Stefan Kohl

Residue Class-Wise Affine Groups

English Translation of the Author's Thesis

Restklassenweise affine Gruppen

This thesis is published in original in German at the following sites:

- 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`

The numbers of theorems and pages in the english translation are the same as in the original version. Thus if you cite e.g. Theorem 2.12.8 or refer to page 64, it makes no difference whether you use the original or the translation. Exception: The german summary (pages with roman numbers xi-xiv) is not present in the english translation. This does not affect the other page numbers.

This copy has been made on 27/01/06.

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

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

Contents

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 RCWA($\mathbb{Z}$) of all residue class-wise affine bijections of the ring of integers.

Results

It is shown that the group 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 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 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 $n \equiv 2 \bmod 3$, 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

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

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.

Acknowledgements

I thank my thesis advisor Prof. Dr. Wolfgang Kimmerle for giving me room for my work on the subject which I have chosen myself.

A valuable contribution to the proof of Theorem 2.11.9 has been made by Prof. Dr. Wolfgang Rump, who has also provided various useful hints and has always argued that residue class-wise affine groups are a promising field of research. For all of this I would like to express my sincerest gratitude.

In the same way I would like to thank Prof. Dr. Bettina Eick for giving me valuable advice in many instances, for suggesting various improvements to the documentation of my GAP package RCWA, which I have developed in parallel with writing this thesis, and – *last but not least* – for all of her words of encouragement and motivation.

Further I would like to thank the persons mentioned before as well as various colleagues in particular from the GAP Group for many interesting discussions.

I would like to thank the *Institut für Geometrie und Topologie* for providing me with an office for my own and for a good working atmosphere.

For financial support I would like to thank the *Centre for Interdisciplinary Research in Computational Algebra* in St Andrews and the *Lehrstuhl D für Mathematik* of the *RWTH Aachen*.

My special thanks go to my parents who provided the needed financial means during all the time I worked on writing this thesis.

CHAPTER 1

Introduction

1.1 Basic Definitions

In the following, we define a class of mappings of rings to themselves.

The set of these mappings of a given ring with countably many elements is countable, and is accessible to computational investigations.

First of all, we need to specify which rings we intend to consider:

1.1.1 Definition In this thesis, let R always denote an infinite euclidean ring which has at least one prime ideal and all of whose proper residue class rings are finite.

Further we assume that a mapping $|.| : R \to R$ is given which maps each element of R to some 'standard associate'. In case $R = \mathbb{Z}$, let this be the absolute value. Greatest common divisors and least common multiples are always normed via $|.|$.

Now we can define our mappings:

1.1.2 Definition 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 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 $c_{r(m)} = |c_{r(m)}|$.

Further we define the

- *Multiplier* $\mathrm{Mult}(f)$ of f by $\operatorname{lcm}_{r(m)\in R/mR} a_{r(m)}$, the
- *Divisor* $\mathrm{Div}(f)$ of f by $\operatorname{lcm}_{r(m)\in R/mR} c_{r(m)}$, and the
- *Prime Set* $\mathcal{P}(f)$ of f by the set of prime divisors of $\mathrm{Mod}(f)\cdot\mathrm{Mult}(f)\cdot\mathrm{Div}(f)$.

1.1.3 Examples In the following, some examples of rcwa mappings are given:

1. In a certain sense the Collatz mapping T which has already been mentioned in the Summary is something like the 'prototype' of an rcwa mapping.

   It is $\mathrm{Mod}(T) = \mathrm{Div}(T) = 2$, $\mathrm{Mult}(T) = 3$ and $\mathcal{P}(T) = \{2, 3\}$. The mapping T is surjective, but not injective – given $n \equiv 2\ (3)$ we have $T^{-1}(n) = \{(2n-1)/3, 2n\}$.

2. An example of a bijective rcwa mapping which has already been considered by Lothar Collatz as well is

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

   The permutation α maps the residue class 0(2) bijectively to 0(3), the residue class 1(4) bijectively to 1(3) and the residue class 3(4) bijectively to 2(3). It is $\mathrm{Mod}(\alpha) = \mathrm{Div}(\alpha) = 4$, $\mathrm{Mult}(\alpha) = 3$ and $\mathcal{P}(\alpha) = \{2, 3\}$. Further it is $\forall n \in \mathbb{Z}\ (-n)^\alpha = -(n^\alpha)$, or in different words, the mapping α centralizes the involution $\varsigma : n \mapsto -n$. The only fixed points of α are -1, 0 and 1. It seems likely that the only finite cycles of the permutation α are the transpositions $\pm$(2 3), the 5-cycles $\pm$(4 6 9 7 5) and the 12-cycles $\pm$(44 66 99 74 111 83 62 93 70 105 79 59).

