. Ist k die Ordnung der von σ auf $\mathcal{P}$ induzierten Permutation, so fixiert und respektiert σ^k die Partition $\mathcal{P}$, und ist folglich ganz. Die Umkehrung ist trivial. $\square$

2.5.11 Beispiel Es seien g, h und $\mathcal{P}$ wie in Beispiel 2.5.3. Dann ist $\mathrm{ord}((gh)_{\mathcal{P}}) = 20$. Dementsprechend fixiert $(gh)^{20}$ die Partition $\mathcal{P}$, die Abbildung $(gh)^{20}$ ist also ganz.

Man erhält aus Satz 2.5.8 *en passant* ein einfaches Kriterium dafür, daß eine gegebene bijektive rcwa-Abbildung wild ist:

2.5.12 Folgerung *Es sei $\sigma \in \mathrm{RCWA}(R)$ nicht ausbalanciert. Dann ist σ wild.*

Beweis: Angenommen, die Abbildung σ sei nicht ausbalanciert, aber dennoch zahm. Dann respektiert σ nach Satz 2.5.8 eine Partition $\mathcal{P}$ von R in endlich viele Restklassen. Nach Voraussetzung gibt es nun jedoch ein Primelement $p \in \mathbb{P}(R)$, welches $\mathrm{Div}(\sigma)$, nicht jedoch $\mathrm{Mult}(\sigma)$ teilt oder umgekehrt. Wegen Lemma 1.3.1b, Aussage (3) und (4) kann o.E. ersteres angenommen werden. Mit Lemma 1.1.8, Aussage (1) schließt man auf die Existenz eines Zykels $(r_0(m_0), \dots, r_{l-1}(m_{l-1})) \subseteq \mathcal{P}$ so, daß $\exists i \in \{0, \dots, l-1\} : \ p | (m_i / m_{(i+1) \bmod l})$, aber $\nexists j \in \{0, \dots, l-1\} : \ p | (m_{(j+1) \bmod l} / m_j)$. Dies liefert offenbar einen Widerspruch. □

2.5.13 Beispiele Nach Folgerung 2.5.12 sind die Abbildungen α und ξ aus Beispiele 1.1.3 beide wild. Es sind jedoch nicht alle ausbalancierten Bijektionen auch zahm – vgl. etwa das Beispiel

$$\nu\nu^\alpha : \quad n \longmapsto \begin{cases} 2n+3 & \text{falls } n \in 0(3), \\ 2n+4 & \text{falls } n \in 1(3), \\ \frac{n+2}{2} & \text{falls } n \in 2(6), \\ \frac{n+3}{2} & \text{falls } n \in 5(6) \end{cases}$$

mit $\nu : n \mapsto n+1$. Die Abbildung $\nu\nu^\alpha$ ist zugleich ein Beispiel eines Produkts zahmer Abbildungen, welches selbst nicht zahm ist.

Zumindest die Surjektivität von σ muß man in Folgerung 2.5.12 tatsächlich voraussetzen, wie das Beispiel $f \in \mathrm{Rcwa}(\mathbb{Z}), \ n \mapsto 2n$ zeigt.

Das bis hierher erlangte Wissen über respektierte Partitionen erlaubt es, eine sehr enge Beziehung zwischen zahmen und ganzen rcwa-Gruppen aufzudecken:

2.5.14 Satz *Besitzt R die starke Restklassenteilbarkeitseigenschaft, dann sind genau die Abbildungen $g \in \mathrm{RCWA}(R)$ und genau die endlich erzeugten Gruppen $G < \mathrm{RCWA}(R)$ zahm, die zu einer ganzen Abbildung bzw. Gruppe konjugiert sind.*

Beweis: Es genügt, die Aussage für rcwa-Gruppen zu zeigen. Wegen Bemerkung 1.8.2 und Lemma 1.8.3, Aussage (3) sind zu ganzen Gruppen konjugierte endlich erzeugte rcwa-Gruppen zahm. Es genügt also zu zeigen, daß zahme Gruppen stets zu ganzen konjugiert sind. Es sei also $G < \mathrm{RCWA}(R)$ zahm. Nach Satz 2.5.8 respektiert die Gruppe G eine Partition $\mathcal{P}$ von R in endlich viele Restklassen. Gemäß Voraussetzung läßt sich $m \in R$ so wählen, daß $|R/mR| = |\mathcal{P}|$. Nach Lemma 2.1.4 gibt es nun eine auf allen Elementen von $\mathcal{P}$ affine Abbildung $\sigma \in \mathrm{RCWA}(R)$, welche eine Bijektion von $\mathcal{P}$ auf R/mR induziert. Die Gruppe G^σ respektiert nach Lemma 2.5.6, Aussage (2) statt deren Urbild deren Bild, und Lemma 2.5.4 liefert die Behauptung. □

2.5.15 Beispiel Es sei G die Gruppe aus Beispiel 2.5.3. Wie dort vorgeführt wurde, respektiert G eine Partition $\mathcal{P}_G$ der Länge 14. Entsprechend dem Vorgehen im Beweis von Satz 2.5.14 läßt sich eine Abbildung σ konstruieren, die die Partition $\mathcal{P}_G$ auf die Partition $\mathbb{Z}/14\mathbb{Z} = \{0(14), \dots, 13(14)\}$ abbildet:

$$\sigma \in \mathrm{RCWA}(\mathbb{Z}): \quad n \longmapsto \begin{cases} \frac{7n}{6} & \text{falls } n \in \ \ 0(12), \\ \frac{7n-1}{6} & \text{falls } n \in \ \ 1(12), \\ \frac{7n-9}{6} & \text{falls } n \in \ \ 3(12), \\ \frac{7n-10}{6} & \text{falls } n \in \ \ 4(12), \\ \frac{7n-11}{6} & \text{falls } n \in \ \ 5(12), \\ \frac{7n-12}{6} & \text{falls } n \in \ \ 6(12), \\ \frac{7n-13}{6} & \text{falls } n \in \ \ 7(12), \\ \frac{7n-21}{6} & \text{falls } n \in \ \ 9(12), \\ \frac{7n-22}{6} & \text{falls } n \in 10(12), \\ \frac{7n-23}{6} & \text{falls } n \in 11(12), \\ \frac{7n+106}{12} & \text{falls } n \in \ \ 2(24), \\ \frac{7n+76}{12} & \text{falls } n \in \ \ 8(24), \\ \frac{7n+46}{12} & \text{falls } n \in 14(24), \\ \frac{7n+16}{12} & \text{falls } n \in 20(24). \end{cases}$$

Damit ist G^σ ganz, und es ist $\mathrm{Mod}(G^\sigma) = 14$.

Die Gestalt von Bahnen unter der Operation von zahmen Gruppen auf dem zugrundeliegenden Ring läßt sich leicht beschreiben, wenn man weiß, wie Bahnen unter der Operation von Untergruppen der affinen Gruppe aussehen:

2.5.16 Satz *Ist die Gruppe $G < \mathrm{RCWA}(R)$ zahm und $\Omega \subseteq R$ eine Bahn unter der Operation von G auf R, dann gibt es eine Restklasse $r(m) \subseteq R$ und eine auf $r(m)$ operierende Untergruppe $U \leqslant \mathrm{AFF}(R)$ so, daß Ω gleich der Vereinigung der Bilder einer Bahn von U auf $r(m)$ unter endlich vielen nicht-konstanten affinen Abbildungen ist.*

Beweis: Nach Satz 2.5.8 gibt es eine Partition $\mathcal{P}$ von R in endlich viele Restklassen so, daß G auf $\mathcal{P}$ in natürlicher Weise als Permutationsgruppe operiert, und daß die Einschränkung eines beliebigen Elements von G auf eines der Elemente von $\mathcal{P}$ stets affin ist. Es sei N der Kern der Operation von G auf $\mathcal{P}$. Nach Lemma 2.1.3 operiert die Gruppe N auf einer beliebigen Restklasse in $\mathcal{P}$ wie eine Untergruppe von $\mathrm{AFF}(R)$. Da der Quotient G/N isomorph zu einer Untergruppe von $\mathrm{Sym}(\mathcal{P})$, also insbesondere endlich ist, besitzt jede Bahn von N auf R nur endlich viele Bilder unter Elementen von G, woraus wegen der Wahl von $\mathcal{P}$ die Behauptung folgt. $\square$

Im Falle $R = \mathbb{Z}$ hat dies folgende Konsequenzen:

2.5.17 Folgerung Die Bahnen unter der Operation von Untergruppen von

$$\mathrm{AFF}(\mathbb{Z}) = \langle \nu : n \mapsto n+1,\ \varsigma : n \mapsto -n \rangle$$

auf Restklassen von $\mathbb{Z}$ sind einelementige oder zweielementige Mengen oder Vereinigungen von einer oder zwei ganzen Restklassen. Nach Satz 2.5.16 ist eine Bahn auf $\mathbb{Z}$ unter der Operation einer zahmen Gruppe also entweder endlich oder eine Vereinigung endlich vieler Restklassen.

Die Bahnen unter der Operation einer zahmen Gruppe lassen sich rechnerisch im allgemeinen ohne weiteres bestimmen. Es läßt sich also insbesondere in der Regel leicht klären, ob eine gegebene zahme Gruppe transitiv auf dem Grundring operiert. Dies soll anhand eines Beispiels demonstriert werden:

2.5.18 Beispiel Mit RCWA kann man leicht nachrechnen, daß die Gruppe $G = \langle g, h \rangle$ aus Beispiel 2.5.3 transitiv auf $\mathbb{Z}$ operiert. Beispielsweise operiert die zyklische Gruppe $\langle [g, h] \rangle$ transitiv auf der Restklasse $2(6)$, die Bahn dieser Restklasse unter der Operation von G ist

$$\begin{aligned}\Omega := \{&2(6), 1(3), 0(6) \cup 5(6), 3(6) \cup 5(6), 3(6) \cup 2(12), 0(6) \cup 2(12),\\ &3(6) \cup 8(12), 0(6) \cup 8(12), 1(6) \cup 8(12), 1(6) \cup 2(12), 4(6) \cup 8(12),\\ &4(6) \cup 2(12), 4(6) \cup 5(6), 1(6) \cup 5(6), 0(6) \cup 4(6), 3(6) \cup 4(6),\\ &0(6) \cup 1(6), 1(6) \cup 3(6), 0(3), 5(6) \cup 2(12), 5(6) \cup 8(12)\},\end{aligned}$$

und die Vereinigung der 21 Elemente von Ω ist ganz $\mathbb{Z}$. Es sei nebenbei bemerkt, daß die Operation von G auf Ω primitiv ist, und daß die von G auf Ω induzierte Permutationsgruppe isomorph zu S_7 ist.

2.6 Zahme Darstellungen von Gruppen

Der nun folgende Satz liefert eine vollständige Klassifikation derjenigen Gruppen, welche treue zahme R-rcwa-Darstellungen besitzen. Um die Existenz einer solchen Darstellung für die betreffenden Gruppen zu zeigen, wird eine weiterentwickelte Form der Konstruktion aus Satz 2.1.2 verwendet. Der Beweis der anderen Richtung, also daß tatsächlich alle zahmen rcwa-Gruppen die angegebene Struktur besitzen, stützt sich auf respektierte Partitionen.

2.6.1 Satz *Eine Gruppe G besitzt genau dann eine treue zahme R-rcwa-Darstellung, wenn es ein $m \in \mathbb{N}$ so gibt, daß G isomorph zu einer Untergruppe des Kranzprodukts $\mathrm{AFF}(R) \wr \mathrm{S}_m$ ist.*

Beweis:

a) Es ist zu zeigen, daß eine Untergruppe von $\mathrm{AFF}(R) \wr \mathrm{S}_m$, $m \in \mathbb{N}$ stets eine treue zahme R-rcwa-Darstellung besitzt. Offenbar genügt es, eine solche Darstellung der Gruppe $\mathrm{AFF}(R) \wr \mathrm{S}_m$ selbst zu konstruieren. Wir wählen $a \in R \setminus (R^\times \cup \{0\})$, und setzen

$$\sigma \in \mathrm{RCWA}(R): \quad n \longmapsto \begin{cases} a \cdot n & \text{falls} \;\; n \notin 0(a^{m-1}), \\ n/a^{m-1} & \text{falls} \;\; n \in 0(a^{m-1}) \setminus 0(a^m), \\ n & \text{falls} \;\; n \in 0(a^m) \end{cases}$$

sowie

$$\tau \in \mathrm{RCWA}(R): \quad n \longmapsto \begin{cases} a \cdot n & \text{falls} \;\; n \notin 0(a), \\ n/a & \text{falls} \;\; n \in 0(a) \setminus 0(a^2), \\ n & \text{falls} \;\; n \in 0(a^2). \end{cases}$$

Dann ist bereits $\langle \sigma, \tau \rangle \cong \mathrm{S}_m$, denn ein m-Zykel und eine Transposition auf der Partition $\mathcal{P}$ von $R \setminus 0(a^m)$ in die Mengen $M_k := \{n \in R \mid a^k | n, \; a^{k+1} \nmid n\}$, $k = 0, \dots, m-1$ erzeugen die volle symmetrische Gruppe auf $\mathcal{P}$. Jetzt ist noch die affine Gruppe von R zu 'verbauen'. Hierzu bedienen wir uns des Monomorphismus

$$\phi: \; \mathrm{AFF}(R) \longrightarrow \mathrm{RCWA}(R), \quad (n \mapsto u \cdot n + k) \;\longmapsto\; \alpha(u,k),$$

wobei $\alpha(u,k)$ gegeben sei durch

$$n \longmapsto \begin{cases} u \cdot n + r \cdot (1-u) + k \cdot a^m & \text{falls} \;\; n \in r(a) \;\; \text{für} \;\; r \neq 0, \\ n & \text{falls} \;\; n \in 0(a) \end{cases}$$

(vgl. Lemma 2.1.3). Der Support des Bildes von ϕ ist M_0. Dies ist eine der von $\langle \sigma, \tau \rangle$ permutierten m Mengen. Folglich ist $\langle \sigma, \tau, \alpha(u,k) \rangle \cong \mathrm{AFF}(R) \wr \mathrm{S}_m$, wobei u über ein Erzeugendensystem von $R^\times$ und k über ein Erzeugendensystem von $(R,+)$ läuft.

Ferner sieht man, daß der Modul dieser Gruppe gleich a^m ist, die Zahmheitsbedingung also erfüllt ist.

b) Es sei $G < \mathrm{RCWA}(R)$ zahm. Zu zeigen ist, daß es ein $m \in \mathbb{N}$ so gibt, daß G isomorph zu einer Untergruppe von $\mathrm{AFF}(R) \wr \mathrm{S}_m$ ist. Nach Satz 2.5.8 gibt es eine Partition $\mathcal{P}$ von R in endlich viele Restklassen so, daß G auf $\mathcal{P}$ in natürlicher Weise als Permutationsgruppe operiert, und daß die Einschränkung eines beliebigen Elements von G auf eines der Elemente von $\mathcal{P}$ stets affin ist. Der Kern der Operation von G auf $\mathcal{P}$ ist daher isomorph zu einer Untergruppe von $\mathrm{AFF}(R)^{|\mathcal{P}|}$, und damit G selbst zu einer von $\mathrm{AFF}(R) \wr \mathrm{S}_{|\mathcal{P}|}$. □

Um auch den Fall $\mathrm{char}(R) \neq 0$ mit abzudecken, wurde die Konstruktion einer treuen Darstellung der S_m im ersten Teil des Beweises im Unterschied zu Satz 2.1.2 auf der multiplikativen anstatt auf der additiven Struktur von R aufgebaut. In Satz 2.1.2 findet die 1 Verwendung als Nicht-Torsionselement von $(R,+)$. Hier wurde stattdessen auf ein Nicht-Torsionselement a des Monoids $(R,\cdot)$ zurückgegriffen.

Satz 2.6.1 liefert ein Rezept, um Matrixdarstellungen zahmer Gruppen über K zu gewinnen. Zuvor ist aber eine Bezeichnung einzuführen, die im folgenden manchmal nützlich sein wird:

2.6.2 Definition Hinfort werde die treue Darstellung

$$\varphi: \ \mathrm{AFF}(K) \longrightarrow \mathrm{GL}(2,K), \quad (x \mapsto ax+b) \ \longmapsto \ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

bezeichnet als *Standarddarstellung* von $\mathrm{AFF}(K)$.

2.6.3 Korollar *Eine zahme Gruppe $G < \mathrm{RCWA}(R)$ besitzt stets eine treue Matrixdarstellung über K.*

Beweis: Nach Satz 2.6.1 ist jede zahme Gruppe $G < \mathrm{RCWA}(R)$ isomorph zu einer Untergruppe von $\mathrm{AFF}(R) \wr \mathrm{S}_m$ für genügend großes m. Es genügt also zu zeigen, daß die Gruppe $\mathrm{AFF}(R) \wr \mathrm{S}_m$ selbst eine treue Matrixdarstellung über K besitzt. Bekanntlich besitzt jedoch $\mathrm{AFF}(R)$ eine treue K-Darstellung vom Grad 2 (vgl. Definition 2.6.2) und S_m eine vom Grad m, beispielsweise die 'natürliche' Darstellung mittels Permutationsmatrizen. Folglich ist die nun naheliegende Bijektion des Kranzprodukts dieser Gruppen auf die Gruppe aller $2m \times 2m$ - Blockpermutationsmatrizen, deren von Null verschiedene Blöcke im Bild besagter Darstellung von $\mathrm{AFF}(R)$ liegen, die gesuchte treue Darstellung. $\square$

2.6.4 Beispiel Die Gruppe G aus Beispiel 2.5.3 respektiert eine Partition der Länge 14. Daher besitzt sie eine treue Matrixdarstellung vom Grad $2 \cdot 14 = 28$ über $\mathbb{Q}$.

Satz 2.6.1 liefert außerdem in Verbindung mit Satz 2.6A in [DM96] die folgende Aussage:

2.6.5 Korollar Es sei $k \in \mathbb{N}$ beliebig. Dann kann eine endliche Erweiterung $G \trianglerighteq N$ einer Untergruppe $N \leqslant \mathrm{AFF}(R)^k$ stets in $\mathrm{AFF}(R) \wr \mathrm{S}_m$ eingebettet werden, sofern m mindestens gleich dem Produkt von k und dem kleinsten Grad einer treuen Permutationsdarstellung von G/N ist. Eine solche Gruppe G besitzt also stets eine treue zahme R-rcwa-Darstellung.

Über manchen Ringen sind endlich erzeugte zahme rcwa-Gruppen sogar bereits endlich:

2.6.6 Korollar *Ist jede endlich erzeugte Untergruppe von* $\mathrm{AFF}(R)$ *endlich, dann sind auch endlich erzeugte zahme rcwa-Gruppen* $G < \mathrm{RCWA}(R)$ *endlich.*

Beweis: Sind endlich erzeugte Untergruppen von $\mathrm{AFF}(R)$ stets endlich, dann sind auch endlich erzeugte Untergruppen von $\mathrm{AFF}(R) \wr \mathrm{S}_m$ für gegebenes $m \in \mathbb{N}$ stets endlich: Angenommen, es gäbe eine endlich erzeugte unendliche Untergruppe. Dann hätte der Kern der Operation dieser Untergruppe auf der Menge der m Blöcke endlichen Index, wäre also ebenfalls unendlich, und nach Satz 1.6.11 in [Rob96] endlich erzeugt. Damit könnten allerdings die Projektionen dieses Kerns auf die m Blöcke nicht alle endlich sein, im Widerspruch zur Voraussetzung. Satz 2.6.1 liefert nun die Behauptung. □

Die Polynomringe $\mathbb{F}_q[x]$ genügen der Voraussetzung von Korollar 2.6.6, da sie Primzahlcharakteristik und endliche Einheitengruppe haben, und die durch die Gradabbildung induzierte Partition in endliche Teilmengen unter Multiplikation mit Einheiten invariant bleibt. Auf Ringe der Charakteristik 0 läßt sich Korollar 2.6.6 hingegen offensichtlich nicht anwenden, denn dort besitzt z.B. die zahme Abbildung $\nu : n \mapsto n+1$ unendliche Ordnung.

Im folgenden sollen die R-rcwa-Darstellungen 'geeigneter' endlicher Gruppen bis auf Konjugation klassifiziert werden.

2.6.7 Satz *Es besitze* R *die schwache Restklassenteilbarkeitseigenschaft, und es sei* G *eine endliche Gruppe mit zu den Ordnungen der Torsionselemente von* $\mathrm{AFF}(R)$ *teilerfremder Ordnung. Dann werden die* R*-rcwa-Darstellungen der Gruppe* G *bis auf Konjugation parametrisiert durch die nichtleeren Teilmengen der Menge der Äquivalenzklassen ihrer transitiven endlichen Permutationsdarstellungen.*

Beweis: Zu zeigen ist, daß sich R-rcwa-Darstellungen von G in bis auf Konjugation eindeutiger Weise Mengen nichtäquivalenter transitiver endlicher Permutationsdarstellungen zuordnen lassen. Aufgrund der Endlichkeit von G brauchen nur zahme Darstellungen betrachtet zu werden. Es seien solche gegeben durch $\varphi_i : G \to H_i < \mathrm{RCWA}(R)$, $i \in \{1,2\}$, und es seien $\mathcal{P}_1$ und $\mathcal{P}_2$ von H_1 bzw. H_2 respektierte Partitionen von R (vgl. Satz 2.5.8).

Im folgenden sei weiter stets $i \in \{1,2\}$. Aufgrund der Teilerfremdheitsbedingung und der Endlichkeit von G ist der Kern der Operation von H_i auf $\mathcal{P}_i$ trivial, es ist also bereits $(H_i)_{\mathcal{P}_i} \cong H_i$. Es seien $\Omega_{i,j}$ die Bahnen von $(H_i)_{\mathcal{P}_i}$ auf $\mathcal{P}_i$, und $H_{i,j}$ die auf den Mengen $\Omega_{i,j}$ induzierten transitiven Permutationsgruppen. Da H_i treu auf $\mathcal{P}_i$ operiert, induzieren die Gruppen $H_{i,j}$ auf den Mengen $\cup\Omega_{i,j} \subseteq R$ unendliche Serien zu $H_{i,j}$ permutationsisomorpher (endlicher) Permutationsgruppen. Es ist zu zeigen, daß H_1 und H_2 genau dann in $\mathrm{RCWA}(R)$ zueinander konjugiert sind, wenn die Mengen der Permutationsisomorphietypen von Gruppen $H_{1,j}$ und $H_{2,j}$ miteinander übereinstimmen.

Notwendig ist diese Bedingung sicher, da nicht permutationsisomorphe Permutationsgruppen nicht einmal in der vollen symmetrischen Gruppe $\mathrm{Sym}(R)$ zueinander konjugiert sind. Es folgt, daß die gesuchte Zuordnung zumindest wohldefiniert ist. Um zu sehen, daß die Bedingung auch hinreichend ist, gilt es zu überlegen, wie sich verschiedene Anzahlen permutationsisomorpher $H_{1,j}$ und $H_{2,j}$ 'aufeinanderkonjugieren' lassen. Hierzu verfeinert man die Partitionen $\mathcal{P}_i$ wie folgt zu von den Gruppen H_i ebenfalls respektierten Partitionen $\tilde{\mathcal{P}}_i$ so, daß die Gruppen $(H_i)_{\tilde{\mathcal{P}}_i}$ zueinander permutationsisomorph sind:

1. Setze $\mathcal{H}_i$ gleich der Menge der Gruppen $H_{i,j}$, und initialisiere $\tilde{\mathcal{P}}_i$ mit $\mathcal{P}_i$.

2. Wähle ein $H_{1,j} \in \mathcal{H}_1$.

3. Es seien $j_{i,1}, \ldots, j_{i,k_i}$ die Indices der zu $H_{1,j}$ permutationsisomorphen Gruppen in $\mathcal{H}_1 \cup \mathcal{H}_2$. Ist $k_1 = k_2$, so fahre fort bei Schritt (5).

4. Setze $t_i := \mathrm{kgV}(k_1, k_2)/k_i$, und tue für alle $\Omega \in \{\Omega_{i,j_{i,1}}, \ldots, \Omega_{i,j_{i,k_i}}\}$ folgendes:

   - Wähle eine Restklasse $r(m) \in \Omega$.
   - Schreibe $r(m)$ als disjunkte Vereinigung von t_i Restklassen $r_1(m_1), \ldots, r_{t_i}(m_{t_i})$ – dies geht aufgrund der Voraussetzung der schwachen Restklassenteilbarkeitseigenschaft.
   - Setze $\tilde{\mathcal{P}}_i := \tilde{\mathcal{P}}_i \setminus \Omega$.
   - Für $l \in \{1, \ldots, t_i\}$ setze $\tilde{\mathcal{P}}_i := \tilde{\mathcal{P}}_i \cup r_l(m_l)^{H_i}$.

   Nach Konstruktion respektiert H_i die Partition $\tilde{\mathcal{P}}_i$ jetzt immer noch, und da der Kern der Operation von H_i auf $\mathcal{P}_i$ trivial ist, bleiben ferner die Permutationsisomorphietypen der auf Teilmengen dieser Partitionen induzierten transitiven Permutationsgruppen invariant.

   Jetzt induzieren H_1 auf $\tilde{\mathcal{P}}_1$ und H_2 auf $\tilde{\mathcal{P}}_2$ dieselbe Anzahl $\mathrm{kgV}(k_1, k_2)$ zu $H_{1,j}$ permutationsisomorpher Bilder.

5. Setze $\mathcal{H}_i := \mathcal{H}_i \setminus \{H_{i,j_{i,1}}, \ldots, H_{i,j_{i,k_i}}\}$.

6. Falls $\mathcal{H}_i \neq \emptyset$, fahre fort bei Schritt (2), andernfalls fertig.

Wegen Lemma 2.1.4 und Lemma 2.5.6, Aussage (2) gibt es ein $\sigma \in \mathrm{RCWA}(R)$ so, daß H_1^σ die Partition $\tilde{\mathcal{P}}_2$ respektiert, und daß $(H_1^\sigma)_{\tilde{\mathcal{P}}_2}$ permutationsisomorph zu $(H_1)_{\tilde{\mathcal{P}}_1}$ ist. Die Gruppen $(H_1^\sigma)_{\tilde{\mathcal{P}}_2}$ und $(H_2)_{\tilde{\mathcal{P}}_2}$ sind nun in $\mathrm{Sym}(\tilde{\mathcal{P}}_2) < \mathrm{RCWA}(R)$ zueinander konjugiert. Damit sind aber auch $(H_1)_{\tilde{\mathcal{P}}_1}$ und $(H_2)_{\tilde{\mathcal{P}}_2}$, und wegen der Treue der Gruppenoperationen auf den respektierten Partitionen auch H_1 und H_2 in $\mathrm{RCWA}(R)$ zueinander konjugiert. Dies zeigt die Injektivität der Zuordnung.

Ein direktes Produkt endlicher transitiver Permutationsgruppen läßt sich stets ohne 'überzählige' Fixpunkte in $\mathrm{Sym}(\mathcal{P}) < \mathrm{RCWA}(R)$ einbetten, sofern die Kardinalität von $\mathcal{P}$ gleich dessen Grad ist. Da R die schwache Restklassenteilbarkeitseigenschaft besitzt, gibt es immer eine Partition $\mathcal{P}$ von R geeigneter Länge. Daher ist die Zuordnung ebenfalls surjektiv. □

2.6.8 Beispiel Es sollen die Äquivalenzklassen ganzzahliger rcwa - Darstellungen der nichtabelschen Gruppe G_{21} der Ordnung 21 gezählt werden. An treuen transitiven Darstellungen besitzt diese Gruppe die reguläre Darstellung vom Grad 21 und eine Darstellung vom Grad 7 auf der Menge der Nebenklassen nach einer zyklischen Untergruppe der Ordnung 3. Darüberhinaus gibt es eine transitive Darstellung vom Grad 3, deren Kern der Normalteiler von G_{21} der Ordnung 7 ist, und wie immer natürlich die triviale Darstellung. Man kommt also auf 4 nichtäquivalente transitive Permutationsdarstellungen. Da eine Menge der Kardinalität 4 genau $2^4 - 1 = 15$ nichtleere Teilmengen besitzt, ist nach Satz 2.6.7 die Anzahl der nichtäquivalenten ganzzahligen rcwa-Darstellungen von G_{21} gleich 15. Hiervon sind (nicht im allgemeinen, aber in diesem Fall) genau diejenigen treu, die zu Mengen gehören, die mindestens eine der beiden treuen Darstellungen enthalten. Diese lassen sich leicht abzählen – es handelt sich um genau 12 Stück. Natürlich hätte man genausogut auch jeden anderen Ring als $\mathbb{Z}$, der den Voraussetzungen des Satzes genügt, also z.B. $\mathbb{F}_2[x]$ oder $\mathbb{Z}_{(2)}$, zugrunde legen können und wäre auf dieselben Ergebnisse gekommen.

2.7 Konjugiertenklassen von RCWA(R)

Das folgende Korollar zu Satz 2.6.7 klärt im Falle $\mathrm{char}(R) = 0$ vollständig, wieviele Konjugiertenklassen von Elementen einer vorgegebenen endlichen Ordnung die Gruppe $\mathrm{RCWA}(R)$ besitzt:

2.7.1 Korollar *(Anzahl der Konjugiertenklassen von Torsionselementen in* $\mathrm{RCWA}(R)$*.) Es besitze R die schwache Restklassenteilbarkeitseigenschaft, und es sei $r \in \mathbb{N}$. Dann gilt:*

a) *Besitzt der Ring R eine Torsionseinheit, deren Ordnung zu r nicht teilerfremd ist, dann besitzt die Gruppe* $\mathrm{RCWA}(R)$ *unendlich viele Konjugiertenklassen von Elementen der Ordnung r.*

b) *Ist r teilerfremd zu den Ordnungen sämtlicher Torsionselemente von* $\mathrm{AFF}(R)$*, dann besitzt die Gruppe* $\mathrm{RCWA}(R)$ *genau so viele Konjugiertenklassen von Elementen der Ordnung r, wie es Teilmengen der Menge der Teiler von r mit kleinstem gemeinsamen Vielfachen r gibt.*

Beweis:

a) Es genügt, eine Konstruktionsvorschrift für rcwa-Abbildungen der Ordnung r mit jeder vorgegebenen endlichen Anzahl k von Fixpunkten anzugeben, die um 1 größer ist als die Kardinalität eines geeignet gewählten Restklassenrings von R. Diese Abbildungen sind dann nicht einmal in der vollen symmetrischen Gruppe $\mathrm{Sym}(R)$ zueinander konjugiert.

Es sei $u \neq 1$ eine Torsionseinheit des Rings R, deren Ordnung r teilt. Ferner sei $a \in R \setminus (R^\times \cup \{0\})$. Wir wählen $m \in R$ so, daß $|R/mR| = k-1$, und setzen

$$\sigma_u \in \mathrm{RCWA}(R): \ n \ \longmapsto \ un + (n \mod m)(1-u), \text{ sowie}$$

$$\sigma_r \in \mathrm{RCWA}(R): \ n \ \longmapsto \begin{cases} a \cdot n & \text{falls } n \notin 0(a^{r-1}), \\ n/a^{r-1} & \text{falls } n \in 0(a^{r-1}) \setminus 0(a^r), \\ u \cdot n & \text{falls } n \in 0(a^r). \end{cases}$$

Die Abbildung σ_u hat dieselbe Ordnung wie u und als Fixpunkte die $k-1$ Elemente von $\mathfrak{R}(m)$, und σ_r hat die Ordnung r und den einzigen Fixpunkt 0.

Es seien nun $f_1, f_2 \in \mathrm{Rcwa}(R)$ injektive Abbildungen, deren Bilder eine Partition von R bilden – solche Abbildungen gibt es nach Lemma 2.1.4. Wegen $\mathrm{ord}(u)|r$ ist $\sigma := \sigma_u^{\pi_{f_1}} \cdot \sigma_r^{\pi_{f_2}}$ wie gewünscht eine Abbildung der Ordnung r mit genau k Fixpunkten.

b) Hier läßt sich Satz 2.6.7 anwenden. Man macht dabei Gebrauch von der bekannten Formel für die Anzahl transitiver Permutationsdarstellungen zyklischer Gruppen. □

2.7.2 Folgerung Nach Korollar 2.7.1 besitzt die Gruppe $\mathrm{RCWA}(\mathbb{Z})$ jeweils

- unendlich viele Konjugiertenklassen von Elementen einer vorgegebenen geraden Ordnung, aber nur jeweils
- endlich viele Konjugiertenklassen von Elementen einer vorgegebenen ungeraden Ordnung.

Für Ringe der Charakteristik p deckt die Aussage von Korollar 2.7.1 immerhin noch alle zu p teilerfremden Ordnungen von Elementen von $\mathrm{RCWA}(R)$ ab.

2.8 Mehr zu respektierten Partitionen

In den vorangegangenen drei Abschnitten wurde bereits dargelegt, daß das Konzept einer respektierten Partition in den Beweisen diverser Strukturaussagen zu rcwa-Gruppen eine Schlüsselrolle spielt.

In diesem Abschnitt werden die dortigen Überlegungen fortgeführt. Konkret wird etwa untersucht, wie sich die von einer zahmen rcwa-Abbildung auf einer respektierten Partition induzierte Permutation durch geeignete Wahl der Partition beeinflussen läßt. Dies ist von Interesse im Zusammenhang mit der Suche nach Normalteilern von $\mathrm{RCWA}(R)$. Desweiteren wird untersucht, unter welchen Voraussetzungen an den zugrundeliegenden Ring R alle zahmen Abbildungen sogar bereits endliche Ordnung haben. Schließlich wird ein Kriterium dafür hergeleitet, daß sich zwei gegebene Partitionen von R in dieselbe Anzahl von Restklassen vermittels einer zahmen rcwa-Abbildung aufeinander abbilden lassen.

Zunächst wird eine Aussage zur Verfeinerbarkeit respektierter Partitionen benötigt:

2.8.1 Lemma *Es sei $G < \mathrm{RCWA}(R)$ zahm, $\mathcal{P}$ eine respektierte Partition von G und $t \in \mathbb{N}$ Kardinalität eines Restklassenrings von R. Dann läßt sich $\mathcal{P}$ verfeinern zu einer von G ebenfalls respektierten Partition $\tilde{\mathcal{P}}$ der Länge $t \cdot |\mathcal{P}|$.*

Beweis: Da R nach Voraussetzung einen Restklassenring der Kardinalität t besitzt, läßt sich eine Restklasse $r(m) \in \mathcal{P}$ stets schreiben als Vereinigung von t Restklassen $r_1(\tilde{m}), \ldots, r_t(\tilde{m})$ gleichen Moduls. Dies liefert eine Partition $\tilde{\mathcal{P}}$ von R in $t \cdot |\mathcal{P}|$ Restklassen. Die Einschränkungen der Elemente von G auf eine Restklasse $r(m) \in \mathcal{P}$ sind nach Voraussetzung stets affin. Deshalb bilden die Bilder der Restklassen $r_1(\tilde{m}), \ldots, r_t(\tilde{m})$ in einer Partition von $r(m)$ unter einem Element $g \in G$ stets eine Partition des Bildes von $r(m)$ unter g in Restklassen gleichen Moduls. Es folgt, daß die Gruppe G auch auf der Partition $\tilde{\mathcal{P}}$ als Permutationsgruppe operiert. □

Daß zwei gegebene zahme Gruppen notwendigerweise eine gemeinsame zahme Obergruppe besitzen, ist offenkundig falsch. Es läßt sich aber folgende Aussage treffen:

2.8.2 Lemma *Besitzt R die starke Restklassenteilbarkeitseigenschaft, so besitzen je zwei zahme Gruppen $G, H < \mathrm{RCWA}(R)$ zueinander konjugierte zahme Obergruppen.*

Beweis: Es seien $\mathcal{P}_G$ und $\mathcal{P}_H$ respektierte Partitionen von G bzw. H. Da der Ring R nach Voraussetzung Restklassenringe jeder von 0 verschiedenen endlichen Kardinalität besitzt, lassen sich $\mathcal{P}_G$ und $\mathcal{P}_H$ nach Lemma 2.8.1 verfeinern zu von G bzw. H ebenfalls respektierten Partitionen $\tilde{\mathcal{P}}_G$ und $\tilde{\mathcal{P}}_H$ der gleichen Länge $l := \mathrm{kgV}(|\mathcal{P}_G|, |\mathcal{P}_H|)$. Nach Lemma 2.1.4 gibt es nun eine auf allen Elementen von $\tilde{\mathcal{P}}_G$ affine Abbildung $\sigma \in \mathrm{RCWA}(R)$ so, daß $\tilde{\mathcal{P}}_G^\sigma = \tilde{\mathcal{P}}_H$. Setzt man $\tilde{G} := G^\sigma$ und $\tilde{H} := H^{\sigma^{-1}}$, so respektiert nach Lemma 2.5.6, Aussage (2) die Gruppe $\tilde{G}$ die Partition $\tilde{\mathcal{P}}_H$ und die Gruppe $\tilde{H}$ die Partition $\tilde{\mathcal{P}}_G$. Die beiden Gruppen $\hat{G} := \langle G, \tilde{H} \rangle > G$ und $\hat{H} := \langle \tilde{G}, H \rangle > H$ respektieren nach Lemma 2.5.6, Aussage (1) ebenfalls die Partitionen $\tilde{\mathcal{P}}_G$ bzw. $\tilde{\mathcal{P}}_H$. Daher sind sie nach Satz 2.5.8 zahm. Ferner gilt wie gefordert $\hat{G}^\sigma = \hat{H}$. □

Es folgt unmittelbar:

2.8.3 Folgerung Besitzt der Ring R die starke Restklassenteilbarkeitseigenschaft und sind die Abbildungen $g, h \in \mathrm{RCWA}(R)$ zahm, dann gibt es stets ein $\sigma \in \mathrm{RCWA}(R)$ so, daß die von g und h^σ erzeugte Gruppe, also insbesondere $g \cdot h^\sigma$, zahm ist.

2.8.4 Bemerkung Man kann einer zahmen rcwa-Abbildung g nicht so ohne weiteres eine Signatur zuordnen. Naheliegend wäre es zwar, die Signatur von g einfach gleich der Signatur der von g auf einer respektierten Partition induzierten Permutation zu setzen.

Der Haken an der Sache ist, daß diese nicht eindeutig bestimmt ist. Häufig respektiert eine zahme rcwa-Abbildung sowohl Partitionen, auf denen sie eine gerade wie auch Partitionen, auf denen sie eine ungerade Permutation induziert.

Beispielsweise respektiert die Abbildung $\nu \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto n+1$ die triviale Partition sowie die Partitionen $\{0(2), 1(2)\}$ und $\{0(3), 1(3), 2(3)\}$ von $\mathbb{Z}$ und induziert auf diesen die Identität, eine Transposition bzw. einen 3-Zykel.

Eine nützliche Aussage läßt sich aber dennoch treffen:

2.8.5 Lemma *Ist* $\mathrm{char}(R) = 0$, *besitzt R die schwache Restklassenteilbarkeitseigenschaft und ist der Exponent der Einheitengruppe von R endlich, dann gibt es zu jeder zahmen Abbildung $\sigma \in \mathrm{RCWA}(R)$ unendlicher Ordnung ein $e \in \mathbb{N}$ und eine von σ^e respektierte Partition $\mathcal{P}$ von R so, daß σ^e auf $\mathcal{P}$ eine Transposition induziert. Zu vorgegebenem $l \in \mathbb{N}$ lassen sich ferner e und $\mathcal{P}$ so wählen, daß $|\mathcal{P}| \geqslant l$.*

Beweis: Nach Satz 2.5.8 und Lemma 2.8.1 respektiert σ eine Partition $\tilde{\mathcal{P}}$ mit $|\tilde{\mathcal{P}}| \geqslant l$. Es sei $e_1 := \mathrm{ord}(\sigma_{\mathcal{P}})$, $e_2 := \exp(R^\times)$ und $e := e_1 \cdot e_2$. Dann respektiert und fixiert σ^{e_1} die Partition $\tilde{\mathcal{P}}$, die affinen Teilabbildungen von σ^{e_1} auf den Restklassen $r(m) \in \tilde{\mathcal{P}}$ sind also nach Lemma 2.1.3 von der Form $n \mapsto u_r n + r(1-u_r) + \tilde{k}_r m$ für $u_r \in R^\times$ und $\tilde{k}_r \in R$. Durch schlichtes Potenzieren in $\mathrm{AFF}(R)$ sieht man jetzt, daß die affinen Teilabbildungen von $\sigma^e = \sigma^{e_1 e_2}$ auf ebendiesen Restklassen von der Form $n \mapsto n + k_r m$ mit $k_r \in R$ sind. Wegen $\mathrm{ord}(\sigma) = \infty$ ist $\sigma^e \neq 1$. Folglich läßt sich eine Restklasse $r(m) \in \tilde{\mathcal{P}}$ so wählen, daß $k_r \neq 0$. Nun läßt sich eine neue, von σ^e ebenfalls respektierte Partition $\mathcal{P}$ von R konstruieren, indem man in $\tilde{\mathcal{P}}$ erstens die Restklasse $r(m)$ aufspaltet in Restklassen (mod $k_r m$) und zweitens eine dieser Restklassen weiter aufspaltet in zwei Restklassen. Dies ist möglich, da vorausgesetzt wurde, daß R die schwache Restklassenteilbarkeitseigenschaft besitzt. Diese Restklassen haben dann nach Lemma 1.1.10 notwendigerweise beide denselben Modul $\tilde{m}$ mit $|R/\tilde{m}R| = 2 \cdot |R/k_r m R|$, denn die einzige Partition von 1 in genau zwei Stammbrüche ist $1 = 1/2 + 1/2$. Die affine Teilabbildung $n \mapsto n + k_r m$ bildet nun die Restklassen (mod $k_r m$) auf sich selbst ab und vertauscht die beiden letztgenannten Restklassen. Da die Permutation $(\sigma^e)_{\mathcal{P}}$ den 'Rest' von $\mathcal{P}$ konstruktionsgemäß fixiert, handelt es sich wie gewünscht um eine Transposition. □

Es sei bemerkt, daß die Forderung $\mathrm{char}(R) = 0$ im Beweis gar nicht benötigt wird – sie ist aber auch redundant, d.h. deren Fortlassen würde die Aussage nicht verschärfen:

2.8.6 Satz *Ist* $\mathrm{char}(R) \neq 0$ *und* $\exp(R^\times) < \infty$, *so haben alle zahmen Abbildungen $\sigma \in \mathrm{RCWA}(R)$ endliche Ordnung.*

Beweis: Es sei $p := \mathrm{char}(R)$, $\sigma \in \mathrm{RCWA}(R)$ zahm, $\mathcal{P}$ eine von σ respektierte Partition und $e := \mathrm{ord}(\sigma_{\mathcal{P}}) \cdot \exp(R^\times)$. Dann respektiert und fixiert σ^e die Partition $\mathcal{P}$, und die affinen Teilabbildungen von σ^e sind von der Form $n \mapsto n + k \cdot \mathrm{Mod}(\sigma^e)$ für gewisse $k \in R$. Man schließt sofort, daß die affinen Teilabbildungen von $(\sigma^e)^p$ von der Form $n \mapsto n + p \cdot k \cdot \mathrm{Mod}(\sigma^e) = n$ sind, was die Behauptung impliziert. □

Die Konstruktion aus dem Beweis von Lemma 2.8.5 soll anhand eines einfachen Beispiels veranschaulicht werden:

2.8.7 Beispiel Die Abbildungen g und h sowie die Partition $\mathcal{P}$ seien gegeben wie in Beispiel 2.5.3. Der Ring der ganzen Zahlen genügt offenbar den Voraussetzungen, und das Produkt $\sigma := gh$ ist eine zahme Abbildung unendlicher Ordnung. Damit ist Lemma 2.8.5 auf σ anwendbar. Es gibt also ein $e \in \mathbb{N}$ und eine Verfeinerung $\mathcal{P}'$ von $\mathcal{P}$ so, daß σ^e auf $\mathcal{P}'$ eine Transposition induziert. Nachrechnen ergibt $\mathrm{ord}(\sigma_{\mathcal{P}}) = 20 =: e_1$, und es ist $\exp(\mathbb{Z}^\times) = 2 =: e_2$. Es ist also $e_1 e_2 = 40 =: e$. Wieder durch Nachrechnen sieht man, daß σ^e gegeben ist durch

$$n \longmapsto \begin{cases} n + 120 & \text{falls } n \in 0(6) \cup 1(6), \\ n - 96 & \text{falls } n \in 2(6), \\ n - 48 & \text{falls } n \in 3(6) \cup 4(6) \cup 5(6). \end{cases}$$

Wir entscheiden uns dafür, die Restklasse 3(12) in 4 Restklassen (mod 48) aufzuteilen, und setzen $\mathcal{P}' := (\mathcal{P} \setminus \{3(12)\}) \cup \{3(48), 15(48), 27(48), 39(48)\}$. Desweiteren wählen wir aus den Restklassen (mod 48) die Restklasse 3(48) und teilen sie in 2 Restklassen (mod 96), d.h. wir setzen $\mathcal{P}' := (\mathcal{P}' \setminus \{3(48)\}) \cup \{3(96), 51(96)\}$. Damit ist

$$\begin{aligned} \mathcal{P}' = \{&0(12), 1(12),\ 4(12),\ 5(12),\ 6(12),\ 7(12),\ 9(12), 10(12), 11(12), \\ &2(24), 8(24), 14(24), 20(24), 15(48), 27(48), 39(48),\ 3(96), 51(96)\}, \end{aligned}$$

und die Abbildung σ^e induziert auf $\mathcal{P}'$ die Transposition $(3(96), 51(96))$.

Nach Lemma 2.1.4 lassen sich je zwei Partitionen von R in dieselbe Anzahl von Restklassen stets durch bijektive rcwa-Abbildungen aufeinander abbilden. Es soll untersucht werden, unter welchen Umständen dies sogar mit zahmen Abbildungen geht. Die Bedingung, die dabei herauskommt, läßt sich wohl am einfachsten vermittels einer Eigenschaft gewisser gewichteter Graphen beschreiben:

2.8.8 Definition Es sei Γ ein endlicher, ungerichteter und schlingenfreier Graph mit Knoten $v_i,\ i \in \{1, \dots, k\}$, denen jeweils Gewichte $n_i \in \mathbb{N}$ zugeordnet seien. Der Graph Γ heiße *ausgleichbar*, falls es möglich ist, auf die folgende Weise in endlich vielen Schritten zu erreichen, daß alle n_i gleich sind:

1. Wähle ein Paar (v_i, v_j) adjazenter Knoten von Γ.

2. Setze $n_i := n_i + 1$ und $n_j := n_j + 1$.

3. Falls noch nicht alle n_i gleich sind, weiter bei Schritt (1), sonst fertig.

2.8.9 Satz *Der Ring R besitze die schwache Restklassenteilbarkeitseigenschaft, es sei $k \in \mathbb{N}$ und es seien*

$$\mathcal{P}_i \; = \; \{r_{i,1}(m_{i,1}), r_{i,2}(m_{i,2}), \dots, r_{i,k}(m_{i,k})\}, \quad i \in \{1,2\}$$

Partitionen von R in jeweils k Restklassen. Ferner sei Γ der bipartite Graph mit den $2k$ Knoten $r_{i,j}(m_{i,j})$, derer zwei genau dann adjazent seien, wenn sie sich als Mengen nichttrivial schneiden. Es sei m das kleinste gemeinsame Vielfache der Moduln der Restklassen in $\mathcal{P}_1$ und $\mathcal{P}_2$. Den Knoten $r_{i,j}(m_{i,j})$ von Γ seien die Gewichte $n_{i,j} := |R/mR|/|R/m_{i,j}R|$ zugeordnet. Ist der Graph Γ ausgleichbar und ist $G \leqslant \mathrm{RCWA}(R)$ eine rcwa-Gruppe mit $\mathrm{Sym}(\mathcal{P}) < G$ für jede Partition $\mathcal{P}$ von R in eine hinreichend große endliche Anzahl von Restklassen, dann gibt es ein zahmes Element $\sigma \in G$ so, daß $\mathcal{P}_1^\sigma = \mathcal{P}_2$.

Beweis: Wegen Lemma 2.1.4, Satz 2.5.8 und Lemma 2.8.1 genügt es zu zeigen, daß die Partitionen $\mathcal{P}_1$ und $\mathcal{P}_2$ eine gemeinsame Verfeinerung $\mathcal{P} = \{r_1(m_1), r_2(m_2), \dots, r_l(m_l)\}$ so besitzen, daß die Restklassen $r_{1,j}(m_{1,j})$ und $r_{2,j}(m_{2,j})$ für beliebiges $j \in \{1, \dots, k\}$ Vereinigungen jeweils gleich vieler Restklassen $r_i(m_i)$ aus $\mathcal{P}$ sind. Setzt man $m := \mathrm{kgV}_{i,j}\, m_{i,j}$, dann sind die Knoten $r_{i,j}(m_{i,j})$ des Graphen Γ Vereinigung von genau $n_{i,j}$ Restklassen (mod m). Da Γ ausgleichbar ist und R die schwache Restklassenteilbarkeitseigenschaft besitzt, läßt sich die gesuchte Partition $\mathcal{P}$ ausgehend von der Partition R/mR völlig analog zu dem in Definition 2.8.8 angegebenen Verfahren gewinnen – die Addition von 1 zu $n_{i,j}$ entspricht einfach der 'Teilung' einer in $r_{i,j}(m_{i,j})$ liegenden Restklasse der Partition in zwei disjunkte andere Restklassen. Man beachte hierzu, daß die geteilte Restklasse stets auch in genau einem zu $r_{i,j}(m_{i,j})$ adjazenten Knoten $r_{3-i,\tilde{j}}(m_{3-i,\tilde{j}})$ von Γ liegt, und daß sich letzterer durch eine geeignete Wahl der zu teilenden Restklasse frei unter den zu $r_{i,j}(m_{i,j})$ adjazenten Knoten wählen läßt. □

2.8.10 Beispiel Als kleines Beispiel soll hier die Konstruktion einer zahmen Abbildung $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ so angegeben werden, daß $\mathcal{P}_1^\sigma = \mathcal{P}_2$ gilt für $\mathcal{P}_1 := \{0(2), 1(4), 3(4)\}$ und $\mathcal{P}_2 := \{0(3), 1(3), 2(3)\}$. Man sieht leicht, daß der Graph Γ hier der vollständige bipartite Graph mit 6 Knoten ist. Die Knoten $0(2), 1(4), 3(4), 0(3), 1(3), 2(3)$ haben nach der Setzung in Satz 2.8.9 die Gewichte $6, 3, 3, 4, 4, 4$. Man sieht, daß Γ ausgleichbar ist, indem man in dem in Definition 2.8.8 angegebenen Verfahren hintereinander die Gewichte für die Paare $(1(4), 0(3))$, $(1(4), 0(3))$, $(1(4), 1(3))$, $(3(4), 1(3))$, $(3(4), 2(3))$ und $(3(4), 2(3))$ von Knoten von Γ inkrementiert. Ferner ist $m = \mathrm{kgV}(2, 3, 4) = 12$, begonnen wird also mit der Partition $\mathbb{Z}/12\mathbb{Z}$. Entsprechendes Verfeinern der Partitionen $\mathcal{P}_1$ und $\mathcal{P}_2$ liefert

$$\{0(12), 2(12), 4(12), 6(12), 8(12), 10(12)\} \cup \{1(12), 5(12), 9(12)\} \cup \{3(12), 7(12), 11(12)\}$$

bzw.

$$\{0(12), 3(12), 6(12), 9(12)\} \cup \{1(12), 4(12), 7(12), 10(12)\} \cup \{2(12), 5(12), 8(12), 11(12)\}.$$

Den genannten Manipulationen der Gewichte der Knoten von Γ entsprechende Teilungen von Restklassen sind zum Beispiel (in zu obigen Angaben konsistenter Reihenfolge)

$$\begin{array}{lll} 9(12) \rightsquigarrow 9(24) \cup 21(24), & 9(24) \rightsquigarrow 9(48) \cup 33(48), & 1(12) \rightsquigarrow 1(24) \cup 13(24), \\ 7(12) \rightsquigarrow 7(24) \cup 19(24), & 11(12) \rightsquigarrow 11(24) \cup 23(24), & 11(24) \rightsquigarrow 11(48) \cup 35(48). \end{array}$$

Dies liefert die Partition

$$\begin{aligned} \mathcal{P} \;=\; \{&0(12),\; 2(12),\; 4(12), 6(12), 8(12), 10(12),\; 1(24), 13(24),\; 5(12), \\ &9(48), 33(48), 21(24), 3(12), 7(24), 19(24), 11(48), 35(48), 23(24)\}. \end{aligned}$$

Eine Abbildung σ mit den gewünschten Eigenschaften läßt sich nun unschwer anhand von Lemma 2.1.4 konstruieren – man erhält z.B.

$$\sigma \in \mathrm{RCWA}(\mathbb{Z}): \quad n \longmapsto \begin{cases} n & \text{falls } n \in \ \ 0(12) \cup 1(12) \cup 11(12), \\ n+1 & \text{falls } n \in \ \ 2(12), \\ n-1 & \text{falls } n \in \ \ 3(12) \cup 5(12), \\ n+2 & \text{falls } n \in \ \ 4(12), \\ 4n-15 & \text{falls } n \in \ \ 6(12), \\ 4n+1 & \text{falls } n \in \ \ 8(12), \\ 2n+1 & \text{falls } n \in 10(12), \\ \frac{n+3}{2} & \text{falls } n \in \ \ 7(24), \\ \frac{n+5}{2} & \text{falls } n \in \ \ 9(24), \\ \frac{n-3}{2} & \text{falls } n \in 19(24), \\ \frac{n-1}{2} & \text{falls } n \in 21(24). \end{cases}$$

Die Abbildung σ ist nebenbei bemerkt nicht nur zahm, sondern besitzt sogar endliche Ordnung – man kann nachrechnen, daß $\mathrm{ord}(\sigma) = 30$. Ohne den Wunsch nach einer zahmen Abbildung hätte auch die Abbildung α aus Beispiele 1.1.3 der Bedingung genügt, denn es ist ebenfalls $\mathcal{P}_1^\alpha = \mathcal{P}_2$.

2.9 Das Erzeugnis der zahmen Abbildungen in RCWA(Z)

In den vorangegangenen Abschnitten wurde die Struktur zahmer rcwa-Abbildungen und -Gruppen näher untersucht. Es ist naheliegend zu fragen, welche Struktur die von *allen* zahmen Abbildungen erzeugte Untergruppe N von $\mathrm{RCWA}(\mathbb{Z})$ besitzt.

Wegen Lemma 1.8.3 handelt es sich um einen Normalteiler. In diesem Abschnitt soll ein elegantes Erzeugendensystem desselben vorgestellt werden.

Darüberhinaus wird die Collatz'sche Permutation α aus Beispiele 1.1.3 in 73 Faktoren aus dem besagten Erzeugendensystem sowie eine ganze Abbildung faktorisiert. Dies zeigt konstruktiv, daß $\alpha \in N$.

2.9.1 Definition Es sei $\nu \in \mathrm{RCWA}(R) : n \mapsto n+1$, $\varsigma \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto -n$ und $\tau \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto n + (-1)^n$. Vermittels der Einschränkungsmonomorphismen aus Definition 2.3.1 werden aus diesen drei Abbildungen einige 'Grundbausteine' für zahme Abbildungen abgeleitet:

1. Der zu einer Restklasse $r(m)$ von R gehörige *Klassenshift* $\nu_{r(m)} \in \mathrm{RCWA}(R)$ sei definiert durch $\nu^{\pi_{n \mapsto mn+r}}$.

2. Die zu einer Restklasse $r(m)$ von $\mathbb{Z}$ gehörige *Klassenspiegelung* $\varsigma_{r(m)} \in \mathrm{RCWA}(\mathbb{Z})$ sei definiert durch $\varsigma^{\pi_{n \mapsto mn+r}}$.

3. Die zu zwei disjunkten Restklassen $r_1(m_1)$ und $r_2(m_2)$ von $\mathbb{Z}$ gehörige *Klassentransposition* $\tau_{r_1(m_1),r_2(m_2)} \in \mathrm{RCWA}(\mathbb{Z})$ sei definiert durch τ^{π_μ}, wobei

$$\mu = \mu_{r_1(m_1),r_2(m_2)} \in \mathrm{Rcwa}(\mathbb{Z}), \quad n \longmapsto \begin{cases} \dfrac{m_1 n + 2r_1}{2} & \text{falls } \ n \in 0(2), \\ \dfrac{m_2 n + (2r_2 - m_2)}{2} & \text{falls } \ n \in 1(2) \end{cases}$$

die Restklassen $0(2)$ bzw. $1(2)$ auf $r_1(m_1)$ bzw. $r_2(m_2)$ abbildet (vgl. Lemma 2.1.3).

Um der Eindeutigkeit willen wird in diesem Zusammenhang stets angenommen, daß für alle auftretenden Restklassen $r(m)$ stets $r \in \mathfrak{R}(m)$ ist.