3. The permutation

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

   fixes the degree of any polynomial. Therefore it has only finite cycles. However it is easy to show that ξ has infinite order, thus that there is no upper bound on the cycle lengths. We have $\mathrm{Mod}(\xi) = \mathrm{Div}(\xi) = x^2+1$, $\mathrm{Mult}(\xi) = x^2+x+1$ and $\mathcal{P}(\xi) = \{x+1, x^2+x+1\}$.

1.1.4 Definition We will repeatedly use the following notation:

1. By definition, R is an euclidean ring. As is well known, this implies that R is in particular a principal ideal domain and a unique factorization domain. We denote the set of prime elements of R by $\mathbb{P}(R)$.

2. We consider residue classes $r(m) \in R/mR$ from a set-theoretic point of view, and write for $n \equiv r \bmod m$ apart from the common shorthand $n \equiv r\ (m)$ also $n \in r(m)$.

3. Let $\mathfrak{R}(m)$ denote a set of representatives for the residue classes (mod m). In case $R = \mathbb{Z}$, let $\mathfrak{R}(m) := \{0, 1..m-1\}$.

4. We denote the quotient field of R by K.

For many purposes, it is convenient to introduce a partial order on R:

1.1.5 Definition We say that an element $n_1 \in R$ is *greater* (resp. *smaller*) than another element $n_2 \in R$, if $|R/n_1R|$ is greater (resp. smaller) than $|R/n_2R|$.

We say that a subset $S \subset R$ is *bounded* if there is a constant $c \in \mathbb{N}$ such that $\forall n \in S \ \ |R/nR| < c$.

Let $(n_k) \subset R$ be a sequence of elements of R such that $\lim_{k\to\infty} |R/n_kR| = \infty$. Then we use the abbreviated notation $\lim_{k\to\infty} n_k = \infty$.

It is easy to see that these definitions are in line with the usual definitions of '$<$', 'bounded' etc. for $R = \mathbb{Z}$.

We fix the mapping $|.|$ for the rings $R \neq \mathbb{Z}$ which are used in this thesis explicitly:

1.1.6 Definition Given $n \in \mathbb{Z}_{(\pi)}$, let $|n|$ be the greatest product of primes $p \in \pi$ which divides n. Given $P \in \mathbb{F}_q[x]$, let $|P|$ be the quotient of the polynomial P by its leading coefficient.

Obviously we need the affine groups of R and K:

1.1.7 Definition We denote the monoid of affine mappings of R by $\mathrm{Aff}(R)$, and the group of bijective affine mappings (the *affine group*) of R by $\mathrm{AFF}(R)$. The elements of $\mathrm{AFF}(R)$ are the mappings $n \mapsto un + k$, $u \in R^\times$, $k \in R$. Analogously, we denote the affine group of K by $\mathrm{AFF}(K)$. Where there is no risk of a misunderstanding, we identify affine mappings of R resp. K with their restrictions to residue classes of R. Further we speak of them as *affine partial mappings* of rcwa mappings.

We will frequently need the following lemma about affine mappings of K:

1.1.8 Lemma *Let $\alpha \in \mathrm{AFF}(K) : n \mapsto (an+b)/c,\ a,b,c \in R,\ \gcd(a,b,c) = 1$. Further let $r, m \in R$. Then the following hold:*

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

Proof:

1. For $t \in R$ we have
$$(r+tm)^\alpha \ = \ \frac{a(r+tm)+b}{c} \ = \ \frac{ar+b}{c} + \frac{atm}{c} \ = \ r^\alpha + t \cdot \frac{am}{c}.$$
This immediately implies our assertion.
2. The mapping α^k, $k \in \mathbb{N}$ is given by $n \mapsto (a^k n + \tilde{b}_k)/c^k$ for a certain $\tilde{b}_k$, hence certainly not the identity, if a or c is not a unit. The condition $r(m)^\alpha \subseteq R$ implies $am/c \in R$. Hence by Assertion (1), α^k maps the residue class $r(m)$ onto $r^{\alpha^k}(a^k m/c^k)$. The latter residue class can only be equal to $r(m)$ if a and c are units.
3. The condition $\alpha \in \mathrm{AFF}(R)$ implies that a and c are units. Hence by Assertion (1), the mapping α maps $r(m)$ to $r^\alpha(m)$. Obviously, two residue classes (mod m) are either disjoint or equal. □