2.9.2 Bemerkung Wie man leicht sieht und die Namen andeuten, sind ein Klassenshift $\nu_{r(m)} \in \mathrm{RCWA}(R)$ und eine Klassenspiegelung $\varsigma_{r(m)} \in \mathrm{RCWA}(\mathbb{Z})$ gegeben durch

$$n \longmapsto \begin{cases} n+m & \text{falls } \ n \in r(m), \\ n & \text{sonst,} \end{cases} \qquad \text{bzw.} \quad n \longmapsto \begin{cases} -n+2r & \text{falls } \ n \in r(m), \\ n & \text{sonst.} \end{cases}$$

Eine Klassentransposition $\tau_{r_1(m_1),r_2(m_2)}$ ist eine Involution, die die disjunkten Restklassen $r_1(m_1)$ und $r_2(m_2)$ miteinander vertauscht. Konkret: Es ist

$$\tau_{r_1(m_1),r_2(m_2)} \in \mathrm{RCWA}(\mathbb{Z}), \quad n \longmapsto \begin{cases} \dfrac{m_2 n + (m_1 r_2 - m_2 r_1)}{m_1} & \text{falls } \ n \in r_1(m_1), \\ \dfrac{m_1 n + (m_2 r_1 - m_1 r_2)}{m_2} & \text{falls } \ n \in r_2(m_2), \\ n & \text{sonst.} \end{cases}$$

Man sieht sofort, daß $\tau_{r_1(m_1),r_2(m_2)} = \tau_{r_2(m_2),r_1(m_1)}$.

Wegen Korollar 2.3.3 sind die von ν, ς bzw. τ verschiedenen Abbildungen $\nu_{r(m)}$, $\varsigma_{r(m)}$ bzw. $\tau_{r_1(m_1),r_2(m_2)}$ jeweils zueinander konjugiert. Enthält also ein beliebiger Normalteiler der Gruppe $\mathrm{RCWA}(\mathbb{Z})$ eine solche Abbildung, dann enthält er bereits die gesamte betreffende Serie.

2.9.3 Satz *Sämtliche zahmen Abbildungen in* $\mathrm{RCWA}(\mathbb{Z})$ *lassen sich als Produkte von Klassenshifts* $\nu_{r(m)}$*, Klassenspiegelungen* $\varsigma_{r(m)}$ *und Klassentranspositionen* $\tau_{r_1(m_1),r_2(m_2)}$ *schreiben.*

Beweis: Da endliche symmetrische Gruppen von Transpositionen erzeugt werden, und die Abbildungen $\nu_{r(m)}$ und $\varsigma_{r(m)}$ die größte Untergruppe von $\mathrm{AFF}(\mathbb{Z})$ erzeugen, die auf der Restklasse $r(m)$ operiert, folgt die Aussage sofort aus Satz 2.5.8. □

Hieraus folgt direkt:

2.9.4 Satz Der Normalteiler $N \trianglelefteq \mathrm{RCWA}(\mathbb{Z})$ wird von Klassenshifts, Klassenspiegelungen und Klassentranspositionen erzeugt.

Die Gruppe N wird also insbesondere erzeugt von Bildern der drei Abbildungen ν, ς und τ unter Einschränkungsmonomorphismen. Wegen $\nu = (n \mapsto -n) \cdot (n \mapsto -n+1)$ lassen sich damit auch alle Elemente von N als Produkte von Involutionen schreiben.

2.9.5 Beispiel Übernimmt man die Abbildung g der Ordnung 7 aus Beispiel 2.5.3, so kann man sich leicht davon überzeugen, daß $g = \tau_{0(6),1(6)} \cdot \tau_{0(6),5(6)} \cdot \tau_{0(6),3(6)} \cdot \tau_{0(6),4(6)} \cdot \tau_{1(3),2(6)}$ eine Faktorisierung von g in Klassentranspositionen ist.

Es erscheint zunächst einmal nicht abwegig zu vermuten, die Abbildungen $\nu_{r(m)}$, $\varsigma_{r(m)}$ und $\tau_{r_1(m_1),r_2(m_2)}$ würden eine ausbalancierte Untergruppe von $\mathrm{RCWA}(\mathbb{Z})$ erzeugen. Dies bedeutete, daß $N \neq \mathrm{RCWA}(\mathbb{Z})$. Daß N jedoch nicht ausbalanciert ist, zeigt das folgende Beispiel:

2.9.6 Beispiel Produkte von Klassentranspositionen sind nicht notwendigerweise ausbalanciert. Mehr noch: Multiplikator und Divisor eines solchen können sogar zueinander teilerfremd sein. Um dies zu sehen, sei $\sigma_1 := \tau_{1(6),0(8)} \cdot \tau_{5(6),4(8)}$, $\sigma_2 := \tau_{0(4),1(6)} \cdot \tau_{2(4),5(6)}$ und $\sigma_3 := \tau_{2(6),1(12)} \cdot \tau_{4(6),7(12)}$. Zur Illustration: Es ist

$$\sigma_1: \ n \longmapsto \begin{cases} \frac{3n+4}{4} & \text{falls } n \in 0(8), \\ \frac{4n-4}{3} & \text{falls } n \in 1(6), \\ \frac{3n+8}{4} & \text{falls } n \in 4(8), \\ \frac{4n-8}{3} & \text{falls } n \in 5(6), \\ n & \text{sonst}, \end{cases} \qquad \sigma_2: \ n \longmapsto \begin{cases} \frac{3n+2}{2} & \text{falls } n \in 0(4), \\ \frac{2n-2}{3} & \text{falls } n \in 1(6), \\ \frac{3n+4}{2} & \text{falls } n \in 2(4), \\ \frac{2n-4}{3} & \text{falls } n \in 5(6), \\ n & \text{sonst}, \end{cases}$$

$$\text{sowie} \quad \sigma_3: \ n \longmapsto \begin{cases} 2n-3 & \text{falls } n \in 2(6), \\ \frac{n+3}{2} & \text{falls } n \in 1(12), \\ 2n-1 & \text{falls } n \in 4(6), \\ \frac{n+1}{2} & \text{falls } n \in 7(12), \\ n & \text{sonst}. \end{cases}$$

Die Abbildungen σ_1, σ_2 und σ_3 sind Involutionen, deren Produkt gegeben ist durch

$$\sigma_1\sigma_2\sigma_3 : \quad n \longmapsto \begin{cases} \frac{3n+4}{2} & \text{falls } n \in 2(4), \\ n+1 & \text{falls } n \in 1(6), \\ n & \text{falls } n \in 3(6), \\ \frac{n}{2} & \text{falls } n \in 0(12), \\ n-3 & \text{falls } n \in 4(12), \\ n-1 & \text{falls } n \in 5(6) \cup 8(12). \end{cases}$$

Dieses Beispiel liefert nebenbei noch ein paar weitere Aussagen:

2.9.7 Bemerkung Es gilt:

- Ausbalanciertheit ist keine Klasseninvariante. Zum Beispiel ist zwar $\sigma_1\sigma_2\sigma_3$ nicht ausbalanciert, aber es gilt $\mathrm{Mult}((\sigma_1\sigma_2\sigma_3)^{\sigma_2}) = \mathrm{Div}((\sigma_1\sigma_2\sigma_3)^{\sigma_2}) = 36$.

- Auch wilde Abbildungen können vermittels einer Involution zu ihrer Inversen konjugiert sein. Beispielsweise ist offenbar $(\sigma_1\sigma_2)^{\sigma_2} = (\sigma_1\sigma_2)^{-1}$, und man rechnet leicht nach, daß $\sigma_1\sigma_2$ wild ist.

- Die Gruppe $\langle\sigma_1, \sigma_2\rangle$ ist wild und isomorph zu D_∞. Die unendliche Diedergruppe besitzt also eine treue wilde rcwa-Darstellung über $\mathbb{Z}$.

Man kann vermuten, daß Definition 2.9.1 tatsächlich ein Erzeugendensystem für die ganze Gruppe $\mathrm{RCWA}(\mathbb{Z})$ liefert:

2.9.8 Vermutung Es ist $N = \mathrm{RCWA}(\mathbb{Z})$.

2.9.9 Beispiel Wie bereits erwähnt, ist die Permutation α aus Beispiele 1.1.3 bereits von anderen Leuten untersucht worden. Günther Wirsching zitiert etwa in [Wir96] einen Artikel von Jeffrey C. Lagarias [Lag85] mit der Aussage, Lothar Collatz hätte diese Abbildung – um genau zu sein: α^{-1} – in seinem Notizbuch unter dem Datum 1. Juli 1932 aufgeführt. Darüberhinaus stellt er fest, es sei bislang unbekannt, ob der Zykel

$$(\ldots\ 32\ 43\ 57\ 38\ 51\ 34\ 45\ 30\ 20\ 27\ 18\ 12\ 8\ 11\ 15\ 10\ 13\ 17\ 23\ 31\ 41\ 55\ \ldots)$$

dieser Permutation endlich oder unendlich ist.

Hier soll die Permutation α in die Erzeugenden $\nu_{r(m)}$, $\varsigma_{r(m)}$ und $\tau_{r_1(m_1),r_2(m_2)}$ des Normalteilers $N \trianglelefteq \mathrm{RCWA}(\mathbb{Z})$ faktorisiert werden. Der Umstand, daß sämtliche affinen Teilabbildungen von α einen Faktor 3 im Zähler und eine Potenz von 2 im Nenner haben, erschwert eine Faktorisierung in ausbalancierte Erzeugende sehr erheblich.

Es seien $\sigma_1, \sigma_2, \sigma_3$ wie in Beispiel 2.9.6. Setzt man $\sigma := \sigma_1\sigma_2\sigma_3$ und

$$\begin{aligned}\theta \;:=\; & \nu^{-4} \cdot \tau_{3(144),139(288)} \cdot \tau_{75(144),235(288)} \cdot \tau_{101(144),43(288)} \cdot \tau_{27(36),23(72)} \cdot \tau_{17(36),47(72)} \\ & \cdot \tau_{70(72),71(144)} \cdot \tau_{65(72),143(144)} \cdot \tau_{29(144),91(288)} \cdot \tau_{27(36),70(72)} \cdot \tau_{17(36),3(72)} \cdot \tau_{29(72),187(288)} \\ & \cdot \tau_{65(72),283(288)} \cdot \tau_{3(36),8(72)} \cdot \tau_{5(36),32(72)} \cdot \tau_{15(36),56(72)} \cdot \tau_{3(36),91(288)} \cdot \tau_{5(36),187(288)} \\ & \cdot \tau_{15(36),283(288)} \cdot \tau_{23(24),7(48)} \cdot \tau_{8(24),33(48)} \cdot \tau_{13(24),43(96)} \cdot \tau_{17(36),91(288)} \cdot \tau_{29(36),283(288)} \\ & \cdot \tau_{4(12),20(24)} \cdot \tau_{21(24),19(48)} \cdot \tau_{29(36),283(288)} \cdot \tau_{3(36),1(48)} \cdot \tau_{15(36),25(48)} \cdot \tau_{27(36),11(48)} \\ & \cdot \tau_{5(36),35(48)} \cdot \tau_{17(36),36(48)} \cdot \tau_{29(36),9(48)} \cdot \tau_{33(48),91(288)} \cdot \tau_{20(24),187(288)} \cdot \tau_{7(48),283(288)} \\ & \cdot \sigma \cdot \nu^4 \cdot \sigma^4,\end{aligned}$$

dann ist $\alpha\theta^{-1}$ ganz, also erst recht zahm. Mithin handelt es sich nach Satz 2.9.3 um ein Produkt von Abbildungen $\nu_{r(m)}$, $\varsigma_{r(m)}$ und $\tau_{r_1(m_1),r_2(m_2)}$. Aufgrund der angegebenen Faktorisierung von θ läßt sich deshalb auch α als Produkt derartiger Abbildungen schreiben.

Die Abbildung σ mit Multiplikator 3 und Divisor 2 spielt in diesem Beispiel insofern eine zentrale Rolle, als eine Division von α durch eine geeignete Potenz von σ die Potenzen von 2 und 3 relativ gleichmäßig auf Zähler und Nenner der affinen Teilabbildungen verteilt. Der nächste Konstruktionsschritt war die Elimination des Primfaktors 3 aus Multiplikator und Divisor, und als letzter Schritt blieb die Reduktion einer Abbildung mit Multiplikator und Divisor 4 (und Modul 288) auf eine ganze Abbildung $\alpha\theta^{-1}$ der Ordnung 101616.

Die angegebene Zerlegung von α wurde in recht mühevoller ‘Puzzlearbeit’ mit RCWA gewonnen. Ein Vergleich mit dem Versuch eines Anfängers, einen verdrehten Rubik's Cube zurückzudrehen – das Analogon zu dessen Drehungen sind hier die Multiplikationen mit Klassentranspositionen und Klassenshifts – erscheint naheliegend insofern, als zwar einige Heuristiken verwendet wurden, aber die Frage nach einem Algorithmus bislang unbeantwortet bleibt. Ein wesentlicher Unterschied ist jedoch, daß der Rubik's Cube a priori endlich ist.

Transpositionen in endlichen symmetrischen Gruppen lassen sich nicht als Kommutatoren schreiben. Anders liegen die Dinge für Klassentranspositionen in $\mathrm{RCWA}(\mathbb{Z})$:

2.9.10 Lemma *Klassentranspositionen lassen sich als Kommutatoren schreiben, liegen also insbesondere in* $\mathrm{RCWA}(\mathbb{Z})'$.

Beweis: Man rechnet leicht nach, daß $\tau = [\tau_1, \tau_2]$ mit

$$\tau_1 :\ n \mapsto \begin{cases} n+1 & \text{falls } n \in 0(4) \cup 1(4), \\ n-2 & \text{falls } n \in 2(4), \\ n & \text{falls } n \in 3(4) \end{cases} \qquad \text{und} \qquad \tau_2 :\ n \mapsto \begin{cases} n+1 & \text{falls } n \in 0(4), \\ n+2 & \text{falls } n \in 1(4), \\ n & \text{falls } n \in 2(4), \\ n-3 & \text{falls } n \in 3(4). \end{cases}$$

Diese Zerlegung läßt sich auf eine gegebene Klassentransposition $\tau_{r_1(m_1),r_2(m_2)}$ übertragen durch Übergang zu Bildern unter dem zur Abbildung $\mu_{r_1(m_1),r_2(m_2)}$ aus der Definition einer Klassentransposition in 2.9.1 assoziierten Einschränkungsmonomorphismus. □

Die im Beweis von Lemma 2.9.10 angegebene Darstellung von τ als Kommutator gewinnt man aus der Gleichung $(12)(34) = [(123),(124)]$ durch Übergang zu Bildern unter der rcwa-Darstellung φ_4 von S_4 aus Satz 2.1.2.

Über die Ordnungen der Kommutatoren der Klassenshifts $\nu_{r(m)}$ läßt sich eine einfache Aussage treffen:

2.9.11 Lemma *Ist* $\mathrm{char}(R) = 0$, *so gilt*

$$\mathrm{ord}([\nu_{r_1(m_1)}, \nu_{r_2(m_2)}]) \;=\; \begin{cases} \infty & \textit{falls} \;\; r_1(m_1) \subsetneq r_2(m_2) \vee r_1(m_1) \supsetneq r_2(m_2), \\ 1 & \textit{falls} \;\; r_1(m_1) = r_2(m_2) \vee r_1(m_1) \cap r_2(m_2) = \emptyset, \\ 3 & \textit{sonst.} \end{cases}$$

Beweis: Offenbar ist $\mathrm{supp}([\nu_{r_1(m_1)}, \nu_{r_2(m_2)}]) \subseteq r_1(m_1) \cup r_2(m_2)$. Der Fall der Gleichheit oder Disjunktheit der Restklassen $r_1(m_1)$ und $r_2(m_2)$ ist trivial. Als erstes wird der Fall einer echten Teilmengenbeziehung betrachtet, wobei ohne Einschränkung angenommen werden kann, daß $r_1(m_1) \subsetneq r_2(m_2)$ – im Falle der umgekehrten Inklusion würde man einfach die Inverse des Kommutators betrachten. Ausmultiplizieren liefert

$$[\nu_{r_1(m_1)}, \nu_{r_2(m_2)}] \in \mathrm{RCWA}(R), \quad n \;\longmapsto\; \begin{cases} n - m_1 & \text{falls} \;\; n \equiv r_1 \;(m_1), \\ n + m_1 & \text{falls} \;\; n \equiv r_1 + m_2 \;(m_1), \\ n & \text{sonst,} \end{cases}$$

und damit wegen $\mathrm{char}(R) = 0$ die Behauptung. Setzt man $r(m) := r_1(m_1) \cap r_2(m_2)$, dann erhält man im verbleibenden Fall

$$[\nu_{r_1(m_1)}, \nu_{r_2(m_2)}] \in \mathrm{RCWA}(R), \quad n \;\longmapsto\; \begin{cases} n + m_2 & \text{falls} \;\; n \equiv r \;(m), \\ n - m_1 & \text{falls} \;\; n \equiv r + m_1 \;(m), \\ n + m_1 - m_2 & \text{falls} \;\; n \equiv r + m_2 \;(m), \\ n & \text{sonst,} \end{cases}$$

und diese Permutation hat offenkundig Ordnung 3. □

Der Versuch, eine vergleichbare Aussage für Produkte zweier Klassentranspositionen zu gewinnen, führt zu einer sehr unübersichtlichen Vielzahl möglicher Fälle. Man erhält u.a. Abbildungen verschiedener endlicher Ordnungen (vage Vermutung: genau derjenigen Ordnungen, die 60 teilen – jedenfalls kommen mit möglicher Ausnahme von 5 alle diese vor, und es haben sich bisher keine weiteren gefunden) und Abbildungen unendlicher Ordnung sowohl mit unendlichen als auch nur mit endlichen Zykeln.

2.10 Bedingungen an Normalteiler von RCWA(R)

In diesem Abschnitt werden Reichhaltigkeitsbedingungen an nichttriviale Normalteiler von $\mathrm{RCWA}(R)$ hergeleitet. Konkret geht es darum, zu untersuchen, ob bzw. was für zahme Untergruppen ein Normalteiler von $\mathrm{RCWA}(R)$ besitzen muß.

Zunächst sind aber ein paar Vorarbeiten erforderlich:

2.10.1 Lemma *Es sei $\sigma \in \mathrm{RCWA}(R)$, $m := \mathrm{Mod}(\sigma)$ und $\nu \in \mathrm{RCWA}(R)$ eine ganze Abbildung, die die Partition R/mR von R respektiert und festläßt. Dann ist der Kommutator $c := [\sigma, \nu]$ ganz.*

Beweis: Es sei α eine beliebige affine Teilabbildung von c. Gemäß Definition und nach Lemma 2.1.3 ist α das Kompositum

- einer affinen Teilabbildung $\alpha_{\sigma^{-1}} : n \mapsto (c_1 n - b_1)/a_1$ von σ^{-1},
- einer affinen Teilabbildung $\alpha_{\nu^{-1}} : n \mapsto u_1 n + r_1(1-u_1) + k_1 m$ von ν^{-1},
- einer affinen Teilabbildung $\alpha_\sigma : n \mapsto (a_2 n + b_2)/c_2$ von σ und
- einer affinen Teilabbildung $\alpha_\nu : n \mapsto u_2 n + r_2(1-u_2) + k_2 m$ von ν

für gewisse Koeffizienten $a_1, a_2, b_1, b_2, c_1, c_2, r_1, r_2, k_1, k_2 \in R$ und $u_1, u_2 \in R^\times$. Da die Abbildung ν die Partition R/mR respektiert und festläßt, gilt $a_1 = a_2$, $b_1 = b_2$ und $c_1 = c_2$. Es sei φ die Standarddarstellung von $\mathrm{AFF}(K)$. Nach Determinantenmultiplikationssatz gilt

$$\begin{aligned}\det(\alpha^\varphi) &= \det({\alpha_{\sigma^{-1}}}^\varphi) \cdot \det({\alpha_{\nu^{-1}}}^\varphi) \cdot \det({\alpha_\sigma}^\varphi) \cdot \det({\alpha_\nu}^\varphi) \\ &= \frac{c_1}{a_1} \cdot u_1 \cdot \frac{a_1}{c_1} \cdot u_2 \;=\; u_1 \cdot u_2 \in R^\times,\end{aligned}$$

wegen $R^\alpha \cap R \neq \emptyset$ also $\alpha \in \mathrm{AFF}(R)$. Dies heißt jedoch nichts anderes, als daß die Abbildung c wie behauptet ganz ist. $\square$

2.10.2 Lemma *In der Situation von Lemma 2.10.1 ist der Kommutator $[\sigma, \nu\sigma]$ zahm.*

Beweis: Es ist $[\sigma, \nu\sigma] = \sigma^{-1}(\nu\sigma)^{-1}\sigma\nu\sigma = \sigma^{-2}\sigma^\nu\sigma = (\sigma^{-1}\sigma^\nu)^\sigma = [\sigma, \nu]^\sigma$. Die Behauptung folgt mit Lemma 2.10.1 und Lemma 1.8.3, Aussage (1). $\square$

2.10.3 Beispiel Lemma 2.10.2 ist der Grund dafür, daß die Kommutatoren $[\alpha, \nu_{1(4)}\alpha]$ und $[\alpha, \nu_{3(4)}\alpha]$ in Beispiele 1.5.2 zahm sind.

Es gibt keinen Normalteiler, der außer 1 nur wilde Elemente enthält:

2.10.4 Lemma *Ist* $N \lhd \mathrm{RCWA}(R)$ *ein nichttrivialer Normalteiler, so enthält* N *ein ganzes Element* $g \neq 1$.

Beweis: Es sei $\sigma \in N \setminus \{1\}$ und $m := \mathrm{Mod}(\sigma)$. Es kann o.E. angenommen werden, daß es eine Restklasse $r(m)$ so gibt, daß $r(m)^\sigma \neq r(m)$, denn anderenfalls wäre σ bereits ganz. Es sei $\nu := \nu_{r(m)}$ und $g := [\sigma, \nu] = \sigma^{-1}\sigma^\nu$. Nach Definition eines Normalteilers ist $g \in N$, und wegen $r(m)^\sigma \neq r(m)$ ist $g \neq 1$. Die Abbildung g ist jedoch ganz gemäß Lemma 2.10.1. □

Man kann darüberhinaus zeigen, daß ein Normalteiler sogar zahme (und damit auch ganze) Elemente unendlicher Ordnung besitzen muß, sofern die Gruppe $(R, +)$ nicht nur Torsionselemente besitzt:

2.10.5 Lemma *Ist* $\mathrm{char}(R) = 0$ *und* $N \lhd \mathrm{RCWA}(R)$ *ein nichttrivialer Normalteiler, so enthält* N *ein ganzes Element* g *unendlicher Ordnung.*

Beweis: Gemäß Lemma 2.10.4 enthält N ein ganzes Element $\tilde{g} \neq 1$. Es kann im folgenden o.E. angenommen werden, daß $\mathrm{ord}(\tilde{g}) < \infty$, denn anderenfalls wäre das gesuchte Element bereits identifiziert. Es sei $m := \mathrm{Mod}(\tilde{g})$. Die Abbildung $\tilde{g}$ respektiert nach Lemma 2.5.4 die Partition R/mR. Wir wählen eine Restklasse $r(m)$ so, daß $\tilde{g}|_{r(m)} \neq 1$, und setzen $\nu := \nu_{r(m)}$. Es sei $g := [\tilde{g}, \nu] = \tilde{g}^{-1}\tilde{g}^\nu$. Nach Definition eines Normalteilers ist $g \in N$. Desweiteren ist mit $\tilde{g}$ und ν auch g ganz, und respektiert nach Lemma 2.5.6, Aussage (1) ebenfalls die Partition R/mR. Es genügt also zu zeigen, daß $r(m)^g = r(m)$ und $\mathrm{ord}(g|_{r(m)}) = \infty$. Es sind jetzt zwei Fälle zu unterscheiden:

1. Es ist $r(m)^{\tilde{g}} = r(m)$. Dann ist die Einschränkung $\tilde{g}|_{r(m)}$ nach Lemma 2.1.3 gegeben durch $n \mapsto un + r(1-u) + km$ für ein $k \in R$ und ein $u \in R^\times$. Für $n \in r(m)$ gilt

$$\begin{aligned} n &\xmapsto{\tilde{g}^{-1}} u^{-1}n - u^{-1}km - r(u^{-1} - 1) \\ &\xmapsto{\nu^{-1}} u^{-1}n - (u^{-1}k + 1)m - r(u^{-1} - 1) \\ &\xmapsto{\tilde{g}} n - um \\ &\xmapsto{\nu} n + (1-u)m, \end{aligned}$$

   also $n^g = n + (1-u)m \equiv r\ (m)$. Angenommen, es wäre $u = 1$. Dann müßte aufgrund der Wahl von $r(m)$ zumindest $k \neq 0$ sein, was wegen $\mathrm{char}(R) = 0$ im Widerspruch zur Annahme $\mathrm{ord}(\tilde{g}) < \infty$ steht. Es ist also $u \neq 1$, und wegen $\mathrm{char}(R) = 0$ ist g das gesuchte Element.

2. Es ist $r(m)^{\tilde{g}} \neq r(m)$. In diesem Fall gilt für $n \in r(m)$

$$n \xmapsto{\tilde{g}^{-1}} n^{\tilde{g}^{-1}} \xmapsto{\nu^{-1}} n^{\tilde{g}^{-1}} \xmapsto{\tilde{g}} n \xmapsto{\nu} n + m,$$

   da $n^{\tilde{g}^{-1}} \notin r(m)$. Die Teilabbildung $g|_{r(m)}$ ist also gegeben durch $n \mapsto n + m$, und wegen $\mathrm{char}(R) = 0$ ist g das gesuchte Element. □

Nach Lemma 2.8.5 induziert eine zahme rcwa-Abbildung unendlicher Ordnung auf einer geeignet gewählten Partition eine Transposition. Zusammen mit der Aussage des vorstehenden Lemmas läßt sich schließen, daß ein nichttrivialer Normalteiler von $\mathrm{RCWA}(R)$ ziemlich 'große' zahme Untergruppen besitzen muß:

2.10.6 Satz *Es sei* $\mathrm{char}(R) = 0$*, der Exponent der Einheitengruppe von R sei endlich, und es besitze R die schwache Restklassenteilbarkeitseigenschaft. Ferner sei $N \neq 1$ ein Normalteiler von* $\mathrm{RCWA}(R)$*. Dann gibt es beliebig große $l \in \mathbb{N}$ so, daß* $\mathrm{Sym}(\mathcal{P}) < N$ *für jede Partition $\mathcal{P}$ von R in l Restklassen.*

Beweis: Es sei $l' \in \mathbb{N}$ beliebig. Nach Lemma 2.10.5 enthält N ein ganzes Element g unendlicher Ordnung. Nach Lemma 2.8.5 gibt es einen Exponenten $e \in \mathbb{N}$ und eine von g^e respektierte Partition $\tilde{\mathcal{P}}$ mit $l' \leqslant |\tilde{\mathcal{P}}| =: l$, auf der g^e eine Transposition induziert. Da eine endliche symmetrische Gruppe keinen echten Normalteiler besitzt, der eine Transposition enthält, ist wegen $\mathrm{Sym}(\tilde{\mathcal{P}}) < \mathrm{RCWA}(R)$ sogar $\mathrm{Sym}(\tilde{\mathcal{P}}) < N$. Ist nun $\mathcal{P}$ eine beliebige Partition von R in l Restklassen, dann gibt es nach Lemma 2.1.4 ein $\sigma \in \mathrm{RCWA}(R)$ so, daß $\tilde{\mathcal{P}}^\sigma = \mathcal{P}$. Nach Lemma 2.5.6, Aussage (2) ist $\mathrm{Sym}(\tilde{\mathcal{P}})^\sigma = \mathrm{Sym}(\mathcal{P})$. Aufgrund der Voraussetzung, daß N ein Normalteiler ist, folgt wie behauptet $\mathrm{Sym}(\mathcal{P}) < N$. □

Es sei allerdings ausdrücklich bemerkt, daß man in der Aussage des Satzes nicht so ohne weiteres schreiben könnte '... dann gibt es ein $l_0 \in \mathbb{N}$ so, daß für alle $l > l_0$ gilt ...', und daß außerdem für Partitionen 'kleiner' Länge l bislang nichts ausgesagt werden kann.

Aus Satz 2.10.6 folgt in anderer Weise als in Korollar 2.1.6, daß die Gruppe $\mathrm{RCWA}(R)$ z.B. für $R = \mathbb{Z}$ keine auflösbaren Normalteiler besitzt.

2.11 Ein Normalteiler von RCWA+(Z)

Die Gruppe $\mathrm{RCWA}^+(\mathbb{Z})$ der klassenweise ordnungserhaltenden bijektiven rcwa-Abbildungen von $\mathbb{Z}$ besitzt einen nichttrivialen Normalteiler. In diesem Abschnitt wird dieser als Kern eines Homomorphismus von $\mathrm{RCWA}^+(\mathbb{Z})$ auf $(\mathbb{Z}, +)$ konstruiert.

2.11.1 Definition Es sei $r(m)$ eine Restklasse und $\alpha : n \mapsto (an + b)/c$ eine ordnungserhaltende affine Abbildung mit Definitionsbereich $r(m)$. Die *Determinante* von α sei definiert durch

$$\det(\alpha) \ := \ \frac{b}{am}.$$

Ferner sei die *Determinante* einer rcwa-Abbildung $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ mit Modul m definiert als die Summe der Determinanten ihrer affinen Teilabbildungen, d.h. es ist

$$\det(\sigma) \ = \ \sum_{r(m) \in \mathbb{Z}/m\mathbb{Z}} \det(\sigma|_{r(m)}).$$

Daß man auf diese Weise einen Homomorphismus erhält, erscheint wenig intuitiv. Es ist noch nicht einmal offensichtlich, daß die Determinante einer Abbildung $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ überhaupt stets ganzzahlig ist. Zur Ideenfindung haben sich hier rechnerische Untersuchungen mittels RCWA als äußerst hilfreich erwiesen.

2.11.2 Bemerkung Es sei $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ und $m = \mathrm{Mod}(\sigma)$. Wie üblich seien die Koeffizienten von σ bezeichnet mit $a_{r(m)}$, $b_{r(m)}$ und $c_{r(m)}$, d.h. die Einschränkung $\sigma|_{r(m)}$ von σ auf eine Restklasse $r(m) \in \mathbb{Z}/m\mathbb{Z}$ sei gegeben durch $n \mapsto (a_{r(m)}n + b_{r(m)})/c_{r(m)}$. Dann gilt:

$$\begin{aligned}
\det(\sigma) &= \frac{1}{m} \sum_{r(m) \in \mathbb{Z}/m\mathbb{Z}} \frac{b_{r(m)}}{a_{r(m)}} = \frac{1}{m} \sum_{r=0}^{m-1} \left(\frac{c_{r(m)}}{a_{r(m)}} \cdot \frac{a_{r(m)}r + b_{r(m)}}{c_{r(m)}} - r \right) \\
&= \frac{1}{m} \sum_{r=0}^{m-1} \left(\frac{c_{r(m)}}{a_{r(m)}} r^\sigma - r \right) = \frac{1-m}{2} + \sum_{r=0}^{m-1} \frac{r^\sigma}{(r+m)^\sigma - r^\sigma}.
\end{aligned}$$

Zu beweistechnischen Zwecken wird es sich als zweckmäßig erweisen, Repräsentanten von Restklassen zu fixieren:

2.11.3 Definition Eine Restklasse $r(m)$ mit fixiertem Repräsentanten r wird bezeichnet mit $[r/m]$. Das Bild einer solchen Restklasse $[r/m]$ unter einer affinen Abbildung α sei die Restklasse $r(m)^\alpha$ mit fixiertem Repräsentanten r^α. Es sei $k \in \mathbb{N}$. Die Zerlegung

$$\left[\frac{r}{m}\right] = \left[\frac{r}{km}\right] \cup \left[\frac{r+m}{km}\right] \cup \dots \cup \left[\frac{r+(k-1)m}{km}\right].$$

einer Restklasse $[r/m]$ heiße *repräsentantenstabil*.

Es sei $\mathcal{P}$ eine Partition von $\mathbb{Z}$ in endlich viele Restklassen mit fixierten Repräsentanten. Eine Verfeinerung von $\mathcal{P}$ mittels repräsentantenstabiler Zerlegung enthaltener Restklassen heiße ebenfalls *repräsentantenstabil*.

Restklassen mit fixierten Repräsentanten werden rationale Zahlen zugeordnet:

2.11.4 Definition Für eine Restklasse $[r/m]$ sei

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

Für eine Partition $\mathcal{P}$ von $\mathbb{Z}$ in endlich viele Restklassen mit fixierten Repräsentanten sei

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

und es sei

$$\delta(\mathbb{Z}) := \delta(\mathcal{P}) - \lfloor \delta(\mathcal{P}) \rfloor.$$

Es ist zu zeigen, daß $\delta(\mathbb{Z})$ wohldefiniert ist:

2.11.5 Lemma *Der Wert $\delta(\mathbb{Z})$ ist unabhängig von der Wahl der Partition $\mathcal{P}$.*

Beweis: Zu zeigen ist die Invarianz von $\delta(\mathcal{P})$ mod 1 sowohl unter repräsentantenstabiler Verfeinerung von $\mathcal{P}$ als auch unter Änderung der Repräsentanten der Restklassen in $\mathcal{P}$. Für eine Restklasse $[r/m]$ und $k \in \mathbb{N}$ gilt

$$\begin{aligned}\delta\left(\left[\frac{r}{m}\right]\right) &= \frac{r}{m} - \frac{1}{2} = \frac{r}{m} + \frac{(k-1)k}{2k} - \frac{k}{2} = \frac{kr}{km} + \frac{1+\cdots+(k-1)}{k} - \frac{k}{2} \\ &= \sum_{i=0}^{k-1}\left(\frac{r+im}{km} - \frac{1}{2}\right) = \sum_{i=0}^{k-1}\delta\left(\left[\frac{r+im}{km}\right]\right).\end{aligned}$$

Folglich bleibt $\delta(\mathcal{P})$ invariant unter repräsentantenstabiler Verfeinerung der Partition $\mathcal{P}$. Außerdem gilt für eine Restklasse $[r/m]$ und $k \in \mathbb{Z}$

$$\delta\left(\left[\frac{r}{m}\right]\right) = \frac{r}{m} - \frac{1}{2} = \frac{r+km}{m} - \frac{1}{2} - k = \delta\left(\left[\frac{r+km}{m}\right]\right) - k.$$

Folglich ändert sich $\delta(\mathcal{P})$ bei Änderung der Wahl der Repräsentanten der Restklassen höchstens um eine ganze Zahl. □

2.11.6 Bemerkung Es ist $\delta(\mathbb{Z}) = \delta([0/1]) = 0/1 - 1/2 - \lfloor 0/1 - 1/2 \rfloor = 1/2$. Die explizite Kenntnis dieses Wertes ist im folgenden allerdings nicht erforderlich.

2.11.7 Definition Es sei $\sigma \in \mathrm{RCWA}(\mathbb{Z})$. Eine Partition $\mathcal{P}$ von $\mathbb{Z}$ in endlich viele Restklassen mit fixierten Repräsentanten heiße ein *Träger* von σ, wenn alle Einschränkungen von σ auf Restklassen $[r/m] \in \mathcal{P}$ affin sind.

2.11.8 Lemma Ist $\alpha: \ n \mapsto (an+b)/c$ eine ordnungserhaltende, auf einer Restklasse $[r/m]$ definierte affine Abbildung, dann gilt wegen Lemma 1.1.8, Aussage (1)

$$\delta\left(\left[\frac{r}{m}\right]^{\alpha}\right) = \delta\left(\left[\frac{(ar+b)/c}{am/c}\right]\right) = \frac{r}{m} - \frac{1}{2} + \frac{b}{am} = \delta\left(\left[\frac{r}{m}\right]\right) + \det(\alpha).$$

Es sei $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$, und $\mathcal{P}$ ein Träger von σ. Aus obigem folgt

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

und hieraus mittels Einsetzen in die Definition, daß

$$\delta(\mathbb{Z}) = \delta(\mathbb{Z}^\sigma) = \delta(\mathbb{Z}) + \det(\sigma) - \lfloor \delta(\mathbb{Z}) + \det(\sigma) \rfloor.$$

Jetzt sind sämtliche erforderlichen Vorarbeiten geleistet, um zeigen zu können, daß die Determinantenabbildung tatsächlich ein Epimorphismus von $\mathrm{RCWA}^+(\mathbb{Z})$ auf $(\mathbb{Z}, +)$ ist:

2.11.9 Satz *Die Determinantenabbildung*

$$\mathrm{RCWA}^+(\mathbb{Z}) \;\to\; (\mathbb{Z},+), \quad \sigma \;\mapsto\; \det(\sigma)$$

ist ein Epimorphismus.

Beweis: Es seien $\sigma_1, \sigma_2, \sigma \in \mathrm{RCWA}^+(\mathbb{Z})$. Es ist zu zeigen, daß $\det(\sigma)$ ganzzahlig ist, daß $\det(\sigma^{-1}) = -\det(\sigma)$, daß $\det(\sigma_1\sigma_2) = \det(\sigma_1) + \det(\sigma_2)$, und daß es eine klassenweise ordnungserhaltende bijektive rcwa-Abbildung von $\mathbb{Z}$ mit Determinante 1 gibt.

1. Es ist zu zeigen, daß $\det(\sigma) \in \mathbb{Z}$. Nach Lemma 2.11.8 gilt

   $$\delta\,(\mathbb{Z}) \;=\; \delta\,(\mathbb{Z}) + \det(\sigma) - \lfloor \delta\,(\mathbb{Z}) + \det(\sigma) \rfloor.$$

   Es ist also $\det(\sigma) = \lfloor \delta\,(\mathbb{Z}) + \det(\sigma) \rfloor \in \mathbb{Z}$.

2. Es ist zu zeigen, daß $\det(\sigma^{-1}) = -\det(\sigma)$. Es sei $m := \mathrm{Mod}(\sigma)$, und die Koeffizienten von σ seien bezeichnet mit $a_{r(m)}$, $b_{r(m)}$ und $c_{r(m)}$. Laut Definition trägt die Einschränkung von σ auf eine Restklasse $r(m)$ zur Determinante von σ den Summanden $b_{r(m)}/(m \cdot a_{r(m)})$ bei. Nach Lemma 1.1.8, Aussage (1) ist das Bild der Restklasse $r(m)$ unter σ gleich $r^\sigma(m \cdot a_{r(m)}/c_{r(m)})$. Die Einschränkung von σ^{-1} auf diese Restklasse trägt wegen $a_{r(m)} > 0$ zur Determinante von σ^{-1} den Summanden

   $$\frac{c_{r(m)}}{m \cdot a_{r(m)}} \cdot \frac{-b_{r(m)}}{c_{r(m)}} \;=\; -\frac{b_{r(m)}}{m \cdot a_{r(m)}}$$

   bei. Dies ist genau die additive Inverse des Beitrags von $\sigma|_{r(m)}$ zur Determinante von σ. Es folgt die Behauptung.

3. Es ist zu zeigen, daß $\det(\sigma_1\sigma_2) = \det(\sigma_1) + \det(\sigma_2)$. Es sei $m := \mathrm{Mod}(\sigma_1) \cdot \mathrm{Mod}(\sigma_2)$. Die Partition $\mathcal{P} := \{[0/m], [1/m], \dots, [(m-1)/m]\}$ ist konstruktionsgemäß ein Träger von σ_1 und σ_2, und wegen Lemma 1.3.1a, Aussage (2) einer von $\sigma_1\sigma_2$. Außerdem ist $\mathcal{P}^{\sigma_1}$ wegen Lemma 1.3.1a, Aussage (1) und Lemma 1.1.8, Aussage (1) ein Träger von σ_2. Nach Lemma 2.11.8 gilt daher

   $$\delta\,(\mathcal{P}) + \det(\sigma_1\sigma_2) \;=\; \delta\,(\mathcal{P}^{\sigma_1\sigma_2}) \;=\; \delta\,(\mathcal{P}^{\sigma_1}) + \det(\sigma_2) \;=\; \delta\,(\mathcal{P}) + \det(\sigma_1) + \det(\sigma_2).$$

   Subtraktion von $\delta\,(\mathcal{P})$ vom ersten und letzten Term dieser Gleichungskette liefert die Behauptung.

4. Es wurde bereits gezeigt, daß die Determinantenabbildung ein Homomorphismus von $\mathrm{RCWA}^+(\mathbb{Z})$ nach $(\mathbb{Z},+)$ ist. Dieser ist wie behauptet sogar ein Epimorphismus, denn die Abbildung $\nu \in \mathrm{RCWA}^+(\mathbb{Z}):\ n \mapsto n+1$ liegt im Urbild der 1. □

2.11.10 Bemerkung Die Idee, zum Beweis der Additivität der Determinantenabbildung einer Restklasse $[r/m]$ den Wert $r/m - 1/2$ zuzuordnen, und zu überlegen, welchen Einfluß die Anwendung einer affinen Abbildung auf $[r/m]$ auf diese Invariante hat, stammt ursprünglich von Wolfgang Rump.

2.11.11 Beispiele Klassenshifts haben offensichtlich die Determinante 1. Abbildungen endlicher Ordnung, Kommutatoren sowie deren Produkte liegen hingegen im Kern der Determinantenabbildung. Als Beispiel dafür, daß Inversion den Betrag der Determinante invariant läßt, wird die Abbildung σ aus Beispiel 2.5.15 betrachtet: Es ist

$$\begin{aligned}
\det(\sigma^{-1}) &= \frac{1}{14}\Big(0+\frac{1}{6}+\frac{3}{2}+\frac{5}{3}+\frac{11}{6}+2+\frac{13}{6}+\frac{7}{2}+\frac{11}{3}+\frac{23}{6}-\frac{53}{6}-\frac{19}{3}-\frac{23}{6}-\frac{4}{3}\Big) \\
&= -\frac{1}{24}\Big(0-\frac{1}{7}+\frac{106}{7}-\frac{9}{7}-\frac{10}{7}-\frac{11}{7}-\frac{12}{7}-\frac{13}{7}+\frac{76}{7}-3-\frac{22}{7}-\frac{23}{7} \\
&\qquad +0-\frac{1}{7}+\frac{46}{7}-\frac{9}{7}-\frac{10}{7}-\frac{11}{7}-\frac{12}{7}-\frac{13}{7}+\frac{16}{7}-3-\frac{22}{7}-\frac{23}{7}\Big) \\
&= -\det(\sigma).
\end{aligned}$$

Als Beispiel zur Illustration der Additivität der Determinante werden die Abbildungen α und β aus 1.1.3 bzw. 1.8.5 und deren Produkt betrachtet: Es ist

$$\begin{aligned}
\det(\alpha\beta) &= \frac{1}{20}\Big(0+\frac{13}{27}-\frac{4}{27}-\frac{7}{9}+\frac{2}{27}+\frac{25}{27}+\frac{8}{27}-\frac{1}{3}-\frac{2}{9}-\frac{1}{9} \\
&\qquad +0-\frac{17}{27}-\frac{4}{27}+\frac{1}{3}+\frac{2}{27}-\frac{5}{27}+\frac{8}{27}+\frac{1}{27}-\frac{2}{9}+\frac{7}{27}\Big) \\
&= \frac{1}{4}\Big(0+\frac{1}{3}+0-\frac{1}{3}\Big) \ + \ \frac{1}{5}\Big(0+\frac{1}{9}-\frac{1}{3}-\frac{2}{9}+\frac{4}{9}\Big) \\
&= \det(\alpha) \ + \ \det(\beta).
\end{aligned}$$

Der Kern der Determinantenabbildung selbst ist zwar offensichtlich keine maximale Untergruppe von $\mathrm{RCWA}^+(\mathbb{Z})$, aber die zwischen demselbigen und ganz $\mathrm{RCWA}^+(\mathbb{Z})$ liegenden solchen lassen sich sehr leicht bestimmen:

2.11.12 Bemerkung Ist K der Kern der Determinantenabbildung, p eine Primzahl und $\nu : n \mapsto n+1$, dann hat die Untergruppe $K_p := \langle K, \nu^p \rangle < \mathrm{RCWA}^+(\mathbb{Z})$ den Index p, und ist daher maximal. Der Schnitt aller Untergruppen K_p ist offenbar gleich K, weswegen die Frattini - Untergruppe von $\mathrm{RCWA}^+(\mathbb{Z})$ Untergruppe von K ist.

2.12 Ein Normalteiler von RCWA(Z)

In diesem Abschnitt wird ein Epimorphismus von $\mathrm{RCWA}(\mathbb{Z})$ auf $\mathbb{Z}^\times$ vorgestellt.

In Anlehnung an die gängige Bezeichnung des Epimorphismus $\mathrm{S}_n \to \mathbb{Z}^\times$ wird dieser hier *Signaturabbildung* genannt.

Transpositionen in der symmetrischen Gruppe S_n lassen sich nicht als Produkte zweier Transpositionen schreiben. Im Gegensatz dazu lassen sich Klassentranspositionen in $\mathrm{RCWA}(\mathbb{Z})$ sehr wohl als Produkte zweier Klassentranspositionen ausdrücken. Daher leitet sich die hier betrachtete Signaturabbildung auch nicht direkt von jener endlicher symmetrischer Gruppen ab, sondern entsteht durch Liften eines Epimorphismus $\mathrm{AFF}(\mathbb{Z}) \to \mathbb{Z}^\times$ von der affinen Gruppe auf ganz $\mathrm{RCWA}(\mathbb{Z})$.

In argumentativer Hinsicht erscheint allerdings eine Konstruktion ausgehend von der Determinantenabbildung günstiger:

2.12.1 Definition Im folgenden sei $\exp : z \mapsto e^{2\pi i z}$. Ferner sei $r(m) \subseteq \mathbb{Z}$ eine Restklasse. Die *Signatur* einer affinen Abbildung $\alpha : n \mapsto (an+b)/c$ mit Definitionsbereich $r(m)$ sei definiert durch

$$\mathrm{sgn}(\alpha) \;:=\; \begin{cases} \exp\left(\dfrac{1}{2}\det(\alpha)\right) & \text{falls } \; a > 0, \\ \exp\left(\dfrac{1}{2}\det(\alpha) - \dfrac{r}{m} + \dfrac{1}{2}\right) & \text{falls } \; a < 0 \end{cases}$$

mit $\det(\alpha) := b/(|a|m)$. Ferner sei die *Signatur* einer Abbildung $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ mit Modul m definiert durch

$$\mathrm{sgn}(\sigma) \;:=\; \prod_{r(m)\in\mathbb{Z}/m\mathbb{Z}} \mathrm{sgn}(\sigma|_{r(m)}).$$

2.12.2 Bemerkung Es sei $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ und $m := \mathrm{Mod}(\sigma)$. Verwendet man für die Koeffizienten von σ die Notation aus Bemerkung 2.11.2, dann ist

$$\mathrm{sgn}(\sigma) \;=\; (-1)^{\det(\sigma) + \frac{1}{m} \sum_{r(m):\ a_{r(m)}<0} (m-2r)},$$

wobei die Determinantenabbildung mittels der Setzung

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

auf ganz $\mathrm{RCWA}(\mathbb{Z})$ ausgedehnt sei.

Der verallgemeinerte Determinantenbegriff in Definition 2.12.1 und Bemerkung 2.12.2 ist für sich genommen wenig sinnvoll, und wird hier lediglich als Hilfskonstruktion eingeführt.

Zum Beweis der Aussage, daß die Determinantenabbildung ein Epimorphismus ist, wurde eine Invariante $\delta\left([r/m]\right)$ von Restklassen $[r/m]$ mit fixierten Repräsentanten eingeführt. Ähnliches ist auch hilfreich beim Beweis der Aussage, daß die Signaturabbildung ein Epimorphismus ist. Hier reicht es allerdings nicht, lediglich Vertreter von Restklassen zu fixieren:

2.12.3 Definition Von nun an seien die Restklassen $[r/m]$ außerdem *orientiert*, d.h. die Restklassen $[r/m]$ und $[r/\text{-}m]$ werden jetzt unterschieden. Die Anwendung einer affinen Abbildung auf eine solche Restklasse kehre das Vorzeichen von deren Modul genau dann um, wenn sie ordnungsumkehrend ist. Es sei $k \in \mathbb{N}$. Die Zerlegung

$$\left[\frac{r}{m}\right] \;=\; \left[\frac{r}{km}\right] \cup \left[\frac{r+m}{km}\right] \cup \dots \cup \left[\frac{r+(k-1)m}{km}\right].$$

einer Restklasse $[r/m]$ heiße *repräsentantenstabil* und *orientierungserhaltend*.

Es sei $\mathcal{P}$ eine Partition von $\mathbb{Z}$ in endlich viele orientierte Restklassen mit fixierten Repräsentanten. Eine Verfeinerung von $\mathcal{P}$ mittels repräsentantenstabiler und orientierungserhaltender Zerlegung enthaltener Restklassen heiße ebenfalls *repräsentantenstabil* und *orientierungserhaltend*.

Orientierten Restklassen mit fixierten Repräsentanten werden im folgenden komplexe Zahlen mit Betrag 1 zugeordnet:

2.12.4 Definition Für eine Restklasse $[r/m]$ sei

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

Für Restklassen $r(m)$ ohne fixierten Repräsentanten und ohne fixierte Orientierung werde stets $m > 0$ und $r \in \{0, \dots, m-1\}$ angenommen, und es sei $\varrho\left(r(m)\right) \;:=\; \varrho\left([r/m]\right)$. Ferner sei für eine Partition $\mathcal{P}$ von $\mathbb{Z}$ in endlich viele orientierte Restklassen mit fixierten Repräsentanten

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

und

$$\varrho\left(\mathbb{Z}\right) \;:=\; (-1)^{\epsilon}\cdot\varrho\left(\mathcal{P}\right).$$

Hierbei sei $\epsilon \in \{0,1\}$ so gewählt, daß $\varrho\left(\mathbb{Z}\right) = \exp\left(t\right)$ mit $t \in [0, \frac{1}{2}[$.

Es ist zu zeigen, daß der Wert $\varrho(\mathbb{Z})$ wohldefiniert ist:

2.12.5 Lemma *Es sei $\mathcal{P}$ eine Partition von $\mathbb{Z}$ in endlich viele orientierte Restklassen mit fixierten Repräsentanten. Dann gilt:*

1. *Der Wert $\varrho(\mathcal{P})$ ist invariant unter repräsentantenstabiler und orientierungserhaltender Verfeinerung von $\mathcal{P}$.*
2. *Der Wert $\varrho(\mathcal{P})$ ändert bei Änderung der Repräsentanten von Restklassen in $\mathcal{P}$ höchstens sein Vorzeichen.*
3. *Der Wert $\varrho(\mathcal{P})$ ändert bei Änderung der Vorzeichen der Moduln von Restklassen in $\mathcal{P}$ höchstens sein Vorzeichen.*

Insbesondere ist der Wert $\varrho(\mathbb{Z})$ also unabhängig von der Wahl der Partition $\mathcal{P}$, und damit wohldefiniert.

Beweis:

1. Für eine Restklasse $[r/m]$ mit positivem Modul m und $k \in \mathbb{N}$ gilt
$$\begin{aligned}
\varrho\left(\left[\frac{r}{m}\right]\right) &= \exp\left(\frac{1}{2}\,\delta\left(\left[\frac{r}{m}\right]\right)\right) \\
&= \exp\left(\frac{1}{2}\left(\frac{r}{m} - \frac{1}{2}\right)\right) \\
&= \exp\left(\frac{1}{2}\left(\frac{r}{m} + \frac{(k-1)k}{2k} - \frac{k}{2}\right)\right) \\
&= \exp\left(\frac{1}{2}\left(\frac{kr}{km} + \frac{1 + \cdots + (k-1)}{k} - \frac{k}{2}\right)\right) \\
&= \prod_{i=0}^{k-1} \exp\left(\frac{1}{2}\left(\frac{r+im}{km} - \frac{1}{2}\right)\right) \\
&= \prod_{i=0}^{k-1} \exp\left(\frac{1}{2}\,\delta\left(\left[\frac{r+im}{km}\right]\right)\right) \\
&= \prod_{i=0}^{k-1} \varrho\left(\left[\frac{r+im}{km}\right]\right).
\end{aligned}$$
Im Falle $m < 0$ kehren sich lediglich die Vorzeichen sämtlicher Exponenten um, was keinen Einfluß auf die Gültigkeit der angegebenen Gleichungskette hat. Es folgt die Invarianz von $\varrho(\mathcal{P})$ unter repräsentantenstabiler und orientierungserhaltender Verfeinerung von $\mathcal{P}$.

2. Für $m > 0$ und $k \in \mathbb{Z}$ gilt

$$\begin{aligned}
\varrho\left(\left[\frac{r}{m}\right]\right) &= \exp\left(\frac{1}{2}\,\delta\left(\left[\frac{r}{m}\right]\right)\right) \\
&= \exp\left(\frac{1}{2}\left(\frac{r}{m} - \frac{1}{2}\right)\right) \\
&= \exp\left(\frac{r+km}{2m} - \frac{1}{4} - \frac{k}{2}\right) \\
&= \exp\left(\frac{1}{2}\left(\frac{r+km}{m} - \frac{1}{2}\right)\right) \cdot \exp\left(-\frac{k}{2}\right) \\
&= \exp\left(\frac{1}{2}\,\delta\left(\left[\frac{r+km}{m}\right]\right)\right) \cdot \exp\left(\frac{k}{2}\right) \\
&= \varrho\left(\left[\frac{r+km}{m}\right]\right) \cdot (-1)^k.
\end{aligned}$$

Im Falle $m < 0$ kehren sich wieder lediglich die Vorzeichen der Exponenten um, was keinen Einfluß auf die Gültigkeit der Gleichungskette hat. Ändert man den Repräsentanten einer Restklasse aus $\mathcal{P}$, dann ändert sich also höchstens das Vorzeichen von $\varrho\,(\mathcal{P})$.

3. Die Änderung der Orientierung einer Restklasse $[r/m] \in \mathcal{P}$ ändert $\varrho\,(\mathcal{P})$ um den Faktor

$$\frac{\varrho\left(\left[\frac{r}{-m}\right]\right)}{\varrho\left(\left[\frac{r}{m}\right]\right)} = \frac{\exp\left(-\frac{1}{2}\left(\frac{r}{-m} - \frac{1}{2}\right)\right)}{\exp\left(\frac{1}{2}\left(\frac{r}{m} - \frac{1}{2}\right)\right)} = \exp\left(\frac{1}{2}\right) = -1.$$

Es folgt die Behauptung. □

2.12.6 Bemerkung Der Wert $\varrho\,(\mathbb{Z})$ läßt sich leicht ausrechnen – es ist

$$\varrho\,(\mathbb{Z}) = \exp\left(\frac{1}{2}\,\delta\,(\mathbb{Z})\right) = \exp\left(\frac{1}{4}\right) = i.$$

Seine explizite Kenntnis ist im folgenden allerdings nicht erforderlich.

Es gelten ähnliche Aussagen wie für $\det(\alpha)$ und $\delta([r/m])$:

2.12.7 Lemma *Für eine affine Abbildung α mit Definitionsbereich $r(m)$ gilt*

$$\varrho\left(\left[\frac{r}{m}\right]^\alpha\right) \;=\; \varrho\left(\left[\frac{r}{m}\right]\right)\cdot \operatorname{sgn}(\alpha).$$

Ist $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ und $\mathcal{P}$ eine Partition von $\mathbb{Z}$ in endlich viele orientierte Restklassen mit fixierten Repräsentanten, dann gilt

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

und mithin

$$\varrho\left(\mathbb{Z}^\sigma\right) \;=\; (-1)^\epsilon \cdot \varrho\left(\mathbb{Z}\right)\cdot \operatorname{sgn}(\sigma)$$

für ein geeignetes $\epsilon \in \{0,1\}$.

Beweis: Die Abbildung α sei gegeben durch $n \mapsto (an+b)/c$ für gewisse $a,b,c \in \mathbb{Z}$. Im Fall $a > 0$ überträgt sich die Aussage direkt von Lemma 2.11.8. Es kann also o.E. angenommen werden, daß $a < 0$. Es gilt

$$\begin{aligned}
\varrho\left(\left[\frac{r}{m}\right]^\alpha\right) &= \varrho\left(\left[\frac{(ar+b)/c}{am/c}\right]\right)\\
&= \exp\left(-\frac{1}{2}\,\delta\left(\left[\frac{(ar+b)/c}{am/c}\right]\right)\right)\\
&= \exp\left(-\frac{1}{2}\left(\frac{ar+b}{am}-\frac{1}{2}\right)\right)\\
&= \exp\left(-\frac{r}{2m}+\frac{b}{2|a|m}+\frac{1}{4}\right)\\
&= \exp\left(\frac{1}{2}\left(\frac{r}{m}-\frac{1}{2}\right)\right)\cdot\exp\left(\frac{b}{2|a|m}-\frac{r}{m}+\frac{1}{2}\right)\\
&= \varrho\left(\left[\frac{r}{m}\right]\right)\cdot \operatorname{sgn}(\alpha),
\end{aligned}$$

was zu zeigen war.

Die entsprechende Aussage für eine rcwa-Abbildung σ und eine Partition $\mathcal{P}$ erhält man, indem man $\mathcal{P}$ repräsentantenstabil und ordnungserhaltend zu einem Träger von σ verfeinert, und die soeben gezeigte Aussage auf die Restklassen in $\mathcal{P}$ und die Einschränkungen von σ auf dieselben anwendet. Dies ist zulässig wegen Lemma 2.12.5. □

2.12.8 Satz *Die Signaturabbildung*

$$\mathrm{RCWA}(\mathbb{Z}) \;\rightarrow\; \mathbb{Z}^{\times}, \quad \sigma \;\mapsto\; \mathrm{sgn}(\sigma)$$

ist ein Epimorphismus.

Beweis: Es seien $\sigma_1, \sigma_2, \sigma \in \mathrm{RCWA}(\mathbb{Z})$. Es ist zu zeigen, daß $\mathrm{sgn}(\sigma)$ eine Einheit in $\mathbb{Z}$ ist, daß $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1}$, daß $\mathrm{sgn}(\sigma_1\sigma_2) = \mathrm{sgn}(\sigma_1) \cdot \mathrm{sgn}(\sigma_2)$ und daß es eine bijektive rcwa-Abbildung von $\mathbb{Z}$ mit Signatur -1 gibt.