A class of subsets of the ring R which is important in the context of this thesis is the class of unions of finitely many residue classes. The *Chinese Remainder Theorem* and the demanded finiteness of all proper residue class rings of R imply the following lemma:

1.1.9 Lemma The class of (set theoretic) unions of finitely many residue classes of R is closed under forming unions, intersections and differences.

Given a partition of R into residue classes, there is a corresponding partition of 1 into fractions of the form $1/n$:

1.1.10 Lemma Let $\mathcal{P} = \{r_1(m_1), \ldots, r_l(m_l)\}$ be a partition of R into finitely many residue classes. Then $1 = 1/|R/m_1R| + \cdots + 1/|R/m_lR|$ is a partition of 1 into fractions of the form $1/n$.

We take the opportunity to remind that a *partition* of a set into subsets is – in contrast to a *covering* – always a decomposition into *disjoint* subsets.

1.2 Images and Preimages Under rcwa Mappings

How do images of rcwa mappings look like, and what can be said about images and preimages of 'suitable' subsets of R under rcwa mappings? – These questions are answered by the following lemma:

1.2.1 Lemma *The following hold:*

1. *The image of an rcwa mapping is always a union of finitely many residue classes of R and a finite subset of R.*

2. *Assume that $f \in \mathrm{Rcwa}(R)$ is not constant on any residue class, and that $S \subseteq R$ is a union of finitely many residue classes. Then image and preimage of S under f are unions of finitely many residue classes as well.*

Proof:

1. Let $f \in \mathrm{Rcwa}(R)$, and set $m := \mathrm{Mod}(f)$. Assume that the restriction of f to a residue class $r(m) \in R/mR$ is given by $n \mapsto (a_{r(m)}n + b_{r(m)})/c_{r(m)}$. In case $a_{r(m)} = 0$ we have $r(m)^f = \{b_{r(m)}\}$, and in case $a_{r(m)} \neq 0$ Lemma 1.1.8, Assertion (1) tells us that
$$r(m)^f \quad = \quad \frac{a_{r(m)} \cdot r + b_{r(m)}}{c_{r(m)}} \quad \left(\frac{a_{r(m)} \cdot m}{c_{r(m)}} \right).$$
We get the claimed assertion, since the image of f equals the union of the images of all residue classes (mod m) under f, and since there are only finitely many of the latter.

2. It is sufficient to prove the assertion for the case that S is a single residue class. Let $m := \mathrm{Mod}(f)$. The intersection $S_{r(m)}$ of S with a residue class $r(m)$ is either empty or a residue class. By Lemma 1.1.8, Assertion (1) the same holds for the image of $S_{r(m)}$ under the restriction of f to $r(m)$.

   Let $\tilde{m} := \mathrm{Mult}(f) \cdot m$. The intersection $\tilde{S}_{\tilde{r}(\tilde{m})}$ of S with a residue class $\tilde{r}(\tilde{m})$ is either empty or a residue class as well. By Lemma 1.1.8, Assertion (1), the mapping f maps any residue class (mod m) onto a union of residue classes (mod $\tilde{m}$). Hence the preimage of the set $\tilde{S}_{\tilde{r}(\tilde{m})}$ under f equals the union of its preimages under zero, one or several affine partial mappings of f, thus is either empty or a union of finitely many residue classes.

   We get the assertion since R/mR and $R/\tilde{m}R$ are finite and since the image (preimage) of S under f equals the union of the images (preimages) of the residue classes $S_{r(m)}$ ($\tilde{S}_{\tilde{r}(\tilde{m})}$) under f. □

1.2.2 Example We would like to determine image and preimage of the residue class $0(5)$ under the Collatz mapping T. In the terminology used in the proof of Lemma 1.2.1, Assertion (2) we have $S = 0(5)$, $S_{0(2)} = S \cap 0(2) = 0(10)$ and $S_{1(2)} = S \cap 1(2) = 5(10)$. It follows ${S_{0(2)}}^T = 0(10)/2 = 0(5)$ and ${S_{1(2)}}^T = (3 \cdot 5(10) + 1)/2 = 8(15)$, and hence $S^T = {S_{0(2)}}^T \cup {S_{1(2)}}^T = 0(5) \cup 8(15)$.