1. Es ist zu zeigen, daß die Signatur von σ tatsächlich eine Einheit in $\mathbb{Z}$ ist. Nach Lemma 2.12.7 gilt $\varrho\,(\mathbb{Z}) = \varrho\,(\mathbb{Z}^{\sigma}) = (-1)^{\epsilon} \cdot \varrho\,(\mathbb{Z}) \cdot \mathrm{sgn}(\sigma)$ für geeignetes $\epsilon \in \{0, 1\}$. Division des linken und des rechten Terms der Gleichungskette durch $\varrho\,(\mathbb{Z})$ liefert die behauptete Aussage.

2. Es ist zu zeigen, daß $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1}$. Es genügt offenbar, dies für eine affine Teilabbildung von σ auf einer Restklasse $r(m)$ zu zeigen. Es sei also

   $$\alpha: \quad r(m) \;\rightarrow\; \frac{ar+b}{c}\left(\frac{|a|m}{c}\right), \quad n \mapsto (an+b)/c$$

   eine solche. Dann ist

   $$\alpha^{-1}: \quad \frac{ar+b}{c}\left(\frac{|a|m}{c}\right) \;\rightarrow\; r(m), \quad n \mapsto (-cn+b)/-a.$$

   Im Fall $a > 0$ gilt $\mathrm{sgn}(\alpha^{-1}) = \exp\left(-b/(2am)\right) = \mathrm{sgn}(\alpha)^{-1}$, und im Fall $a < 0$ gilt

   $$\begin{aligned}
   \mathrm{sgn}(\alpha^{-1}) &= \exp\left(\frac{b}{2c|am/c|} - \frac{(ar+b)/c}{|am/c|} + \frac{1}{2}\right) = \exp\left(\frac{b}{2|a|m} - \frac{ar+b}{|a|m} + \frac{1}{2}\right) \\
   &= \exp\left(\frac{b}{2|a|m} + \frac{r}{m} - \frac{b}{|a|m} + \frac{1}{2}\right) = \exp\left(-\frac{b}{2|a|m} + \frac{r}{m} - \frac{1}{2}\right) \\
   &= \mathrm{sgn}(\alpha)^{-1}.
   \end{aligned}$$

   Es folgt die Behauptung.

3. Es ist zu zeigen, daß $\mathrm{sgn}(\sigma_1\sigma_2) = \mathrm{sgn}(\sigma_1) \cdot \mathrm{sgn}(\sigma_2)$. Es sei $\mathcal{P}$ eine Partition von $\mathbb{Z}$ in endlich viele orientierte Restklassen mit fixierten Repräsentanten. Nach Lemma 2.12.7 gilt

   $$\varrho\,(\mathcal{P}) \cdot \mathrm{sgn}(\sigma_1\sigma_2) \;=\; \varrho\,(\mathcal{P}^{\sigma_1\sigma_2}) \;=\; \varrho\,(\mathcal{P}^{\sigma_1}) \cdot \mathrm{sgn}(\sigma_2) \;=\; \varrho\,(\mathcal{P}) \cdot \mathrm{sgn}(\sigma_1) \cdot \mathrm{sgn}(\sigma_2).$$

   Division des linken und des rechten Terms der Gleichungskette durch $\varrho\,(\mathcal{P})$ liefert die Behauptung.

4. Die Abbildung $\varsigma \in \mathrm{RCWA}(\mathbb{Z}): \; n \mapsto -n$ besitzt die Signatur -1. $\square$

In Definition 2.9.1 wurden drei unendliche Serien bijektiver rcwa-Abbildungen von $\mathbb{Z}$ vorgestellt, die entweder ganz RCWA($\mathbb{Z}$) oder aber einen nichttrivialen Normalteiler erzeugen (vgl. Satz 2.9.4). Es soll die Signatur dieser Abbildungen bestimmt werden:

2.12.9 Lemma *Für eine Restklasse $r(m)$ von $\mathbb{Z}$ gilt stets* $\mathrm{sgn}(\nu_{r(m)}) = \mathrm{sgn}(\varsigma_{r(m)}) = -1$. *Für zwei disjunkte Restklassen $r_1(m_1)$ und $r_2(m_2)$ von $\mathbb{Z}$ gilt stets* $\mathrm{sgn}(\tau_{r_1(m_1),r_2(m_2)}) = 1$.

Beweis: Einsetzen in den Ausdruck in Bemerkung 2.12.2 liefert

$$\mathrm{sgn}(\nu_{r(m)}) \;=\; (-1)^{\frac{1}{m}\left(\frac{0}{1}+\dots+\frac{0}{1}+\frac{m}{1}\right)+0} \;=\; -1$$

und

$$\mathrm{sgn}(\varsigma_{r(m)}) \;=\; (-1)^{\frac{1}{m}\left(\frac{2r}{1}+\frac{0}{1}+\dots\right)+\frac{1}{m}(m-2r)} \;=\; -1$$

sowie – mit ein klein wenig mehr Überlegung –

$$\mathrm{sgn}(\tau_{r_1(m_1),r_2(m_2)}) \;=\; (-1)^{\frac{1}{m_1m_2}(m_1r_2-m_2r_1+m_2r_1-m_1r_2)} \;=\; 1.$$

Im letztgenannten Fall wird davon Gebrauch gemacht, daß der Modul der Klassentransposition $\tau_{r_1(m_1),r_2(m_2)}$ ein Teiler von m_1m_2 ist, und daß $r_i(m_i)$ ($i \in \{1,2\}$) sich als Vereinigung von m_{3-i} Restklassen (mod m_1m_2) schreiben läßt. □

2.12.10 Beispiel Die Collatz'sche Permutation α aus Beispiele 1.1.3 hat die Determinante 0, und mithin die Signatur $(-1)^0 = 1$. Nach Lemma 2.12.9 besitzt die Klassenspiegelung $\varsigma_{1(5)}$ die Signatur -1. Satz 2.12.8 besagt nun, daß $\mathrm{sgn}(\alpha \cdot \varsigma_{1(5)}) = -1$. Dies soll zur Illustration direkt nachgerechnet werden. Es ist

$$\alpha \cdot \varsigma_{1(5)}: \quad n \longmapsto \begin{cases} \frac{3n}{2} & \text{falls} \quad n \in 0(2) \setminus 4(10), \\ \frac{-3n+7}{4} & \text{falls} \quad n \in 1(20), \\ \frac{3n-1}{4} & \text{falls} \quad n \in 3(20) \cup 7(20) \cup 11(20) \cup 19(20), \\ \frac{-3n+4}{2} & \text{falls} \quad n \in 4(10), \\ \frac{3n+1}{4} & \text{falls} \quad n \in 5(20) \cup 9(20) \cup 13(20) \cup 17(20), \\ \frac{-3n+9}{4} & \text{falls} \quad n \in 15(20). \end{cases}$$

Einsetzen in die Definition liefert $\det(\alpha \cdot \varsigma_{1(5)}) = \frac{2}{5}$, sowie einen 'Korrekturterm' im Exponenten von $\frac{1}{20}((20-2\cdot1)+(20-2\cdot4)+(20-2\cdot14)+(20-2\cdot15)) = \frac{3}{5}$. Hieraus errechnet sich – wie erwartet – die Signatur $(-1)^{2/5+3/5} = -1$.

Nach Bemerkung 2.12.2 ist die Signatur einer Abbildung $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ gleich $(-1)^{\det(\sigma)}$, und nach Lemma 2.12.9 besitzen Klassenshifts und Klassenspiegelungen die Signatur -1. Es gilt also:

2.12.11 Korollar Es sei $m \in \mathbb{N}$ und $r \in \mathbb{Z}$. Dann kommutiert das folgende Diagramm:

$$
\begin{tikzcd}
 & & \langle \nu, \varsigma \rangle \arrow[d, equal] & 1 & \\
1 \arrow[r] & \langle \nu^2, \nu\varsigma \rangle \arrow[r, hook, "\mathrm{id}"] \arrow[ddrr, hook, "\pi_{n \mapsto mn+r}"] & \mathrm{AFF}(\mathbb{Z}) \arrow[r, two heads, "{\nu \mapsto -1,}", "\varsigma \mapsto -1"'] \arrow[dr, hook, "\pi_{n \mapsto mn+r}"] & \mathbb{Z}^\times \arrow[r] \arrow[u] & 1 \\
 & & & \mathrm{RCWA}(\mathbb{Z}) \arrow[u, "\mathrm{sgn}"] & (\mathbb{Z},+) \arrow[u] \arrow[ul, "n \mapsto (-1)^n"'] \\
 & & & \ker \mathrm{sgn} \arrow[u, hook, "\mathrm{id}"] & \mathrm{RCWA}^+(\mathbb{Z}) \arrow[u, two heads, "\det"] \arrow[ul, hook, "\mathrm{id}"'] \\
 & & & 1 \arrow[u] & \ker \det \arrow[u, hook, "\mathrm{id}"] \arrow[ul, hook, "\mathrm{id}"'] \\
 & & & & 1 \arrow[u]
\end{tikzcd}
$$

Die waagrecht bzw. senkrecht eingezeichneten Sequenzen sind kurz exakt.

Wie beliebig ist die Signaturabbildung gewählt? – Ein paar Aussagen hierzu liefert die folgende

2.12.12 Bemerkung Welche Werte könnte ein Epimorphismus von RCWA($\mathbb{Z}$) auf $\mathbb{Z}^\times$ für Klassenshifts, Klassenspiegelungen und Klassentranspositionen sonst noch annehmen?

Unter Annahme der Invarianz eines solchen Epimorphismus unter Einschränkungsmonomorphismen kommt für das Bild einer Klassentransposition nur die 1 in Frage, denn es ist $\tau = \tau_{0(4),1(4)} \cdot \tau_{2(4),3(4)}$. An der Gleichung $\varsigma \cdot \varsigma_{0(2)} \cdot \varsigma_{1(2)} \cdot \nu_{1(2)}^{-1} = 1$ erkennt man ferner, daß Klassenshifts und Klassenspiegelungen dasselbe Bild haben müssen.

Folglich ist die Signaturabbildung der einzige unter Einschränkungsmonomorphismen invariante Epimorphismus von RCWA($\mathbb{Z}$) auf $\mathbb{Z}^\times$, dessen Kern nicht den von allen Klassenshifts, Klassenspiegelungen und Klassentranspositionen erzeugten Normalteiler enthält (vgl. Satz 2.9.4).

2.13 Offene Fragen

Folgende Fragen bleiben bislang unbeantwortet:

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

  Besitzt die Gruppe RCWA($\mathbb{Z}$) weitere Normalteiler?

  Falls ja: Wie sehen diese bzw. die zugehörigen Faktorgruppen aus?

- Ist der Kern der Signaturabbildung bzw. der Determinantenabbildung einfach?

  Falls nein: Welche Normalteiler besitzen diese Gruppen?

- Wird die Gruppe RCWA($\mathbb{Z}$) von der Menge der zahmen Abbildungen erzeugt?

  Sofern dies der Fall ist: Besitzt sie bezüglich dieser Menge als Erzeugendensystem endlichen Durchmesser, und wenn ja, welchen?

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

- Sind endlich erzeugte rcwa-Gruppen stets sogar endlich präsentiert?

- Gibt es zu jedem $k \in \mathbb{N}$ rcwa-Gruppen, die auf einer unendlichen Bahn k-fach transitiv, aber nicht $k+1$-fach transitiv operieren?

- Besitzen die Gruppen GL($n, \mathbb{Z}$) treue ganzzahlige rcwa-Darstellungen? Besitzt die freie Gruppe vom Rang 2 eine solche?

- Ist das Konjugiertheits- bzw. das Enthaltenseinsproblem in endlich erzeugten rcwa-Gruppen algorithmisch entscheidbar? – Das GAP - Package RCWA bietet für beide Probleme Verfahren an, die 'in vielen Fällen' praktikabel sind.

KAPITEL 3

Trajektorien und Monotonisierungen

Die $3n + 1$ - Vermutung trifft eine Aussage über die Zahlenfolge $n, n^T, n^{T^2}, \ldots$, die man erhält, wenn man die Collatz-Abbildung T iteriert auf eine natürliche Zahl n anwendet.

Es ist naheliegend zu fragen, was sich ändert, wenn man die Collatz-Abbildung durch eine andere Abbildung ersetzt. Um interessante Aussagen erwarten zu können, wird man die Klasse der betrachteten Abbildungen einschränken müssen. Den Fokus des Interesses auf rcwa-Abbildungen als der Collatz-Abbildung besonders 'ähnlicher' Abbildungen zu lenken erscheint nicht unangebracht.

Dieser Fragenkomplex wurde bislang überhaupt nicht angeschnitten. In diesem Kapitel sollen ein paar Betrachtungen hierzu nachgeholt werden.

3.1 Definition Ist $f : R \to R$ eine Abbildung und ist $n \in R$, dann bezeichnet man die Folge $(n^{f^k})_{k\in\mathbb{N}_0}$ als *Trajektorie* von f mit *Startwert* n.

Zur Illustration seien ein paar Beispiele für Trajektorien der Collatz-Abbildung angegeben:

3.2 Beispiele Die Trajektorien von T mit den Startwerten 15, 27, -5 bzw. -17 sind

$$15, 23, 35, 53, 80, 40, 20, 10, 5, 8, 4, 2, 1, \text{ bzw.}$$

$$\begin{aligned}&27, 41, 62, 31, 47, 71, 107, 161, 242, 121, 182, 91, 137, 206, 103, 155, 233, 350, 175,\\&263, 395, 593, 890, 445, 668, 334, 167, 251, 377, 566, 283, 425, 638, 319, 479, 719,\\&1079, 1619, 2429, 3644, 1822, 911, 1367, 2051, 3077, 4616, 2308, 1154, 577, 866, 433,\\&650, 325, 488, 244, 122, 61, 92, 46, 23, 35, 53, 80, 40, 20, 10, 5, 8, 4, 2, 1, \text{ bzw.}\end{aligned}$$

$$-5, -7, -10, -5, \text{ bzw.}$$

$$-17, -25, -37, -55, -82, -41, -61, -91, -136, -68, -34, -17,$$

wobei jeweils bei 1 bzw. bei Vollendung eines Zyklus abgebrochen wurde.

3.3 Bemerkung Im Laufe des vergangenen halben Jahrhunderts haben schon viele Leute versucht, die $3n+1$ - Vermutung zu beweisen. Die verwendeten Ansätze sind vielfältig. Zu nennen sind hier auf jeden Fall dynamische Systeme und analytische Dichteabschätzungen. Für eine gute Übersicht empfiehlt sich ein Blick in Lagarias' kommentierte Bibliographie [Lag05].

Eine gute Darstellung der $3n + 1$ - Vermutung unter dem Aspekt des ihr zugrundeliegenden dynamischen Systems sowie eine ausführliche elementare Diskussion weiterer Aspekte findet der Leser in der Habilitationsschrift von Günther Wirsching [Wir96]. Die Arbeit von Wirsching ist auch als *Springer Lecture Notes*-Band [Wir98] erschienen. Der Schwerpunkt von Herrn Wirschings Interesse ist, zu zeigen, daß alle Zahlen $n_0 \in \mathbb{N} \setminus 0(3)$ *positive Vorgängerdichte* haben, also daß

$$\liminf_{K \to \infty} \frac{|\{n \in \{1, 2, \ldots, K\} \mid \exists k \in \mathbb{N}_0 : \ n^{T^k} = n_0\}|}{K} \ > \ 0.$$

Diese Aussage ist mit der $3n + 1$ - Vermutung sehr eng verwandt, aber weder impliziert sie sie noch wird sie von ihr impliziert. Eine Beweisskizze mit drei als Vermutungen formulierten Lücken stellt er dar in [Wir03].

Was besagt die $3n + 1$ - Vermutung ? – Letztlich doch im Grunde, daß jede Trajektorie der Collatz-Abbildung T sich nichttrivial mit einer gegebenen endlichen Menge ganzer Zahlen schneidet, oder anders ausgedrückt, daß sie kontrahierend ist im folgenden Sinne:

3.4 Definition Es sei $f : R \to R$ eine beliebige Abbildung des Rings R auf sich selbst. Eine aufsteigende Folge $M_0 \subsetneq M_1 \subseteq M_2 \subseteq \ldots$ von Teilmengen von R so, daß

1. M_0 eine endliche Menge mit $M_0^f = M_0$ ist, daß
2. für jedes $k \in \mathbb{N}$ die Menge M_k das volle Urbild von M_{k-1} unter f ist, und daß
3. $R = \bigcup_{k=0}^{\infty} M_k$ gilt

heiße *Kontraktionssequenz* von f. Gibt es eine solche, dann werde f als *kontrahierend* bezeichnet, und die Menge M_0 heiße *Kontraktionszentrum* von f.

3.5 Bemerkung Kontraktionssequenz und -zentrum einer kontrahierenden Abbildung $f \in \mathrm{Rcwa}(R)$ sind eindeutig bestimmt. Man kann also von *der* Kontraktionssequenz und *dem* Kontraktionszentrum von f sprechen. Ist die Abbildung f kontrahierend und $\sigma \in \mathrm{Sym}(R)$, so ist auch f^σ kontrahierend – ist $(M_k)_{k \in \mathbb{N}_0}$ eine Kontraktionssequenz von f, so ist $(M_k^\sigma)_{k \in \mathbb{N}_0}$ eine solche von f^σ.

3.6 Beispiele Diese Definitionen sollen mit ein paar Beispielen illustriert werden.

1. Der Autor vermutet, daß die Collatz-Abbildung T kontrahierend ist, und daß sie das Kontraktionszentrum
$$M_0 = \{ -136, -91, -82, -68, -61, -55, -41, \\ -37, -34, -25, -17, -10, -7, -5, -1, 0, 1, 2 \}$$
besitzt. Könnte man dies zeigen, dann hätte man die $3n+1$ - Vermutung bewiesen. Die Mengen $M_1, M_2, \dots, M_{25}$ hätten dann die Kardinalitäten 30, 42, 66, 95, 138, 187, 258, 345, 467, 627, 848, 1138, 1529, 2041, 2731, 3646, 4865, 6485, 8651, 11529, 15384, 20506, 27312, 36379 bzw. 48497.

2. Der Autor vermutet, daß die Abbildung
$$T_7 \in \mathrm{Rcwa}(\mathbb{Z}), \quad n \longmapsto \begin{cases} \frac{7n+1}{2} & \text{falls} \quad \mathrm{ggT}(n,6) = 1, \\ \frac{n}{\mathrm{ggT}(n,6)} & \text{sonst} \end{cases}$$
kontrahierend ist und das Kontraktionszentrum
$$M_0 = \{ -360, -206, -103, -66, -60, -59, -38, -19, -17, -11, -10, -5, -3, -1, 0, \\ 1, 2, 4, 19, 38, 65, 67, 143, 167, 195, 228, 235, 429, 501, 585, 823, 1103, 1287, \\ 2206, 2521, 2881, 3861, 4412, 5042, 8824, 10084 \}.$$
besitzt. Dies ist nicht offensichtlich – z.B. liegt erst das 4361. Glied der Trajektorie von T_7 mit Startwert 9595 in M_0, und das bei Glied Nr. 1855 angenommene Maximum dieser Folge ist 45266766717824274611851780017733940744283387822 72.

3. Der Autor vermutet, daß die Abbildung
$$f_6 \in \mathrm{Rcwa}(\mathbb{Z}) : \quad n \longmapsto \begin{cases} \frac{n}{6} & \text{falls} \quad n \in 0(6), \\ \frac{5n+1}{6} & \text{falls} \quad n \in 1(6), \\ \frac{7n-2}{6} & \text{falls} \quad n \in 2(6), \\ \frac{11n+3}{6} & \text{falls} \quad n \in 3(6), \\ \frac{11n-2}{6} & \text{falls} \quad n \in 4(6), \\ \frac{11n-1}{6} & \text{falls} \quad n \in 5(6) \end{cases}$$
ebenfalls kontrahierend ist, und daß ihr Kontraktionszentrum eine Kardinalität $\geqslant 443$ besitzt. Die Trajektorie mit Startwert 3224 erreicht den Fixpunkt 2 nach 19949562 Folgengliedern und einem Ansteigen bis auf ca. $3 \cdot 10^{2197}$. Man beachte hierzu, daß das Produkt der Koeffizienten in den Zählern ($5 \cdot 7 \cdot 11^3 = 46585$) nur wenig kleiner ist als jenes der Koeffizienten in den Nennern ($6^6 = 46656$). Dies bewirkt, daß das Bild einer Zahl n unter der Abbildung f_6 betragsmäßig 'im Schnitt' um den Faktor $\sqrt[6]{46585/46656} \approx 0.999746$ kleiner ist als n selbst. Es erübrigt sich zu bemerken, daß letztere Betrachtung rein heuristisch ist.

4. Eine weitere Abbildung, von der der Autor vermutet, daß sie kontrahierend ist, ist

$$f_5 \in \mathrm{Rcwa}(\mathbb{Z}): \quad n \longmapsto \begin{cases} \frac{7n}{5} & \text{falls } n \in 0(5), \\ \frac{7n-2}{5} & \text{falls } n \in 1(5), \\ \frac{3n-1}{5} & \text{falls } n \in 2(5), \\ \frac{3n+1}{5} & \text{falls } n \in 3(5), \\ \frac{7n+2}{5} & \text{falls } n \in 4(5). \end{cases}$$

Es gilt $\forall n \in \mathbb{Z}\ (-n)^{f_5} = -(n^{f_5})$. Das mutmaßliche Kontraktionszentrum von f_5 besitzt mindestens die Kardinalität $3659 = 1+2\cdot(1\cdot1+5\cdot5+1\cdot141+6\cdot277)$: Fixpunkte von f_5 sind 0 und ±1, Zykel der Länge 5 sind $\pm(4\ 6\ 8\ 5\ 7)$, $\pm(10\ 14\ 20\ 28\ 17)$, $\pm(29\ 41\ 57\ 34\ 48)$, $\pm(35\ 49\ 69\ 97\ 58)$ sowie $\pm(50\ 70\ 98\ 59\ 83)$, betragsmäßig kleinste Elemente von 141-Zykeln sind ±89 und betragsmäßig kleinste Elemente von 277-Zykeln sind ±2536, ±3199, ±12571, ±13075, ±16564 sowie ±27589. Ob das Zustandekommen der genannten 6 Paare von 277-Zykeln lediglich gewissermaßen 'Zufall' ist oder tiefere Gründe hat, ist unklar.

Bereits in der Zusammenfassung wurde darauf hingewiesen, daß es für einen Beweis der $3n+1$ - Vermutung ausreichen würde, eine Permutation $\sigma \in (\mathrm{Sym}(\mathbb{Z})_{\{\mathbb{N}\}})_1$ so zu finden, daß $\forall n \in \mathbb{N} \setminus \{1\}\ n^{T^\sigma} < n$. Wegen der Surjektivität von T kann man diese Bedingung auch gegen die Forderung nach Monotonie von T^σ eintauschen. Dies ist die Motivation für die nachfolgende Definition.

3.7 Definition Es sei R angeordnet, also beispielsweise $R \in \{\mathbb{Z}, \mathbb{Z}_{(\pi)}\}$. Eine Abbildung $f \in \mathrm{Rcwa}(R)$ heiße *monotonisierbar*, falls es eine Permutation $\sigma \in \mathrm{Sym}(R)$ so gibt, daß f^σ monoton ist. Sie heiße *rcwa-monotonisierbar*, wenn man für σ sogar eine rcwa-Abbildung wählen kann. Als *fast (rcwa-)monotonisierbar* bezeichnet werde f, falls es ein $\sigma \in \mathrm{Sym}(R)$ ($\sigma \in \mathrm{RCWA}(R)$) und eine endliche Menge $M \subsetneq R$ so gibt, daß f^σ auf $R \setminus M$ monoton ist.

Um klären zu können, wie die Eigenschaften einer rcwa-Abbildung, monotonisierbar bzw. kontrahierend zu sein, voneinander abhängen, benötigt man folgendes Lemma:

3.8 Lemma *Es sei $f \in \mathrm{Rcwa}(R)$ nicht injektiv und es sei $\mathrm{Mult}(f) \neq 0$. Dann gibt es eine Restklasse $r_0(m_0)$ und zwei disjunkte Restklassen $r_1(m_1)$ und $r_2(m_2)$ von R so, daß $r_0(m_0) = r_1(m_1)^f = r_2(m_2)^f$.*

Beweis: Es sei $m := \mathrm{Mod}(f)$. Da die Abbildung f nach Voraussetzung nicht injektiv ist, gibt es zwei Restklassen $\tilde{r}_1(m)$ und $\tilde{r}_2(m)$, deren Bilder unter f nicht disjunkt sind. Wegen der Voraussetzung $\mathrm{Mult}(f) \neq 0$ sind $\tilde{r}_1(m)^f$ und $\tilde{r}_2(m)^f$ nach Lemma 1.1.8, Aussage (1) ebenfalls Restklassen. Damit ist $r_0(m_0) := \tilde{r}_1(m)^f \cap \tilde{r}_2(m)^f$ gleichfalls eine solche. Die Urbilder $r_1(m_1)$ und $r_2(m_2)$ von $r_0(m_0)$ unter den affinen Teilabbildungen von f auf $\tilde{r}_1(m)$ bzw. $\tilde{r}_2(m)$ sind nach Lemma 1.1.8, Aussage (1) ebenfalls Restklassen. Sie sind ferner disjunkt, da sie Teilmengen verschiedener Restklassen (mod m) sind. □

3.9 Lemma *Ist eine Abbildung $f \in \mathrm{Rcwa}(\mathbb{Z})$ surjektiv, nicht injektiv und fast monotonisierbar, so ist sie kontrahierend.*

Beweis: Es sei $M \subset \mathbb{Z}$ eine endliche Menge und $\sigma \in \mathrm{Sym}(\mathbb{Z})$ so, daß f^σ auf $\mathbb{Z} \setminus M$ monoton ist. Mit f ist auch f^σ surjektiv und nicht injektiv. Es folgt, daß alle bis auf endlich viele $n \in \mathbb{Z}$ unter f^σ auf betragsmäßig kleinere Zahlen abgebildet werden (man stelle sich den Funktionsgraphen vor!). Hieraus folgt die Kontraktionseigenschaft für f^σ, und damit nach Bemerkung 3.5 auch für die Abbildung f selbst. □

Im Beweis der Hauptaussage (3.11) im Zusammenhang mit kontrahierenden rcwa-Abbildungen benötigt man folgendes Lemma:

3.10 Lemma *Zu $f \in \mathrm{Rcwa}(R)$ gibt es ein $c \in R$ so, daß $\forall x \in R \ \ |x^f| \leqslant \mathrm{Mult}(f) \cdot |x| + c$.*

Beweis: Die Aussage folgt per Maximumsbildung über die affinen Teilabbildungen. □

Der folgende Satz liefert eine recht restriktive Bedingung für rcwa-Monotonisierbarkeit:

3.11 Satz *Ist $f \in \mathrm{Rcwa}(\mathbb{Z}) \setminus \mathrm{RCWA}(\mathbb{Z})$ surjektiv und (fast) rcwa-monotonisierbar und ist $\mathrm{Mult}(f) \neq 0$, dann gibt es ein $k \in \mathbb{N}$ so, daß es höchstens endlich viele $n \in \mathbb{Z}$ mit $|n^{f^k}| \geqslant |n|$ gibt.*

Beweis: Aufgrund der (fast-)rcwa-Monotonisierbarkeit von f kann man eine Abbildung $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ und eine endliche Teilmenge $M \subset \mathbb{Z}$ so wählen, daß $\mu := f^\sigma \in \mathrm{Rcwa}(\mathbb{Z})$ monoton auf $\mathbb{Z} \setminus M$ ist. Surjektivität und Nichtinjektivität übertragen sich offenbar von f auf μ, und wegen Lemma 1.3.1, Aussage (a.4) und (b.3) ist $\mathrm{Mult}(\mu) \neq 0$. Folglich gibt es also nach Lemma 3.8 eine Restklasse $r(m) \subset \mathbb{Z}$ so, daß jedes $n \in r(m)$ mindestens zwei verschiedene Urbilder unter μ besitzt. Aus der Surjektivität von μ, der Monotonie von μ auf $\mathbb{Z} \setminus M$ und der Endlichkeit von M kann man jetzt schließen, daß es eine Konstante $c \in \mathbb{N}$ so gibt, daß

$$\forall n \in \mathbb{Z} \ \ |n^\mu| \ < \ \frac{m}{m+1} \cdot |n| + c,$$

und Induktion über $k \in \mathbb{N}$ liefert

$$\forall k \in \mathbb{N} \ \forall n \in \mathbb{Z} \ \ \left|n^{\mu^k}\right| \ < \ \left(\frac{m}{m+1}\right)^k \cdot |n| + k \cdot c.$$

Für beliebiges $k \in \mathbb{N}$ ist $n^{f^k} = n^{\sigma^{-1}\mu^k\sigma}$. Wählt man nun k so, daß

$$\left(\frac{m}{m+1}\right)^k \ < \ \frac{1}{2 \cdot \mathrm{Mult}(\sigma) \cdot \mathrm{Div}(\sigma)} \ ,$$

dann gilt nach Lemma 1.3.1b, Aussage (3) und Lemma 3.10

$$\left|n^{f^k}\right| \ = \ \left|n^{\sigma^{-1}\mu^k\sigma}\right| \ < \ \mathrm{Div}(\sigma) \cdot \left(\frac{m}{m+1}\right)^k \cdot |n| \cdot \mathrm{Mult}(\sigma) + k \cdot c + c' \ < \ \frac{1}{2}|n| + k \cdot c + c'$$

für eine Konstante c' abhängig von σ. Da weder k noch c oder c' von n abhängen, folgt die Behauptung. □

Gibt es ein $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ so, daß T^σ monoton ist? – Nein, so einfach geht's nicht!:

3.12 Bemerkung Mittels Satz 3.11 kann man ohne weiteres schließen, daß die Collatz-Abbildung T nicht fast rcwa-monotonisierbar ist: Die Abbildung T ist zwar surjektiv und nicht injektiv, und es ist $\mathrm{Mult}(T) \neq 0$. Ist aber $n = 2^k m - 1$ für $k, m \in \mathbb{N}$ beliebig, so gilt

$$n^{T^k} \;=\; \frac{3^k n + (3^k - 2^k)}{2^k} \;>\; n.$$

Um ein fast überall monotones Konjugiertes T^σ zu erhalten, müßte man also zumindest auf Abbildungen $\sigma \in \mathrm{Sym}(\mathbb{Z}) \setminus \mathrm{RCWA}(\mathbb{Z})$ ausweichen. Insbesondere dürfte der Quotient n^σ/n nicht beschränkt sein, denn dessen Beschränktheit für rcwa-Abbildungen ist letzten Endes der springende Punkt im Beweis von Satz 3.11.

Zum Abschluß dieses durch die $3n+1$ - Vermutung motivierten kurzen Kapitels soll gezeigt werden, daß die Collatz-Abbildung sich auf natürliche Weise zu einer Permutation von $\mathbb{Z}^2$ fortsetzen läßt:

3.13 Beispiel Die Abbildung

$$\sigma_T \in \mathrm{Sym}(\mathbb{Z}^2): \quad (x,y) \;\longmapsto\; \begin{cases} \left(\frac{3x+1}{2}, 2y\right) & \text{falls } x \in 1(2), \\ \left(\frac{x}{2}, y\right) & \text{falls } x \in 0(6) \cup 2(6), \\ \left(\frac{x}{2}, 2y+1\right) & \text{falls } x \in 4(6) \end{cases}$$

ist eine Permutation, die auf der x-Koordinate wie die Collatz-Abbildung T wirkt, und σ_T^{-1} ist gegeben durch

$$(x,y) \;\longmapsto\; \begin{cases} (2x, y) & \text{falls } x \in 0(3) \cup 1(3), \\ \left(\frac{2x-1}{3}, \frac{y}{2}\right) & \text{falls } x \in 2(3) \text{ und } y \in 0(2), \\ \left(2x, \frac{y-1}{2}\right) & \text{falls } x \in 2(3) \text{ und } y \in 1(2). \end{cases}$$

Die Abbildung σ_T ist affin auf den Restklassen $r(m) \in \mathbb{Z}^2/\langle(6,0),(0,1)\rangle\mathbb{Z}^2$, und σ_T^{-1} ist affin auf den Restklassen $r(m) \in \mathbb{Z}^2/\langle(3,0),(0,2)\rangle\mathbb{Z}^2$.

ANHANG A

Exkurs: Wildheitskriterien

In diesem Exkurs soll die Frage diskutiert werden, woran man erkennt, ob eine gegebene rcwa-Abbildung zahm oder wild ist.

Ein algorithmisch sehr leicht anwendbares ‘Wildheitskriterium’ – namentlich fehlende Ausbalanciertheit – wurde bereits genannt (vgl. Folgerung 2.5.12).

Im folgenden werden zwei weitere derartige Kriterien hergeleitet:

Eine surjektive rcwa-Abbildung ist wild, wenn sie

1. nicht injektiv ist, oder
2. einer ihrer Transitionsgraphen eine schwache Zusammenhangskomponente besitzt, die nicht stark zusammenhängend ist.

Die Beweise stützen sich im wesentlichen auf Aussagen zur Dichte von Bildern und Urbildern offener Mengen unter rcwa-Abbildungen.

Bekanntlich kann man einer Menge $M \subseteq \mathbb{N}$ natürlicher Zahlen stets eine Dichte – die sogenannte *asymptotische* Dichte – zuordnen. Diese setzt man gleich

$$\liminf_{n \to \infty} \underbrace{\frac{|M \cap \{1, 2, \ldots, n\}|}{n}}_{=:\, d_n}.$$

Darüberhinaus bezeichnet man diesen Wert auch als *natürliche* Dichte der Menge M, falls die Folge $(d_n)_{n \in \mathbb{N}}$ konvergiert.

Man sieht leicht, daß für eine beliebige natürliche Zahl k die asymptotische bzw. natürliche Dichte der Menge der k-fachen von Elementen von M gleich dem $\frac{1}{k}$-fachen der asymptotischen bzw. natürlichen Dichte von M selbst ist. Außerdem läßt die Addition einer Konstanten zu den Elementen von M die Dichte offenbar invariant.

Diese Eigenschaften kommen den Bedürfnissen im Hinblick auf rcwa-Abbildungen sehr entgegen. Dies ist die Motivation für die folgende Definition:

A.1 Definition Die Setzungen $\mu(r(m)) := 1/|R/mR|$ für eine Restklasse $r(m) \subseteq R$ sowie $\mu(R \setminus M) := 1 - \mu(M)$ und $\mu(M_1 \cup M_2) := \mu(M_1) + \mu(M_2) - \mu(M_1 \cap M_2)$ für Teilmengen $M, M_1, M_2 \subseteq R$ induzieren einen Dichtebegriff für offene und abgeschlossene Teilmengen von R. Es heiße $\mu(M)$ die *natürliche Dichte* von M.

Der *Modul* $\mathrm{Mod}(M)$ einer offenen oder abgeschlossenen Teilmenge $M \subseteq R$ sei das kleinste $|m|$ so, daß sich M als Vereinigung von Restklassen (mod m) schreiben läßt. Gibt es kein solches m, so sei $\mathrm{Mod}(M) := 0$.

Dieser Dichtebegriff verträgt sich auf naheliegende Weise mit der eingangs angeführten allgemein verwendeten Definition der natürlichen Dichte einer Menge natürlicher Zahlen.

Der Bequemlichkeit halber wird folgende Kurzschreibweise für Urbilder verwendet:

A.2 Konvention Für das volle Urbild eines Elements n bzw. einer Menge M unter einer Abbildung f wird im folgenden auch kurz $n^{f^{-1}}$ bzw. $M^{f^{-1}}$ geschrieben.

Es werden ein paar Grundaussagen zu Dichte und Modul von Bildern und Urbildern offener Mengen unter rcwa-Abbildungen benötigt:

A.3 Lemma *Es sei $M \subseteq R$ offen, $\alpha \in \mathrm{AFF}(K) : n \mapsto (an + b)/c$ und $f \in \mathrm{Rcwa}(R)$. Dann gilt:*

1. $M^\alpha \subseteq R \implies \mu(M^\alpha) = \mu(M) \cdot |R/cR|/|R/aR|$.
2. $\mu(M^f) \leqslant \mu(M) \cdot |R/\mathrm{Div}(f)R|$.
3. $\mathrm{Mod}(M^{f^{-1}}) | \mathrm{Mod}(f) \cdot \mathrm{Mod}(M)$.

Hierbei sei wieder $0|0$.

Beweis: Nach Definition ist die Menge der Restklassen eine Basis der Topologie auf R. Folglich ist die offene Teilmenge M eine Vereinigung von Restklassen.

1. Diese Aussage folgt aus Lemma 1.1.8, Aussage (1), angewandt auf die Elemente einer Partition der Menge M in Restklassen.

2. Diese Aussage folgt aus (1), angewandt auf die affinen Teilabbildungen von f und die Schnitte von M mit den Restklassen (mod $\mathrm{Mod}(f)$). Bilder unter konstanten Teilabbildungen haben die natürliche Dichte 0, fallen also nicht ins Gewicht.

3. Im Fall $\mathrm{Mod}(M) = 0$ ist die Aussage trivial. Es kann also o.E. angenommen werden, daß $\mathrm{Mod}(M) \neq 0$. Es sei $m := \mathrm{Mod}(f)$ und $n \in R$. Ob n^f in M enthalten ist, wird nach Definition bestimmt durch $n^f \bmod \mathrm{Mod}(M)$. Dieser Wert wird bestimmt durch $n \bmod m$ und $n^{f|_{n(m)}} \bmod \mathrm{Mod}(M)$, also durch $n \bmod \mathrm{kgV}(m, \mathrm{Div}(f) \cdot \mathrm{Mod}(M))$. Lemma 1.3.1a, Aussage (1) liefert die Behauptung. □

Es wird ein Begriff für die Summe der Dichte der Bilder der affinen Teilabbildungen einer rcwa-Abbildung benötigt:

A.4 Definition Es sei $f \in \mathrm{Rcwa}(R)$ und $m := \mathrm{Mod}(f)$. Sind die Einschränkungen von f auf die Restklassen $r(m) \in R/mR$ gegeben durch $n \mapsto (a_{r(m)}n + b_{r(m)})/c_{r(m)}$, dann sei die *Bilddichte* $\mu_{\mathrm{img}}(f)$ von f definiert durch

$$\mu_{\mathrm{img}}(f) \;:=\; \sum_{r(m) \in R/mR} \mu(r(m)^f) \overset{\text{falls } \mathrm{Mult}(f) \neq 0}{=} \frac{1}{|R/mR|} \left(\sum_{r(m) \in R/mR} \frac{|R/c_{r(m)}R|}{|R/a_{r(m)}R|} \right).$$

Hierbei wird das rechte Gleichheitszeichen durch Lemma A.3, Aussage (1) gerechtfertigt.

Aus Definition A.4 liest man sofort ab, daß die Bilddichte einer rcwa-Abbildung mit gegebenem Multiplikator und Divisor weder beliebig groß noch beliebig klein sein kann, und daß der Nenner des Bruches ebenfalls beschränkt ist:

A.5 Lemma Für $f \in \mathrm{Rcwa}(R)$ gilt stets $1/|R/\mathrm{Mult}(f)R| \leqslant \mu_{\mathrm{img}}(f) \leqslant |R/\mathrm{Div}(f)R|$ sowie $|R/\mathrm{Mod}(f)R| \cdot |R/\mathrm{Mult}(f)R| \cdot \mu_{\mathrm{img}}(f) \in \mathbb{N}_0$.

Stärkere Aussagen lassen sich treffen, wenn bekannt ist, ob die betreffende Abbildung injektiv, surjektiv oder sogar bijektiv ist:

A.6 Lemma *Es sei $f \in \mathrm{Rcwa}(R)$. Dann gilt:*

1. *f ist injektiv $\Rightarrow \mu_{\mathrm{img}}(f) \leqslant 1$.*
2. *f ist surjektiv $\Rightarrow \mu_{\mathrm{img}}(f) \geqslant 1$.*
3. *f ist bijektiv $\Rightarrow \mu_{\mathrm{img}}(f) = 1$.*

Bei den Ungleichungen in Aussage (1) bzw. (2) ist Gleichheit für Abbildungen f ohne konstante Teilabbildungen genau im Falle der Bijektivität gegeben.

Beweis: Die Behauptungen folgen aus der nach Definition gegebenen Additivität der Dichtefunktion und der Setzung $\mu(R) := 1$. □

Multiplikation mit einer surjektiven, nicht injektiven Abbildung vergrößert die Bilddichte:

A.7 Lemma *Es seien $f, g \in \mathrm{Rcwa}(R)$ surjektive rcwa-Abbildungen ohne konstante Teilabbildungen, und es sei f nicht injektiv. Dann gilt $\mu_{\mathrm{img}}(f \cdot g) > \mu_{\mathrm{img}}(g)$.*

Beweis: Nach Lemma 3.8 gibt es eine Restklasse $r_0(m_0)$ und zwei disjunkte Restklassen $r_1(m_1)$ und $r_2(m_2)$ von R so, daß $r_1(m_1)^f = r_2(m_2)^f = r_0(m_0)$. Setzt man $m_g := \mathrm{Mod}(g)$, dann schneiden sich die Restklassen $r_0(m_g)$ und $r_0(m_0)$ nichttrivial. Es sei $r_0(m)$ deren Schnitt. Aufgrund der Surjektivität von f gilt $\mu_{\mathrm{img}}(f \cdot g) \geqslant \mu_{\mathrm{img}}(g) + \mu(r_0(m)^g) > \mu_{\mathrm{img}}(g)$, was zu zeigen war. □

Jetzt kann die Gültigkeit des erstgenannten Kriteriums gezeigt werden:

A.8 Satz *Ist $f \in \mathrm{Rcwa}(R)$ zwar surjektiv, aber nicht injektiv, so ist f wild.*

Beweis: Angenommen, die Abbildung f sei zahm. Es sei $m := \mathrm{Mod}(\langle f \rangle)$. Dann sind alle Einschränkungen $f^k|_{r(m)}$ $(k \in \mathbb{N})$ von Potenzen von f auf Restklassen (mod m) affin. Wegen Lemma 1.1.8, Aussage (1) sind die Bilder der Restklassen $r(m)$ unter den Potenzen f^k ebenfalls einzelne Restklassen, oder (bedingt durch konstante Teilabbildungen) einelementige Mengen. Es sind zwei Fälle zu unterscheiden:

1. Die Abbildung f besitzt eine konstante Teilabbildung $f|_{r_1(m)} \equiv n$. In diesem Fall gibt es aufgrund der Surjektivität von f und der Wahl von m eine unendliche Folge $r_2(m), r_3(m), r_4(m), \ldots$ paarweise verschiedener Restklassen (mod m) so, daß $\forall k \in \mathbb{N}\ f^k|_{r_k(m)} \equiv n$. Dies steht jedoch im Widerspruch zur Endlichkeit von R/mR.

2. Die Abbildung f besitzt keine konstante Teilabbildung. In diesem Fall folgt aus Lemma A.7, daß $\forall k \in \mathbb{N}\ \ \mu_{\mathrm{img}}(f^{k+1}) > \mu_{\mathrm{img}}(f^k)$. Gemäß Lemma A.5 ist $\mu_{\mathrm{img}}(f^k)$ nach oben durch $|R/\mathrm{Div}(f^k)R|$ beschränkt, aufgrund von Lemma 1.3.1a, Aussage (1) also auch durch $|R/mR|$. Unter Verwendung der 'Nennerschranke' aus Lemma A.5 kann man schließen, daß die Folge $(\mathrm{Mult}(f^k))_{k \in \mathbb{N}}$ nicht beschränkt ist.

   Setzt man $d := |R/mR| + 2$, dann kann man also ein $k_0 \in \mathbb{N}$ und eine Restklasse $r_1(m) \in R/mR$ so wählen, daß $\mu(r_1(m)^{f^{k_0}}) < 1/|R/mR|^d$. Nach Obigem ist $r_1(m)^{f^{k_0}} =: r_0(\tilde{m})$ ebenfalls eine Restklasse, und aus Lemma A.3, Aussage (2) und Lemma 1.3.1a, Aussage (1) folgt, daß $\forall k \in \mathbb{N}\ \ \mu(r_0(\tilde{m})^{f^k}) < 1/|R/mR|^{d-1}$. Mittels folgenden Verfahrens wird nun gezeigt, daß es einen Exponenten $e \in \mathbb{N}$ so gibt, daß für beliebige $k \in \mathbb{N}$ und $r(m) \in R/mR$ stets $\mu(r(m)^{f^{e+k}}) < 1/|R/mR|$ ist:

   1. Setze $i := 2$.
   2. Aufgrund der Surjektivität von f^{k_0} gibt es eine Restklasse $r_i(m) \in R/mR$ so, daß $\mu(r_i(m)^{f^{k_0}} \cap r_{i-1}(m)) \geqslant 1/|R/mR|^2$. Nach Wahl von m sind für $k \in \mathbb{N}_0$ beliebig nun $f^{(i-1)k_0+k}|_{r_i(m)^{f^{k_0}}}$ und $f^{(i-1)k_0+k}|_{r_{i-1}(m)}$ affine Abbildungen, die sich höchstens durch ihren Definitionsbereich unterscheiden. Man kann also unter Verwendung dieser Ungleichung induktiv schließen, daß
   $$\mu(r_i(m)^{f^{ik_0}}) \ \leqslant\ |R/mR|^{i-1} \cdot \mu(r_1(m)^{f^{k_0}}) \ <\ 1/|R/mR|^{d-(i-1)}$$
   sowie $\mu(r_i(m)^{f^{ik_0+k}}) < 1/|R/mR|^{d-i}$. Insbesondere kann für $i \leqslant |R/mR|$ somit kein Bild von $r_i(m)^{f^{ik_0}}$ unter einer Potenz von f mehr mit irgendeiner Restklasse $r_{\tilde{\imath}}(m)$ einen Schnitt mit Dichte $\geqslant 1/|R/mR|^2$ haben $(*)$.
   3. Falls $i < |R/mR|$, setze $i := i + 1$ und fahre fort bei Schritt (2), sonst fertig.

   Wegen $(*)$ sind die $|R/mR|$ Restklassen $r_i(m) \in R/mR$, die man auf die beschriebene Weise erhält, paarweise verschieden. Die genannte Dichteungleichung gilt also für $e := |R/mR| \cdot k_0$. Dies steht im Widerspruch zur Surjektivität von f. □

A.9 Beispiele Drei der vier möglichen Kombinationen von (Nicht-) Injektivität und (Nicht-) Surjektivität lassen keinen Schluß darüber zu, ob die betreffende rcwa-Abbildung zahm oder wild ist – Beispiele über $\mathbb{Z}$:

	zahm	wild
¬injektiv, ¬surjektiv	$f \in \mathrm{Rcwa}(\mathbb{Z})$: $n \mapsto \begin{cases} 2n & \text{falls } n \in 0(2), \\ 2n+2 & \text{falls } n \in 1(2). \end{cases}$	$f \in \mathrm{Rcwa}(\mathbb{Z})$: $n \mapsto \begin{cases} \frac{3n}{2} & \text{falls } n \in 0(2), \\ 2n+2 & \text{falls } n \in 1(2). \end{cases}$
injektiv, ¬surjektiv	$f \in \mathrm{Rcwa}(\mathbb{Z}) : \ n \mapsto 2n.$	$f \in \mathrm{Rcwa}(\mathbb{Z})$: $n \mapsto \begin{cases} \frac{3n}{2} & \text{falls } n \in 0(2), \\ 3n+2 & \text{falls } n \in 1(2). \end{cases}$
¬injektiv, surjektiv	Gibt es nicht, nach Satz A.8.	$T \in \mathrm{Rcwa}(\mathbb{Z})$: $n \mapsto \begin{cases} \frac{n}{2} & \text{falls } n \in 0(2), \\ \frac{3n+1}{2} & \text{falls } n \in 1(2) \end{cases}$ (vgl. Beispiele 1.1.3).
bijektiv	$\nu \in \mathrm{RCWA}(\mathbb{Z}) : \ n \mapsto n+1.$	$\alpha \in \mathrm{RCWA}(\mathbb{Z})$: $n \mapsto \begin{cases} \frac{3n}{2} & \text{falls } n \in 0(2), \\ \frac{3n+1}{4} & \text{falls } n \in 1(4), \\ \frac{3n-1}{4} & \text{falls } n \in 3(4) \end{cases}$ (vgl. Beispiele 1.1.3).

A.10 Lemma *Es sei $f \in \mathrm{Rcwa}(R)$. Gibt es eine Vereinigung endlich vieler Restklassen von R, die echte Teilmenge ihres Bildes sowie echte Obermenge ihres Urbildes unter f ist, dann ist f wild.*

Beweis: Es sei M_0 eine derartige Vereinigung endlich vieler Restklassen, und es sei M_1 das Urbild von M_0 unter f. Nach Satz 2.2.3, Aussage (4) ist die Menge M_1 ebenfalls eine Vereinigung endlich vieler Restklassen, und besitzt folglich echt kleinere natürliche Dichte als M_0. Da das Bild von M_1 unter f eine echte Obermenge von M_1 ist, und Bilder von Elementen außerhalb von M_1 nach Voraussetzung außerhalb von M_0, also insbesondere außerhalb von M_1 liegen, ist das Urbild M_2 von M_1 unter f eine echte Teilmenge von M_1. Diese Argumentation läßt sich iterieren, und liefert eine absteigende

Kette $M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \ldots$ von Vereinigungen endlich vieler Restklassen so, daß stets M_{k+1} das volle Urbild von M_k unter f ist.

Angenommen, f wäre zahm. Es sei $m := \mathrm{Mod}(\langle f \rangle)$. Nach Lemma 1.4.3, Aussage (2) gilt $\forall k \in \mathbb{N}\ \mathrm{Div}(f^k)|m$. Da M_0 das Bild von M_k unter f^k ist, sind die Quotienten $\mu(M_0)/\,\mu(M_k)$ also nach Lemma A.3, Aussage (2) beschränkt durch $|R/mR|$. Es läßt sich nun leicht folgern, daß $\lim_{k\to\infty} \mu(M_k)/\,\mu(M_{k+1}) = 1$, und mithin $\lim_{k\to\infty} \mathrm{Mod}(M_k) = \infty$. Da M_k aber das Urbild von M_0 unter f^k ist, gilt nach Lemma A.3, Aussage (3) aber auch $\forall k \in \mathbb{N}\ \mathrm{Mod}(M_k)|m \cdot \mathrm{Mod}(M_0)$, Widerspruch. □

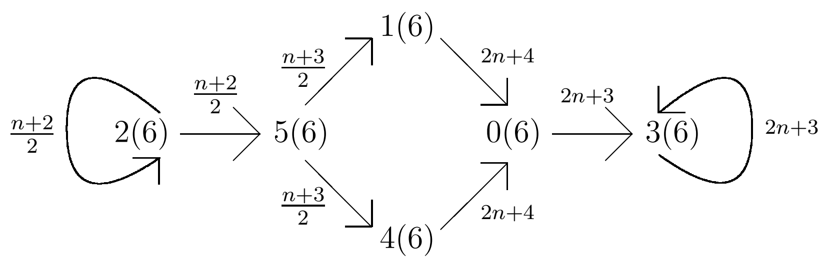
Mithilfe von Lemma A.10 kann jetzt die Gültigkeit des zweiten Kriteriums gezeigt werden:

A.11 Satz *Ist $f \in \mathrm{Rcwa}(R)$ surjektiv und gibt es ein $m \in \mathbb{N}$ so, daß der Transitionsgraph $\Gamma_{f,m}$ von f zum Modul m eine schwache Zusammenhangskomponente besitzt, die nicht stark zusammenhängend ist, so ist f wild.*

Beweis: Nach Voraussetzung läßt sich für geeignetes m eine starke Zusammenhangskomponente Γ_0 von $\Gamma_{f,m}$ wählen, die ein echter Teilgraph einer schwachen Zusammenhangskomponente $\overline{\Gamma}_0$ ist. Da $\overline{\Gamma}_0$ ein endlicher Graph ist, kann man ohne Einschränkung annehmen, daß Γ_0 mit dem Rest von $\overline{\Gamma}_0$ nur durch hinausführende Kanten verbunden ist: Andernfalls könnte man einer hereinführenden Kante in umgekehrter Richtung folgen und gelangte in eine andere starke Zusammenhangskomponente, usw., bis man nach endlich vielen Schritten eine 'Quelle' erreichte, welche der Bedingung genügt.

Es sei $M \subsetneq R$ gleich der Vereinigung der Knoten von Γ_0. Aufgrund der Surjektivität von f ist das Bild von M unter f eine echte Obermenge von M. Weil damit nach Wahl von Γ_0 ferner das Urbild von M unter f eine echte Teilmenge von M ist, kann man mittels Lemma A.10 auf die Wildheit der Abbildung f schließen. □

A.12 Beispiel Es sei α wie in Beispiele 1.1.3, und es sei $\nu : n \mapsto n+1$. Der Transitionsgraph der Abbildung $\nu\nu^\alpha$ zum Modul 6 sieht aus wie folgt:



Dieser Graph ist schwach- aber nicht stark zusammenhängend. Eine starke Zusammenhangskomponente ohne hereingehende Kanten ist $\{2(6)\}$. Die Abbildung $\nu\nu^\alpha$ ist folglich nach Satz A.11 wild.

ANHANG B

Beispiele

In diesem Anhang sollen einige Beispiele für restklassenweise affine Abbildungen und -Gruppen ausführlicher diskutiert werden.

Die Struktur zahmer rcwa-Gruppen hat Satz 2.6.1 bereits geklärt. Die Frage nach der Struktur wilder rcwa-Gruppen hingegen erscheint schwierig. Gleiches gilt für die Frage nach der Gestalt der Bahnen unter ihrer Operation auf dem Grundring. Die folgenden Beispiele sollen dies illustrieren. Zugleich sollen sie aber zeigen, daß auch wilde rcwa-Gruppen rechnerischen Untersuchungen durchaus zugänglich sind.

B.1 Struktur einer wilden rcwa-Gruppe

Es sei α die Collatz'sche Permutation aus Beispiele 1.1.3. Ferner sei β wie in Beispiele 1.8.5, Teil (3) und $\nu : n \mapsto n + 1$. Untersucht werden soll die Gruppe $G := \langle \alpha, \beta, \nu \rangle$.

Es erscheint denkbar, daß die Permutationen α und β eine freie Gruppe vom Rang 2 erzeugen. Die Hinzunahme des Erzeugenden ν liefert hingegen eine Vielzahl von Relationen. Zum Beispiel rechnet man mit RCWA leicht nach, daß $\mathrm{ord}([\alpha\beta, \nu^2]) = 396 = 2^2 \cdot 3^2 \cdot 11$, $\mathrm{ord}([\alpha\beta, \nu^4]) = 182 = 2 \cdot 7 \cdot 13$, $\mathrm{ord}([\alpha\beta, \nu^6]) = 24$, $\mathrm{ord}([\alpha\beta, \nu^{184}]) = \mathrm{ord}([\alpha\beta, \nu^{356}]) = 25$, $\mathrm{ord}([\beta^2, \nu^{17}]) = 5256 = 72 \cdot 73 = 2^3 \cdot 3^2 \cdot 73$, sowie $\mathrm{ord}([\beta^2, \nu^{20}]) = 29$. Exemplarisch sei einer dieser Kommutatoren angegeben – es ist

$$[\alpha\beta, \nu^{356}] \in G : \quad n \longmapsto \begin{cases} 3n - 605 & \text{falls} \ \ n \in 0(9) \cup 7(9), \\ n + 196 & \text{falls} \ \ n \in 1(9) \cup 4(9), \\ 3n - 125 & \text{falls} \ \ n \in 3(9) \cup 6(9), \\ n - 124 & \text{falls} \ \ n \in 2(27) \cup 14(27) \cup 20(27) \cup 23(27), \\ n - 604 & \text{falls} \ \ n \in 5(27), \\ \frac{n+586}{3} & \text{falls} \ \ n \in 8(27) \cup 26(27), \\ \frac{n+106}{3} & \text{falls} \ \ n \in 11(27) \cup 17(27). \end{cases}$$

Rechnerische Untersuchungen legen ferner die folgenden Relationen nahe:

1. Für $k \in \mathbb{Z}$ gilt

$$[\alpha, \nu^k] \text{ wild } \Leftrightarrow \operatorname{ggT}(k, 6) = 1, \text{ sowie}$$

$$\operatorname{ord}([\alpha, \nu^k]) = \begin{cases} 1 & \text{falls } k = 0, \\ 2 & \text{falls } k \in 3(6) \cup \{-2, 2\}, \\ 3 & \text{falls } k \in 4(12) \cup 8(12), \\ \infty & \text{falls } k \in 2(4) \cup 1(6) \cup 5(6) \cup 0(12) \setminus \{-2, 0, 2\}. \end{cases}$$

2. Für $k \in \mathbb{Z}$ gilt

$$\operatorname{ord}([\beta, \nu^k]) = \begin{cases} 1 & \text{falls } k = 0, \\ 3 & \text{falls } k \in 5(15) \cup 10(15), \\ 5 & \text{falls } k \in 3(45) \cup 6(45) \cup 9(45) \cup 18(45) \\ & \qquad \cup 27(45) \cup 36(45) \cup 39(45) \cup 42(45), \\ 6 & \text{falls } k \in \{-2, 2\}, \\ 7 & \text{falls } k \in 13(45) \cup 17(45) \cup 28(45) \cup 32(45), \\ \infty \text{ (zahm)} & \text{falls } k \in (0(15) \cup 2(45) \cup 12(45) \cup 21(45) \\ & \qquad \cup 24(45) \cup 33(45) \cup 43(45)) \setminus \{-2, 0, 2\}, \\ \infty \text{ (wild)} & \text{falls } k \in 1(15) \cup 4(15) \cup 7(15) \\ & \qquad \cup 8(15) \cup 11(15) \cup 14(15). \end{cases}$$

3. Es gilt: $\forall k \in \mathbb{N} \setminus \{2, 4, 6, 12, 24, 184, 356\}$ $\operatorname{ord}([\alpha\beta, \nu^k]) \in \{10, 15, \infty\}$.

4. Für $k \in \mathbb{Z}$ gilt

$$\operatorname{ord}([\alpha^2, \nu^k]) = \begin{cases} 1 & \text{falls } k = 0, \\ 4 & \text{falls } k \in 9(18), \\ 5 & \text{falls } k \in \{-6, 6\}, \\ 7 & \text{falls } k \in 61(144) \cup 83(144), \\ 9 & \text{falls } k \in 16(48) \cup 32(48) \cup 8(144) \cup 136(144), \\ 17 & \text{falls } k \in 134(288) \cup 154(288), \\ 70 & \text{falls } k \in \{-10, 10\}, \\ 90 & \text{falls } k \in \{-14, 14\}, \\ \infty & \text{sonst.} \end{cases}$$

Die sich hier aufdrängende Frage danach, ob die Gruppe G endlich präsentiert ist, bleibt unbeantwortet.

B.2 Zu Automorphismen von RCWA(Z)

Die Abbildungen ν und α aus dem vorigen Abschnitt haben beide unendliche Ordnung. Gibt es einen Automorphismus von $\mathrm{RCWA}(\mathbb{Z})$, der ν auf α abbildet?

Die Abbildung ν ist zahm, α hingegen ist wild. Nach Lemma 1.8.3, Aussage (1) kommt also zumindest kein innerer Automorphismus in Frage. Über Existenz und Gestalt etwaiger äußerer Automorphismen von $\mathrm{RCWA}(\mathbb{Z})$ ist bislang nichts bekannt. Die gestellte Frage kann aber dennoch beantwortet werden:

Es ist $\nu^{n \mapsto -n} = \nu^{-1}$. Die Abbildung ν ist also in $\mathrm{RCWA}(\mathbb{Z})$ zu ihrer Inversen konjugiert. Ferner ist

$$\lim_{k\to\infty} \frac{\mathrm{Mod}(\alpha^k)}{\mathrm{Mod}(\alpha^{-k})} \;=\; \lim_{k\to\infty} \frac{4^k}{3^k} \;=\; \infty.$$

Wegen Lemma 1.3.1c, Aussage (1) sind α und α^{-1} also nicht zueinander konjugiert. Dies impliziert eine negative Antwort auf die gestellte Frage.

B.3 Bahnen unter der Operation einer wilden rcwa-Gruppe

Die Gestalt von Bahnen auf $\mathbb{Z}$ unter der Operation zahmer rcwa-Gruppen wurde durch Folgerung 2.5.17 vollständig aufgeklärt. Aber wie sehen Bahnen unter der Operation wilder rcwa-Gruppen aus?

Offenbar gibt es sowohl endliche als auch unendliche Bahnen unter der Operation derartiger Gruppen. In diesem Abschnitt gilt das Interesse solchen Gruppen, deren Bahnen alle endlich sind.

Auf den Polynomringen $\mathbb{F}_q[x]$ induziert die Gradabbildung eine Partition in endliche Teilmengen, die von wilden rcwa-Abbildungen bzw. -Gruppen festgelassen werden kann (vgl. Beispiele 1.1.3, Teil (3)). Im Gegensatz hierzu ist keineswegs klar, ob es wilde rcwa-Gruppen über $\mathbb{Z}$ gibt, deren Bahnen auf $\mathbb{Z}$ allesamt endlich sind. Hier soll ein Beispiel einer wilden Gruppe $G < \mathrm{RCWA}(\mathbb{Z})$ vorgestellt werden, die diese Eigenschaft anscheinend besitzt. Die Erzeugenden σ_1 und σ_2 von G seien gegeben durch

$$n \;\longmapsto\; \begin{cases} n & \text{falls } \; n \in 0(4), \\ n+1 & \text{falls } \; n \in 1(4) \cup 2(4), \\ n-2 & \text{falls } \; n \in 3(4) \end{cases} \quad \text{bzw.} \quad n \;\longmapsto\; \begin{cases} \frac{3n+3}{2} & \text{falls } \; n \in 1(\;\;6), \\ 2n & \text{falls } \; n \in 3(\;\;9), \\ \frac{n-3}{3} & \text{falls } \; n \in 6(18), \\ n & \text{sonst.} \end{cases}$$

Das Produkt dieser beiden Abbildungen ist wild. Dies sieht man, indem man die Einschränkung der Abbildung $\sigma := \sigma_1\sigma_2$ auf die Restklasse 3(12) betrachtet: Es ist $\sigma|_{3(12)} = \sigma_1|_{3(12)} \cdot \sigma_2|_{3(12)^{\sigma_1}} = \sigma_1|_{3(12)} \cdot \sigma_2|_{1(12)} = (n \mapsto n-2) \cdot (n \mapsto (3n+3)/2) = n \mapsto (3n-3)/2$. Setzt man dementsprechend $\alpha \in \mathrm{AFF}(\mathbb{Q}) : n \mapsto (3n-3)/2$, dann rechnet leicht nach, daß $\forall k \in \mathbb{N}\ \ 3(12) \cap 3(12)^{\alpha^k} = 3(12 \cdot 3^k)$. Folglich ist $12 \cdot 3^k$ eine untere Schranke für den Modul der Abbildung σ^k, und σ mithin wild.

Die Abbildungen σ_1 und σ_2 haben beide die Ordnung 3, und sie besitzen beide Fixpunkte. Daher sind sie als Konsequenz aus Satz 2.6.7 in $\mathrm{RCWA}(\mathbb{Z})$ zueinander konjugiert. Konkret ist $\sigma_1^\theta = \sigma_2$ mit

$$\theta \in \mathrm{RCWA}(\mathbb{Z}): \quad n \longmapsto \begin{cases} \frac{3n-1}{2} & \text{falls } n \in \ \ 1(\ 4), \\ \frac{9n-6}{4} & \text{falls } n \in \ \ 2(\ 4), \\ \frac{9n-15}{2} & \text{falls } n \in \ \ 3(\ 4), \\ \frac{3n+32}{16} & \text{falls } n \in \ \ 0(16), \\ \frac{3n+20}{8} & \text{falls } n \in \ \ 4(16), \\ \frac{9n-72}{16} & \text{falls } n \in \ \ 8(16), \\ \frac{9n+12}{8} & \text{falls } n \in 12(16). \end{cases}$$

Die Gruppe G operiert auf der Menge $\{1, 2, 3, 5, 6, 7, 12, 24\}$ als $\mathrm{E}(8) : \mathrm{F}_{21}$ (GAP -Notation, Ordnung $8 \cdot 21 = 168$) und auf $\{17, 18, 19, 29, 30, 31, 48, 60, 96\}$ als $\mathrm{P\Gamma L}(2, 8)$.

Rechnerische Untersuchungen legen ferner nahe, daß alle Bahnen unter der Operation von G auf $\mathbb{Z}$ endlich sind, und daß G isomorph zum freien Produkt zweier zyklischer Gruppen der Ordnung 3 ist.

Klar ist jedoch noch nicht einmal, daß die Permutation σ nur endliche Zykel besitzt. Um dieser Frage nachzugehen, wird σ im folgenden auf die ‘relevante’ Zusammenhangskomponente des Transitionsgraphen $\Gamma_{\sigma,36}$ eingeschränkt, und es werden im gegebenen Zusammenhang unerhebliche Knoten ‘herausgeschnitten’. Dies liefert eine Permutation, die genau dann nur endliche Zykel besitzt, wenn ebendies für σ gilt. Auf diese Art und Weise kann man zum Beispiel die Abbildung

$$\sigma' \in \mathrm{RCWA}(\mathbb{Z}): \quad n \longmapsto \begin{cases} \frac{3n-3}{2} & \text{falls } n \in \ \ 3(12), \\ \frac{3n+6}{2} & \text{falls } n \in \ \ 6(12), \\ \frac{n+1}{3} & \text{falls } n \in \ \ 5(36), \\ \frac{n-9}{3} & \text{falls } n \in 24(36), \\ 2n & \text{falls } n \in 12(36) \cup 21(36), \\ 2n+2 & \text{falls } n \in \ \ 2(36) \cup 29(36), \\ n+1 & \text{falls } n \in 14(36) \cup 17(36) \cup 26(36), \\ n & \text{sonst.} \end{cases}$$

konstruieren, deren Transitionsgraph zum Modul 36 dargestellt ist in Abbildung B.3.1. Die Zahlen in eckigen Klammern geben die minimale Länge eines Zykels durch den jeweiligen Knoten an. Zykel, die nicht zu einer unendlichen Serie gehören, bleiben hierbei unberücksichtigt.

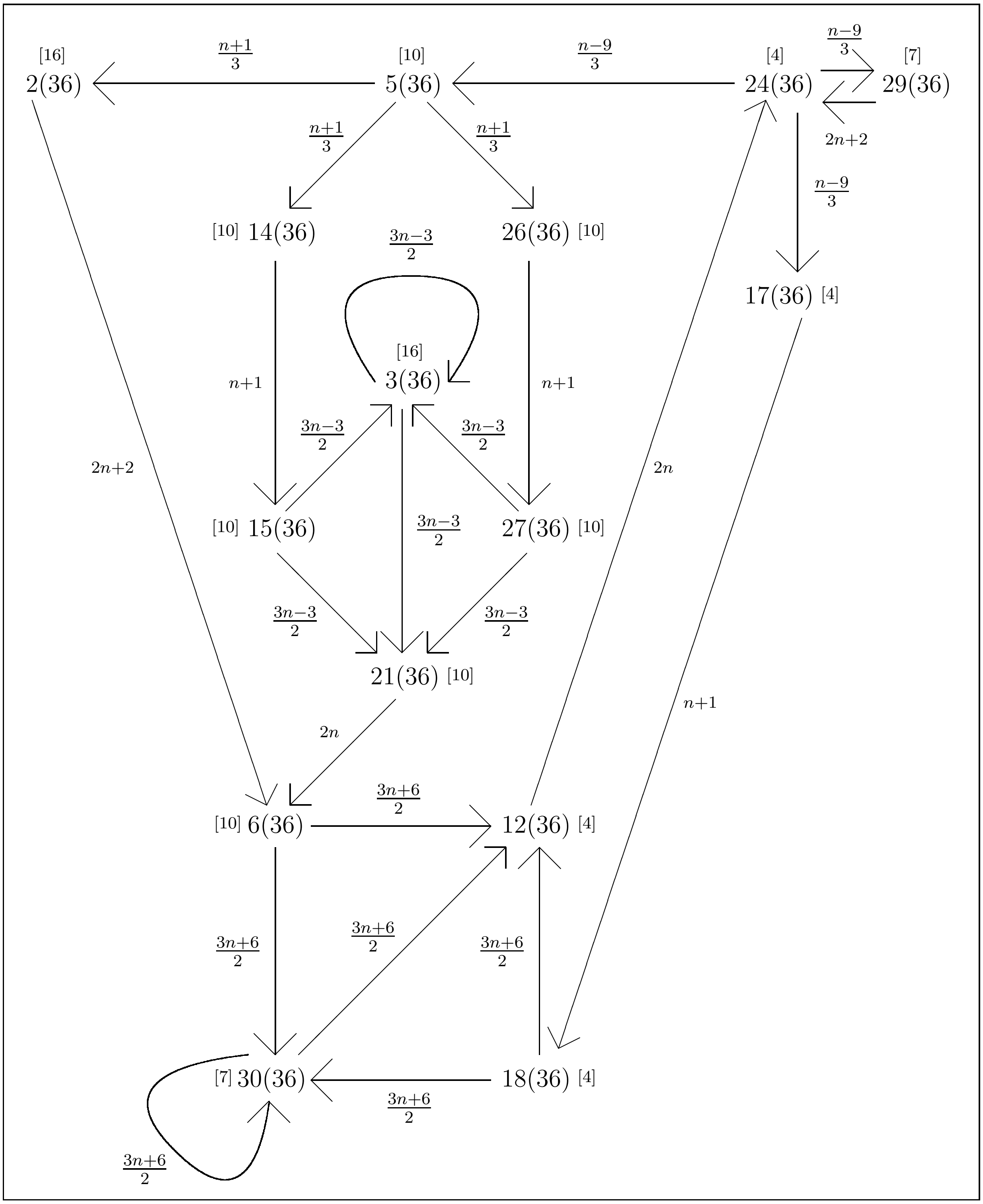


Abbildung B.3.1: Transitionsgraph der Abbildung σ' zum Modul 36.

B.4 Eine wilde rcwa-Abbildung ohne unendliche Zykel

Die Abbildung σ' aus dem letzten Abschnitt ist immer noch relativ kompliziert. Außerdem interessiert im Grunde weniger dieser spezielle Fall, als vielmehr ob es überhaupt wilde rcwa-Abbildungen ohne unendliche Zykel gibt. Deshalb soll im folgenden versucht werden, eine ‘möglichst einfache’ derartige Abbildung zu konstruieren.

Ein Möglichkeit hierzu ist, die Abbildung σ' genauer anzuschauen und zu überlegen, worauf deren besagte Eigenschaft beruhen könnte und auf welche Weise sich gegebenenfalls eine einfachere Abbildung mit den betreffenden Merkmalen ‘zusammenbauen’ ließe. Diese Überlegungen sind zunächst vorwiegend heuristischer Natur. Sie im Detail zu beschreiben wäre ein wenig umständlich. Aus diesem Grunde beschränkt sich der Autor auf die Angabe und Erläuterung des Ergebnisses in Form der Abbildung

$$\kappa := \tau_{2(4),3(4)} \cdot \tau_{3(4),8(12)} \cdot \tau_{4(6),8(12)} : \quad n \longmapsto \begin{cases} \frac{3n+2}{2} & \text{falls } n \in \ \ 2(\ 4), \\ \frac{n+1}{3} & \text{falls } n \in \ \ 8(12), \\ 2n & \text{falls } n \in \ \ 4(12), \\ 2n-2 & \text{falls } n \in 11(12), \\ n-1 & \text{falls } n \in \ \ 3(12) \cup 7(12), \\ n & \text{sonst.} \end{cases}$$

Der Transitionsgraph $\Gamma_{\kappa,12}$ von κ zum Modul 12 sieht aus wie folgt:

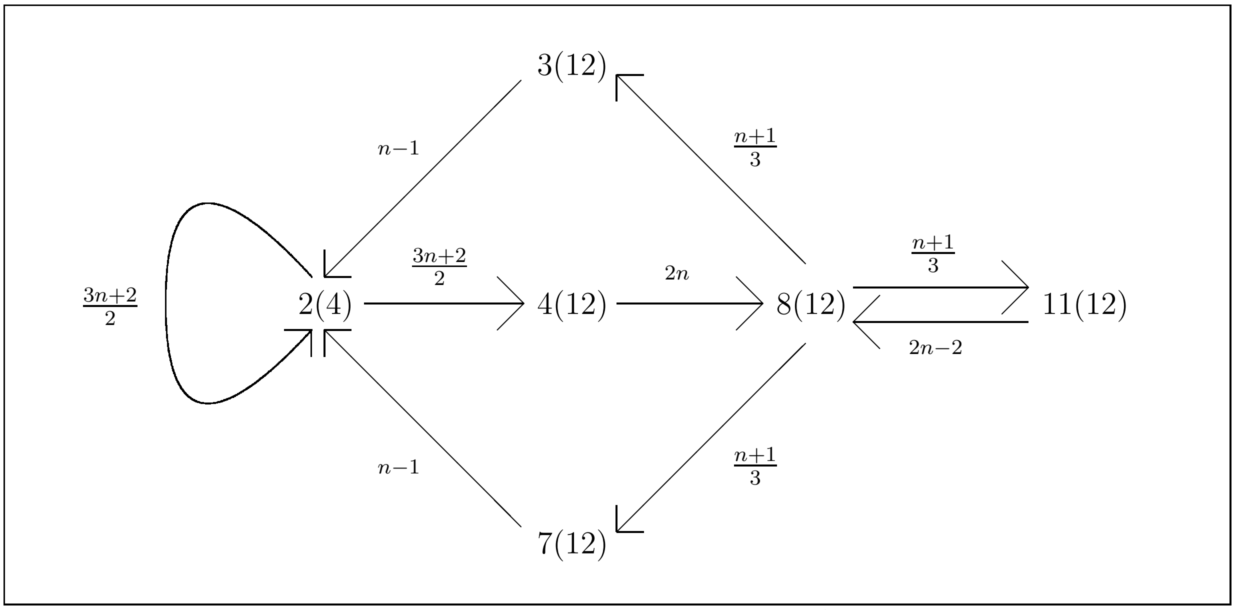


Abbildung B.4.1: Transitionsgraph der Abbildung κ.

Aus Übersichtlichkeitsgründen wurden die drei Knoten 2(12), 6(12) und 10(12) zu einem Knoten 2(4) zusammengefaßt. Zwecks Verdeutlichung der Beziehung zum Transitionsgraphen von σ' aus Abbildung B.3.1 sei die Zuordnung der Knoten der beiden Graphen zueinander angegeben:

- $2(4) \leftrightarrow 6(36) \cup 18(36) \cup 30(36)$
- $3(12) \leftrightarrow 2(36)$
- $4(12) \leftrightarrow 12(36)$
- $7(12) \leftrightarrow 17(36)$
- $8(12) \leftrightarrow 24(36)$
- $11(12) \leftrightarrow 29(36)$
- Alle übrigen Knoten von $\Gamma_{\sigma',36}$ haben sich als verzichtbar erwiesen und wurden daher 'wegoptimiert'.

Aufgrund der Schlinge um 2(4) ist offensichtlich, daß κ wild ist, und die Bijektivität überprüft man – wie immer – durch schlichtes Nachrechnen. Aber warum sind alle Zykel von κ endlich? – Um dieser Frage nachzugehen, definiert man zunächst die affinen Abbildungen $\alpha_{r(m)} := \kappa|_{r(m)}$ für $r(m) \in \{2(4), 3(12), 4(12), 7(12), 8(12), 11(12)\}$, und überzeugt sich davon, daß $\alpha_{2(4)}\alpha_{4(12)}\alpha_{8(12)}\alpha_{7(12)} = 1$ sowie $\alpha_{8(12)}\alpha_{11(12)} = \alpha_{2(4)}{}^{-1}$. Man kann sich nun überlegen, daß κ außer (-1,-4) nur Zykel mit Länge $l \equiv 1$ (3) besitzt, und daß für $k \in \mathbb{N}_0$ die Menge der zu Zykeln der Länge $l = 3k + 1$ gehörigen Zahlen gegeben ist durch

$$\mathcal{C}_k \ := \begin{cases} 1(4) \cup 0(12) \cup \{-2\} & \text{falls } k = 0, \text{ bzw.} \\ \bigcup \left(\left(2(4) \setminus \bigcup\limits_{j=1}^{k-1} \mathcal{C}_j \right) \setminus \bigcup\limits_{j=0}^{k} \left(2(4)^{\kappa^j} \cap 2(4)^{\kappa^{-(k-j)}} \right) \right)^{\langle \kappa \rangle} & \text{falls } k > 0. \end{cases}$$

Ferner kann man sehen, daß die Mengen $\mathcal{C}_k$, $k \in \mathbb{N}_0$ eine Partition von $\mathbb{Z} \setminus \{-4, -1\}$ in nichtleere disjunkte Teilmengen bilden. Hierzu braucht man sich im Grunde nur klarzumachen, daß die Schlinge um 2(4) für kein $n \in 2(4)$ unendlich oft durchlaufen wird, daß es zu jedem $k \in \mathbb{N}$ ein $n \in 2(4)$ so gibt, daß der Zykel von κ, in dem n liegt, den Knoten 2(4) genau k Mal durchläuft (wähle z.B. $n := 2^{k+1} - 2$), und daß ein Durchlauf der Schlinge stets mit genau einem 'Umweg' $8(12) \rightarrow 11(12) \rightarrow 8(12)$ über den Knoten 11(12) 'ausgeglichen' wird (vgl. obige Relationen der affinen Teilabbildungen). Mit Hilfe von RCWA errechnet man

$$\begin{aligned} \mathcal{C}_1 &= 2(24) \cup 3(24) \cup 18(24) \cup 19(24) \cup 4(36) \cup 28(36) \cup 8(72) \cup 56(72), \\ \mathcal{C}_2 &= 6(48) \cup 7(48) \cup 38(48) \cup 39(48) \cup 10(72) \cup 11(72) \cup 58(72) \cup 59(72) \\ &\quad \cup 16(108) \cup 88(108) \cup 20(144) \cup 116(144) \cup 32(216) \cup 176(216), \quad \text{und} \\ \mathcal{C}_3 &= 14(96) \cup 15(96) \cup 78(96) \cup 79(96) \cup 22(144) \cup 23(144) \cup 118(144) \cup 119(144) \\ &\quad \cup 34(216) \cup 35(216) \cup 178(216) \cup 179(216) \cup 44(288) \cup 236(288) \\ &\quad \cup 52(324) \cup 268(324) \cup 68(432) \cup 356(432) \cup 104(648) \cup 536(648). \end{aligned}$$

Die Konstruktion von κ scheint sich nicht noch weiter vereinfachen zu lassen. Man sieht relativ leicht, daß kein Knoten sich einfach fortlassen läßt. Es ist ferner erforderlich, daß der Modul der Abbildung mindestens zwei verschiedene Primteiler besitzt. Die beiden Primteiler braucht man, um einen Knoten zu konstruieren, der sich wie 2(4) im gegebenen Beispiel mit seinem Bild nichttrivial schneidet, aber weder Teil- noch Obermenge desselben ist. Ein derartiger Knoten ist gewissermaßen der Dreh- und Angelpunkt der Konstruktion. Die Wahl von 6 oder 10 als Modul der Abbildung ließe wiederum zu wenig Raum für den Rest der erforderlichen Struktur. Es erübrigt sich zu bemerken, daß dies rein heuristische Betrachtungen sind, die hier lediglich zu Illustrationszwecken ausgeführt werden.

Im folgenden wird eine kleine Zykellängenstatistik für die Permutation κ angegeben. In diese gehen alle Zykel ein, die sich nichttrivial mit dem Intervall $[1, 12^4]$ schneiden:

Zykellänge	Anzahl der Zykel	Zykellänge	Anzahl der Zykel
1	$6912 = 2^8 \cdot 3^3$	25	13
4	$1728 = 2^6 \cdot 3^3$	28	7
7	$864 = 2^5 \cdot 3^3$	31	3
10	$432 = 2^4 \cdot 3^3$	34	2
13	$216 = 2^3 \cdot 3^3$	37	1
16	$108 = 2^2 \cdot 3^3$	40	1
19	$54 = 2^1 \cdot 3^3$	43	0
22	$27 = 2^0 \cdot 3^3$	46	0

B.5 Verketten endlicher Zykel

Die Abbildung κ soll nun ein wenig verändert werden. Konkret soll der Zyklus $8(12) \rightarrow 11(12) \rightarrow 8(12)$ ihres Transitionsgraphen aus Abbildung B.4.1 durch Einfügen einer 'Dreifachgabelung' erweitert werden. Auf diese Weise läßt sich zum Beispiel die Abbildung

$$\tilde{\kappa} \in \mathrm{RCWA}(\mathbb{Z}): \quad n \longmapsto \begin{cases} \frac{3n+2}{2} & \text{falls } n \in 2(4), \\ \frac{n+1}{3} & \text{falls } n \in 8(12), \\ 2n & \text{falls } n \in 4(12), \\ \frac{n+4}{3} & \text{falls } n \in 11(12), \\ 3n+33 & \text{falls } n \in 1(12) \cup 9(12), \\ 3n-39 & \text{falls } n \in 5(12), \\ 2n-4 & \text{falls } n \in 0(12), \\ n-1 & \text{falls } n \in 3(12) \cup 7(12) \end{cases}$$

konstruieren. Der Transitionsgraph $\Gamma_{\tilde{\kappa},12}$ von $\tilde{\kappa}$ zum Modul 12 sieht aus wie folgt:

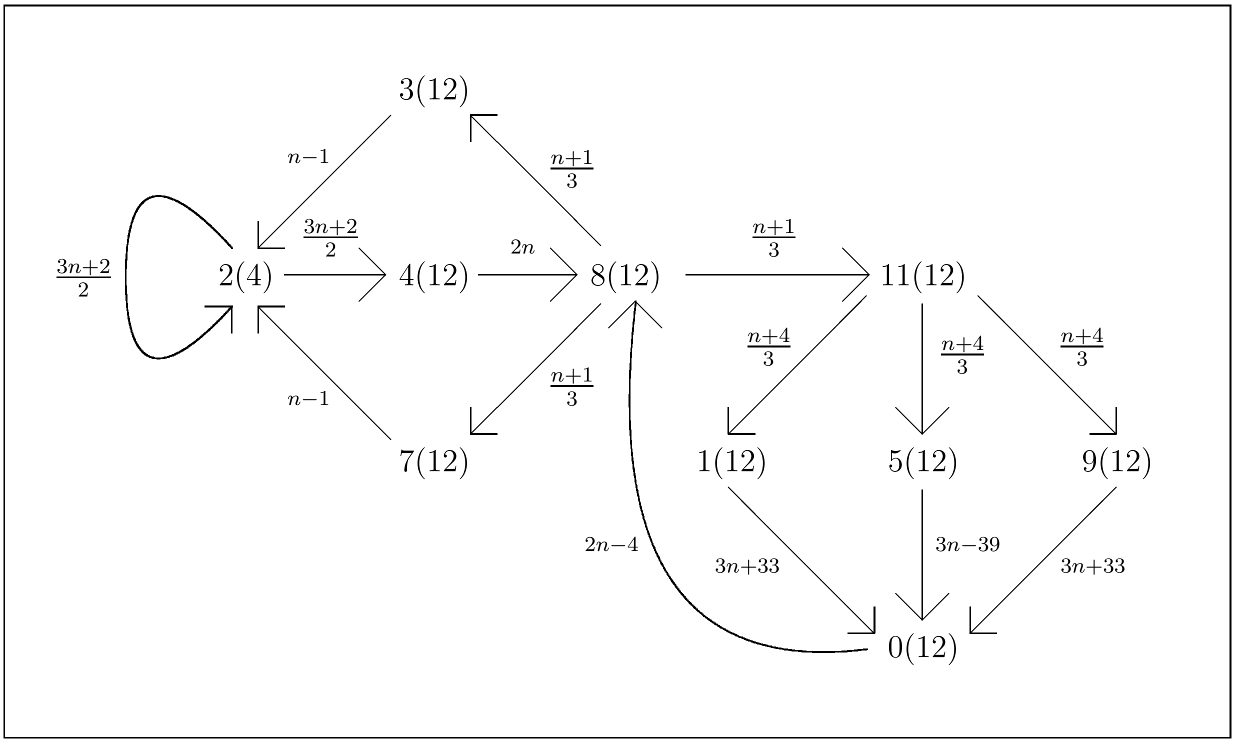


Abbildung B.5.1: Transitionsgraph der Abbildung $\tilde{\kappa}$.

Aus Übersichtlichkeitsgründen wurden wieder geeignete Knoten zusammengefaßt. Man sieht sofort, daß -2 der einzige Fixpunkt von $\tilde{\kappa}$ ist, und mit RCWA rechnet man leicht nach, daß die Menge der zu 4-Zykeln gehörigen Zahlen gegeben ist durch

$$2(24) \cup 3(24) \cup 18(24) \cup 19(24) \cup 4(36) \cup 28(36) \cup 8(72) \cup 56(72) \cup \{25, 71, 108, 212\}$$

$$\subsetneq 2(4) \cup 3(12) \cup 4(12) \cup 7(12) \cup 8(12) \cup \{25, 71, 108, 212\}.$$

Darüberhinaus besitzt $\tilde{\kappa}$ genau dann Zykel einer gegebenen endlichen Länge $l > 4$, wenn $l \equiv 4\ (5)$ und $l \geqslant 74$. Es sind jedoch nicht alle Zykel von $\tilde{\kappa}$ endlich – genauer gesagt, es gibt genau einen unendlichen Zykel. Derselbige durchläuft die Restklassen (mod 12) azyklisch, und die asymptotische Dichte der Menge seiner Elemente ist echt positiv – rechnerische Untersuchungen lassen eine Dichte von $\frac{3}{8}$ erwarten. Demgegenüber besitzt die Menge der zu endlichen Zykeln gehörigen Zahlen anscheinend die Dichte $1 - \frac{3}{8} = \frac{5}{8}$. Stimmen diese Dichteaussagen, so erhält man eine Partition von $\mathbb{Z}$ in die Menge der Fixpunkte (mit Dichte 0), die Menge der zu 4-Zykeln gehörigen Zahlen (mit Dichte $\frac{1}{4}$), die Menge der zu Zykeln der Längen $l \equiv 4\ (5)$ mit $l \geqslant 74$ gehörigen Zahlen (mit Dichte $\frac{3}{8}$) und die Menge der zum unendlichen Zykel gehörigen Zahlen (ebenfalls mit Dichte $\frac{3}{8}$).
Dies soll etwas näher betrachtet werden. Hierzu werden analog zu oben die affinen Abbildungen $\alpha_{r(m)} := \tilde{\kappa}|_{r(m)}$ definiert für

$$r(m) \in \{2(4), 0(12), 1(12), 3(12), 4(12), 5(12), 7(12), 8(12), 9(12), 11(12)\}.$$

Gleiche Abbildungen $\alpha_{r(m)}$ werden hierbei nicht miteinander identifiziert, um die zugehörigen Wege im Transitionsgraphen für den Leser erkennbar zu lassen. Man erhält folgende Gleichungen:

1. $\alpha_{2(4)}\alpha_{4(12)}\alpha_{8(12)}\alpha_{3(12)} = \alpha_{2(4)}\alpha_{4(12)}\alpha_{8(12)}\alpha_{7(12)} = 1.$

2. $\forall k \in \mathbb{N}_0$ $\alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}{\alpha_{2(4)}}^{k+4}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}$ $\alpha_{8(12)}\alpha_{3(12)}{\alpha_{2(4)}}^{2}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}{\alpha_{2(4)}}^{3}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}$ $\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{5(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}{\alpha_{2(4)}}^{2}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{5(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}$ ${\alpha_{2(4)}}^{3}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\left(\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\right)^{k+2}\alpha_{5(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}{\alpha_{2(4)}}^{2}\alpha_{4(12)}$ $\alpha_{8(12)}\alpha_{11(12)}\alpha_{5(12)} = 1.$

3. $\forall k \in \mathbb{N}_0$ $\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}{\alpha_{2(4)}}^{2}\alpha_{4(12)}$ $\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}{\alpha_{2(4)}}^{k+4}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}$ $\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}{\alpha_{2(4)}}^{2}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}{\alpha_{2(4)}}^{3}\alpha_{4(12)}\alpha_{8(12)}$ $\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{5(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}{\alpha_{2(4)}}^{2}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{5(12)}\alpha_{0(12)}$ $\alpha_{8(12)}\alpha_{7(12)}{\alpha_{2(4)}}^{3}\alpha_{4(12)}\left(\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)}\right)^{k}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)} = (n \mapsto n + 324).$

Hierbei liefern die Gleichungen unter Punkt (1) die Zykel der Länge 4, diejenigen unter Punkt (2) die Zykel der Längen $l \equiv 4$ (5) mit $l \geqslant 74$ und diejenigen unter Punkt (3) den unendlichen Zykel. In letzterem Fall wird der der angegebenen Gleichung zugrundeliegende Weg im Graphen hintereinander für jeweils verschiedene k durchlaufen. Beginnt man den 1. Durchlauf bei $n = 0$, dann legen rechnerische Untersuchungen nahe, daß der Wert von k im r. Durchlauf gleich der Bewertung der 2-adischen Zahl $r + \sum_{i=0}^{\infty} 4^i$ ist. In gewissem Sinne kann man sagen, daß der unendliche Zykel eine azyklische Verkettung endlicher Zykel der Längen $l_r \equiv 4$ (5) ist, wobei sich die 'Startwerte' $n \in 0(324)$ jedesmal um 324 verschieben.

B.6 Ein 'erratischer' Zykel, der fast ganz Z überdeckt

Die Konstruktionen aus dem vorigen Abschnitt lassen sich noch weiter ausbauen. Bei Betrachtung der Abbildung κ wurde bemerkt, daß die Schlinge um den Knoten 2(4) und das die Knoten 8(12) und 11(12) verbindende Kantenpaar gewissermaßen als 'Gegenspieler' fungieren. Mit einigem Geschick läßt sich aus drei derartigen Paaren eine Permutation ω zusammensetzen, welche außer den Fixpunkten 4, 6 und 8 sowie den Transpositionen $(-17\ \ -45)$, (13 36) und (17 48) lediglich einen einzelnen Zykel besitzt. Dieser Zykel durchläuft die Restklassen (mod $\mathrm{Mod}(\omega) = 36$) in azyklischer Folge, und umfaßt sämtliche Zahlen $n \in \mathbb{Z} \setminus \{-45, -17, 4, 6, 8, 13, 17, 36, 48\}$. Der Transitionsgraph von ω zum Modul 36 ist dargestellt in Abbildung B.6.1. Aus Übersichtlichkeitsgründen wurden wieder geeignete Knoten zusammengefaßt.

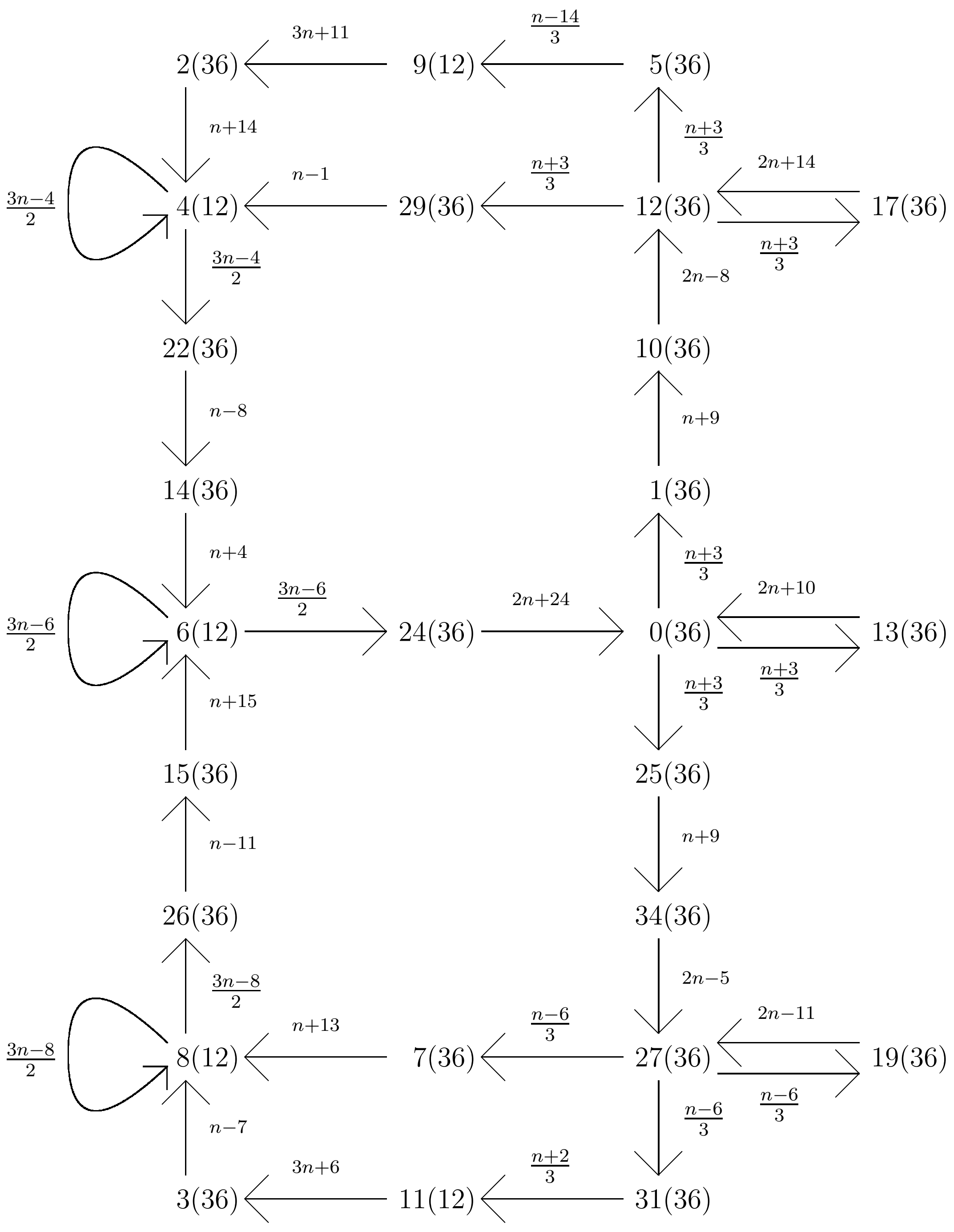


Abbildung B.6.1: Transitionsgraph der Abbildung ω.

Man beachte, daß der Support eines Zykels einer zahmen Abbildung zwar ganz $\mathbb{Z}$ umfassen (Beispiel: $\nu : n \mapsto n + 1$), aber aufgrund von Folgerung 2.5.17 niemals das Komplement einer nichtleeren endlichen Menge sein kann. Ein Ausschnitt des unendlichen Zykels der Permutation ω um 0 ist (… -19 -24 -7 -8 -14 -22 -18 -30 -48 -72 -23 -36 -11 -2 -9 -5 -1 3 -4 -10 -21 -6 -12 0 1 10 12 5 -3 2 16 22 14 18 24 72 25 34 63 19 27 7 20 26 15 …). Der Quotient $\max\{0^{\omega^n} | 0 \leqslant n \leqslant n_{\max}\}/n_{\max}$ ist anscheinend nicht beschränkt. Für $n_{\max} = 10^1, 10^2, \dots, 10^6$ beispielsweise nimmt sein Ganzteil die Werte 2, 10, 32, 81, 430 bzw. 4649 an. Umgekehrt liegen betragsmäßig relativ kleine Zahlen im Zykel 'relativ weit von der 0 entfernt' – es ist etwa $0^{\omega^{133}} = 9$ und $0^{\omega^{11925}} = 249$. Die Permutation ω läßt sich in Elemente des Erzeugendensystems aus Abschnitt 2.9 faktorisieren: Es ist

$$\begin{aligned}
\omega \;=\; & \nu_{3(36)}^{-1} \cdot \nu_{5(36)}^{-1} \cdot \nu_{24(36)} \cdot \nu_{33(36)} \cdot \nu_{35(36)} \\
& \cdot \big((1,5,2,11,7,6,29,26,35,27,16,31,30,28,3,13,17,14,23,15,19,18,25) \\
& \quad (4,33,34,8,21,22,32)(9,10,20)(12,24,36)\big)^{\varphi_{36}} \\
& \cdot \tau_{1(12),0(36)} \cdot \tau_{5(12),12(36)} \cdot \tau_{9(12),27(36)} \cdot \tau_{1(4),4(12)} \cdot \tau_{7(12),2(36)} \cdot \tau_{11(12),3(36)} \\
& \cdot \tau_{4(18),0(36)} \cdot \tau_{6(18),12(36)} \cdot \tau_{8(18),27(36)},
\end{aligned}$$

wobei φ_m die ganzzahlige rcwa-Darstellung der symmetrischen Gruppe S_m aus Satz 2.1.2 bezeichnet. Diese Zerlegung mittels RCWA zu finden ist beträchtlich einfacher als die Faktorisierung der Abbildung α in Beispiel 2.9.9. Der Grund hierfür ist, daß ω ausbalanciert ist. Man liest an der angegebenen Gleichung sofort ab, daß

$$\det(\omega) \;=\; -1 + -1 + 1 + 1 + 1 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 \;=\; 1.$$

B.7 Zum Zusammenhangskomponentenkriterium

In diesem Abschnitt soll ein größeres Beispiel für die Anwendung des 'Wildheitskriteriums' aus Satz A.11 angegeben werden. Es sei σ_1 wie in Abschnitt B.3. Man kann $\tilde{\theta} \in \mathrm{RCWA}(\mathbb{Z})$ so wählen, daß $\sigma_1^{\tilde{\theta}}$ und $\tilde{\sigma} := \sigma_1 \cdot \sigma_1^{\tilde{\theta}}$ gegeben sind durch

$$n \;\mapsto\; \begin{cases} \frac{3n}{2} & \text{falls } n \in 2(\ 4), \\ 2n+1 & \text{falls } n \in 3(\ 6), \\ \frac{n-1}{3} & \text{falls } n \in 7(12), \\ n & \text{sonst} \end{cases} \qquad \text{bzw.} \quad n \;\mapsto\; \begin{cases} n & \text{falls } n \in \ 0(\ 4), \\ \frac{3n+3}{2} & \text{falls } n \in \ 1(\ 4), \\ 2n+3 & \text{falls } n \in \ 2(12), \\ n-2 & \text{falls } n \in \ 3(12) \cup 7(12), \\ \frac{n}{3} & \text{falls } n \in \ 6(12), \\ n+1 & \text{falls } n \in 10(12), \\ 2n-3 & \text{falls } n \in 11(12). \end{cases}$$

Der in Abbildung B.7.1 dargestellte Transitionsgraph $\Gamma_{\tilde{\sigma},12}$ ist schwach-, nicht jedoch stark zusammenhängend.

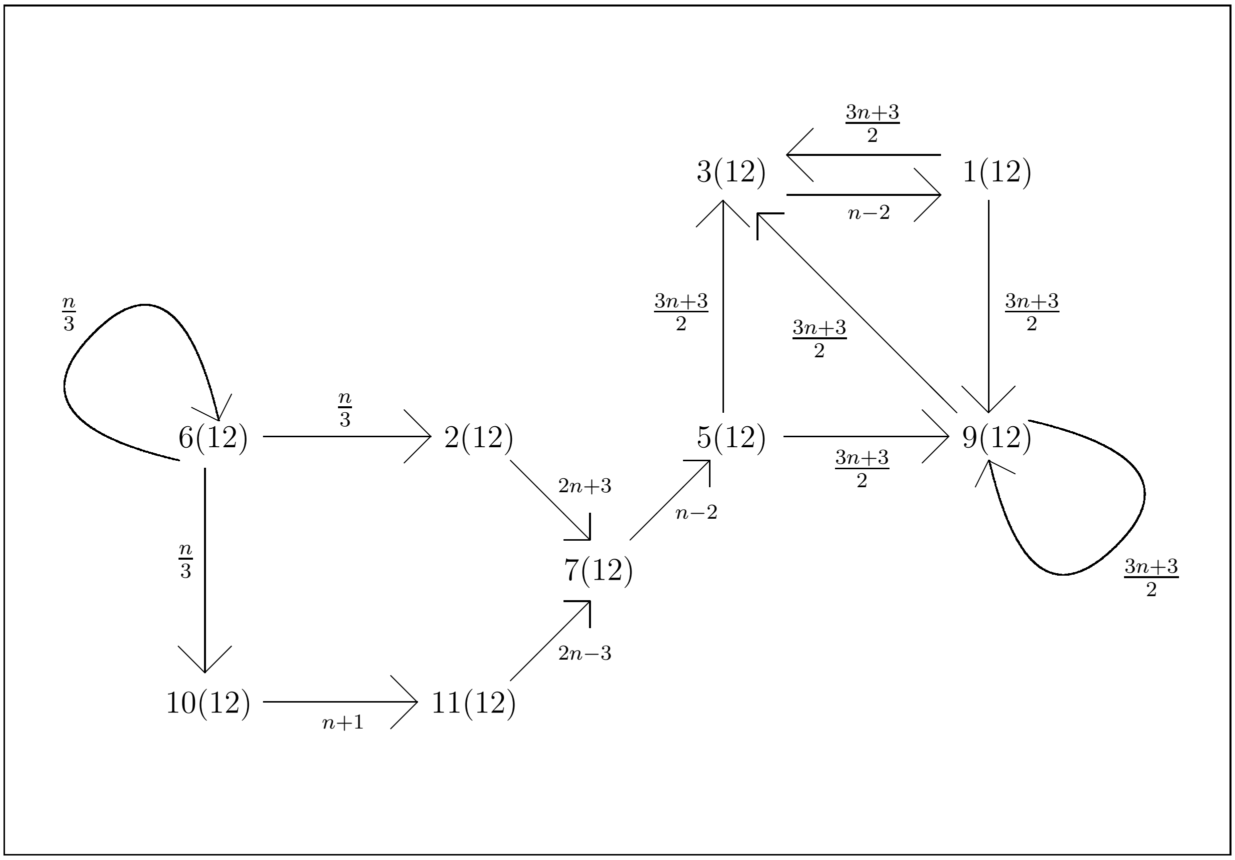


Abbildung B.7.1: Transitionsgraph der Abbildung $\tilde{\sigma}$ zum Modul 12.

Nach Satz A.11 ist die Abbildung $\tilde{\sigma}$ wild. Der Knoten 6(12) besitzt nur herausgehende Kanten. Eine starke Zusammenhangskomponente von $\Gamma_{\tilde{\sigma},12}$, in die ausschließlich Kanten hineingehen, wird von den Knoten 1(12), 3(12) und 9(12) gebildet. Man erkennt sofort, daß jede Trajektorie nach endlich vielen Schritten in diese Zusammenhangskomponente mündet. Ebenfalls leicht zu sehen ist, daß $\tilde{\sigma}$ außer (1 3) keinen nichttrivialen endlichen Zykel besitzt. Ein 'typischer' Zykel von $\tilde{\sigma}$ ist (... 1458 486 162 54 18 6 2 7 5 9 15 13 21 33 51 49 75 73 111 109 165 249 375 ...).

Rechnerische Untersuchungen zu einer größeren Anzahl weiterer Beispiele finden sich im Manual des GAP - Packages RCWA [Koh05].

Symbolverzeichnis

M; $\|M\|$; $\emptyset$	Menge; Kardinalität von M; leere Menge.	Mengen und Abbildungen
$M \cup N$	Vereinigungsmenge von M und N.	
$M \cap N$	Schnittmenge von M und N.	
$M \setminus N$	Differenzmenge von M und N.	
$\cup M$; $\cap M$	Vereinigung / Schnitt der Elemente von M, wobei M eine Menge von Mengen ist.	
id	Identische Abbildung.	
x^f; M^f	Bild des Elementes x / der Menge M unter der Abbildung f.	
$x^{f^{-1}}$; $M^{f^{-1}}$	Urbild des Elementes x / der Menge M unter der Abbildung f.	
$f \cdot g$, fg	Kompositum der Abbildungen f und g; die Abbildung f wird zuerst angewandt.	
$f\|_M$	Einschränkung der Abbildung f auf die Menge M.	
$\operatorname{im} f$	Bild der Abbildung f.	
$\ker \varphi$	Kern des Homomorphismus' φ.	

$\mathbb{N}$	Menge der natürlichen Zahlen (ohne Null).	Ringe und Körper
$\mathbb{N}_0$	Menge der natürlichen Zahlen (einschließlich Null).	
$\mathbb{Z}$	Ring der ganzen Zahlen.	
$\mathbb{Z}_{(p)}, \mathbb{Z}_{(\pi)}$	(Semi-)lokalisierung von $\mathbb{Z}$ an p bzw. π.	
$\mathbb{Q}$	Körper der rationalen Zahlen.	
$\mathbb{F}_q$	Körper mit q Elementen.	
$\mathbb{F}_q[x]$	Polynomring in einer Variablen über $\mathbb{F}_q$.	
R	Euklidischer Ring, dessen Restklassenringe endlich sind.	
K	Quotientenkörper des Rings R.	
$\operatorname{char}(R)$, $\operatorname{char}(K)$	Charakteristik des Rings R / Körpers K.	
$R^\times$	Einheitengruppe des Rings R.	
$\operatorname{Aff}(R)$	Monoid der affinen Abbildungen des Rings R.	
$\operatorname{AFF}(R)$	Gruppe der bijektiven affinen Abbildungen des Rings R.	

	AFF(K)	Affine Gruppe des Körpers K.
	$r(m)$	Restklasse r (mod m).
	$\mathfrak{R}(m)$	Repräsentantensystem für die Restklassen (mod m); es sei stets (r mod m) $\in \mathfrak{R}(m)$.
	$\mathbb{P}(R)$	Menge der Primelemente des Rings R.
	p, q	Primzahl(-potenz), soweit nicht anders angegeben.
	$a\|b$	'a teilt b'.
	$p^k\|\|n$	$p^k\|n$, aber $p^{k+1} \nmid n$.
	ggT	Größter gemeinsamer Teiler.
	kgV	Kleinstes gemeinsames Vielfaches.
	$\det(A)$	Determinante der Matrix A.
	$\exp(z)$	Funktion exp: $\mathbb{C} \to \mathbb{C}$, $z \mapsto e^{2\pi i z}$.
Gruppen, Notation allgemein	G	Gruppe, soweit nicht anders angegeben.
	$\langle g_1, \ldots, g_n \rangle$	Von $g_1, \ldots, g_n$ erzeugte Gruppe bzw. Monoid.
	$\|G\|$	Gruppenordnung von G.
	$\mathrm{ord}(g)$	Ordnung des Gruppenelements g.
	$\exp(G)$	Exponent der Gruppe G (= kgV der Ordnungen der Elemente).
	$[g, h]$	Kommutator von g und h; $[g, h] = g^{-1}h^{-1}gh$.
	$\mathrm{Z}(G)$	Zentrum von G.
	$\mathrm{C}_G(H)$	Zentralisator von H in G.
	$\mathrm{N}_G(H)$	Normalisator von H in G.
	$\mathrm{Aut}(G)$	Automorphismengruppe von G.
	$H \trianglelefteq G$	'H ist Normalteiler von G'.
	$\|G : H\|$	Index von H in G.
	$G \times H$	Direktes Produkt der Gruppen G und H.
	$G \rtimes H$	Semidirektes Produkt der Gruppen G und H (G ist normal).
	$G \wr P$	Kranzprodukt der Gruppe G mit der Permutationsgruppe P.
	G_x	Stabilisator des Punktes x unter der Operation von G.
	$G_{(M)}$	Punktweiser Stabilisator von M unter der Operation von G.
	$G_{\{M\}}$	Mengenweiser Stabilisator von M unter der Operation von G.
	x^G, M^G	Bahn des Punktes x / der Menge von Punkten M unter der Operation von G.
	$\mathrm{supp}(g)$	Support der Permutation g.
	$\mathrm{supp}(G)$	Support der Permutationsgruppe G.
Serien von Gruppen	C_n	Zyklische Gruppe der Ordnung n.
	D_n	Diedergruppe vom Grad n (der Ordnung $2n$).
	$\mathrm{S}_n/\mathrm{Sym}(M)$	Symmetrische Gruppe vom Grad n / auf der Menge M.
	A_n	Alternierende Gruppe vom Grad n.

$\mathrm{GL}(n,q)$	Allgemeine lineare Gruppe vom Grad n über $\mathbb{F}_q$.
$\mathrm{SL}(n,q)$	Spezielle lineare Gruppe vom Grad n über $\mathbb{F}_q$.
$\mathrm{PSL}(n,q)$	Projektive spezielle lineare Gruppe vom Grad n über $\mathbb{F}_q$.
$\Gamma\mathrm{L}(n,q)$	Allgemeine semilineare Gruppe vom Grad n über $\mathbb{F}_q$.
$\mathrm{P}\Gamma\mathrm{L}(n,q)$	Projektive semilineare Gruppe vom Grad n über $\mathbb{F}_q$.

Restklassenweise affine Abbildungen, Gruppen und Monoide

$\mathrm{Rcwa}(R)$	Monoid aller restklassenweise affinen (*rcwa-*) Abbildungen des Rings R (→ Definition 1.3.3).
$\mathrm{RCWA}(R)$	Gruppe aller bijektiven rcwa-Abbildungen des Rings R (→ Definition 1.3.3).
$\mathrm{RCWA}^+(R)$	Gruppe aller klassenweise ordnungserhaltenden bijektiven rcwa-Abbildungen des (angeordneten) Rings R (→ Definition 1.7.1).
$\mathrm{Mod}(f)$	Modul der rcwa-Abbildung f (→ Definition 1.1.2).
$\mathrm{Mod}(G)$	Modul des rcwa-Monoids / der rcwa-Gruppe G (→ Definition 1.4.2).
$\mathrm{Mult}(f)$	Multiplikator der rcwa-Abbildung f (→ Definition 1.1.2).
$\mathrm{Mult}(G)$	Multiplikator des rcwa-Monoids / der rcwa-Gruppe G (→ Definition 1.4.2).
$\mathrm{Div}(f)$	Divisor der rcwa-Abbildung f (→ Definition 1.1.2).
$\mathrm{Div}(G)$	Divisor des rcwa-Monoids / der rcwa-Gruppe G (→ Definition 1.4.2).
$\mathcal{P}(f)$	Zur rcwa-Abbildung f gehörige Primteilermenge (→ Definition 1.1.2).
$\mathcal{P}(G)$	Zum rcwa-Monoid / zur rcwa-Gruppe G gehörige Primteilermenge (→ Definition 1.4.2).
$a_{r(m)}, b_{r(m)}, c_{r(m)}$	Koeffizienten einer rcwa-Abbildung auf der Restklasse $r(m)$ (→ Definition 1.1.2).
$\Gamma_{f,m}$	Transitionsgraph der rcwa-Abbildung f zum Modul m (→ Definition 1.6.1).
$\mu(M)$	Natürliche Dichte von $M \subseteq R$ (→ Definition A.1).
$\mu_{\mathrm{img}}(f)$	Bilddichte der rcwa-Abbildung f (→ Definition A.4).
π_f	Zur rcwa-Abbildung f assoziierter Einschränkungsmonomorphismus (→ Definition 2.3.1).

$\mathcal{P}$	Partition des Rings R in endlich viele Restklassen, soweit nicht anders angegeben.
$\sigma_{\mathcal{P}}$	Von der zahmen rcwa-Abbildung σ auf der respektierten Partition $\mathcal{P}$ induzierte Permutation (→ Definition 2.5.2).
$G_{\mathcal{P}}$	Von der zahmen rcwa-Gruppe G auf der respektierten Partition $\mathcal{P}$ induzierte Permutationsgruppe (→ Definition 2.5.2).
$\mathrm{Sym}(\mathcal{P})$	Zahme rcwa-Gruppe, die die Partition $\mathcal{P}$ respektiert und auf ihr als volle symmetrische Gruppe operiert (→ Definition 2.5.2).
$\det(\sigma)$	Determinante der rcwa-Abbildung $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ (→ Definition 2.11.1).
$[r/m]$	Restklasse $r(m)$ mit fixiertem Repräsentanten r (→ Definition 2.11.3), in Abschnitt 2.12 zusätzlich mit vorzeichenbehaftetem Modul (→ Definition 2.12.3).
$\delta\,([r/m])$	Abbildung $\delta:\ [r/m] \mapsto r/m - 1/2$ (→ Definition 2.11.4).
$\mathrm{sgn}(f)$	Signatur der rcwa-Abbildung f (→ Definition 2.12.1).
$\varrho\,(r(m))$	Abbildung $\varrho:\ [r/m] \mapsto e^{\pm\,\delta([r/m])/2}$ (→ Definition 2.12.4).
$\nu_{r(m)}$, $\varsigma_{r(m)}$, $\tau_{r_1(m_1),r_2(m_2)}$	Klassenshift, Klassenspiegelung, Klassentransposition (→ Definition 2.9.1).
ν, ς, τ	Abbildung $\nu : n \mapsto n+1$, $\varsigma : n \mapsto -n$ bzw. $\tau : n \mapsto n + (-1)^n$ (→ Definition 2.9.1).

Literaturverzeichnis

[BMMN98] 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.

[DM96] John D. Dixon and Brian Mortimer. *Permutation Groups*. Number 163 in Graduate Texts in Mathematics. Springer-Verlag, 1996.

[ET36] Paul Erdös and Paul Turan. On some sequences of integers. *J. London Math. Soc.*, 11:261–264, 1936.

[Für55] Harry Fürstenberg. On the infinitude of primes. *Amer. Math. Monthly*, 62:353, 1955.

[GAP04] The GAP Group. *GAP – Groups, Algorithms, and Programming; Version 4.4*, 2004. (http://www.gap-system.org).

[GT04] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions, 2004. (http://arxiv.org/abs/math.NT/0404188v1).

[Koh05] Stefan Kohl. *RCWA - Residue Class-Wise Affine Groups*, 2005. GAP package (http://www.gap-system.org/Packages/rcwa.html).

[Lag85] Jeffrey C. Lagarias. The 3x+1 problem and its generalizations. *Amer. Math. Monthly*, 92:1–23, 1985.

[Lag05] Jeffrey C. Lagarias. The 3x+1 problem: An annotated bibliography, 2005. (http://arxiv.org/abs/math.NT/0309224).

[Rob96] Derek J. S. Robinson. *A Course in the Theory of Groups*. Number 80 in Graduate Texts in Mathematics. Springer-Verlag, 1996.

[Wir96] Günther J. Wirsching. The dynamical system on the natural numbers generated by the 3n+1 function. Habilitationsschrift, Katholische Universität Eichstätt, 1996.

[Wir98] Günther J. Wirsching. *The Dynamical System Generated by the 3n+1 Function*. Number 1681 in Lecture Notes in Mathematics. Springer-Verlag, 1998.

[Wir03] Günther J. Wirsching. On the problem of positive predecessor density in 3n+1 dynamics. *Disc. and Cont. Dyn. Syst.*, 9(3):771–787, 2003.