The determination of the preimage is a bit more work: Intersecting S with the residue classes (mod $\tilde{m} = \mathrm{Mult}(T) \cdot \mathrm{Mod}(T) = 6$) yields the sets $\tilde{S}_{0(6)} = 0(30)$, $\tilde{S}_{1(6)} = 25(30)$, $\tilde{S}_{2(6)} = 20(30)$, $\tilde{S}_{3(6)} = 15(30)$, $\tilde{S}_{4(6)} = 10(30)$ and $\tilde{S}_{5(6)} = 5(30)$. Their preimages can be determined partial mapping by partial mapping again (caution: T is not injective – thus for $\tilde{r} \equiv 2$ (3) both partial mappings have to be considered). In this way we get the preimages $2{\cdot}0(30) = 0(60)$, $2{\cdot}25(30) = 50(60)$, $2{\cdot}20(30) \cup (2{\cdot}20(30){-}1)/3 = 40(60) \cup 13(20)$, $2 \cdot 15(30) = 30(60)$, $2 \cdot 10(30) = 20(60)$ and $2 \cdot 5(30) \cup (2 \cdot 5(30) - 1)/3 = 10(60) \cup 3(20)$. The full preimage of the residue class $0(5)$ under T is their union, hence $0(10) \cup 3(10)$.

In the following, it will often be convenient to assume that the ring R has one of the following properties:

1.2.3 Definition We say that the ring R has the

- *weak residue class decomposability property*, if it has a residue class ring of cardinality 2, and the
- *strong residue class decomposability property*, if it even has residue class rings of any nonzero finite cardinality.

Of course these terms need a justification:

1.2.4 Remark The ring R has the weak residue class decomposability property if and only if any residue class of R can be written as a disjoint union of two other residue classes.

If R has the weak residue class decomposabiliy property, we can conclude inductively that a disjoint union of k residue classes of R can also be written as a disjoint union of an arbitrary number $\tilde{k} > k$ of residue classes of R.

The strong residue class decomposability property is equivalent to the condition that any residue class can be decomposed into an arbitrary number of disjoint residue classes with the same moduli.

1.2.5 Examples The rings $\mathbb{Z}$, $\mathbb{Z}_{(\pi)}$ with $2 \in \pi$, the ring of Gaussian integers and $\mathbb{F}_2[x]$ for example have the weak residue class decomposability property. For example in $\mathbb{F}_2[x]$, a residue class $a(m)$ can be written as the union of $a(x \cdot m)$ and $a + m(x \cdot m)$. The rings $\mathbb{Z}_{(\pi)}$ with $2 \notin \pi$ and $\mathbb{F}_q[x]$ with $q \neq 2$ do not have this property. The ring $\mathbb{Z}$ has even the strong residue class decomposability property.

1.3 Composita and Inverses of rcwa Mappings

The subject of this thesis are residue class-wise affine *groups*.

But do the bijective residue class-wise affine mappings of the ring R indeed form a group? – This question should be answered in this section.

Further it should be investigated in which way modulus, multiplier and divisor of the product of two rcwa mappings depend on modulus, multiplier and divisor of the factors, and what influence the inversion of a bijective rcwa mapping has on these values.

1.3.1 Lemma *(Composita and inverses of rcwa mappings.)*

a) *Let f and g be rcwa mappings of a ring R. Then $f \cdot g$ (f is applied first) is an rcwa mapping of R as well, and the following hold:*

   1. $\mathrm{Div}(f) | \mathrm{Mod}(f)$.
   2. $\mathrm{Mod}(f \cdot g) | \mathrm{Mod}(f) \cdot \mathrm{Mod}(g)$ *sowie*
      $\mathrm{Mod}(f \cdot g) | \mathrm{Div}(f) \cdot \mathrm{lcm}(\mathrm{Mod}(f), \mathrm{Mod}(g))$.
   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. $\mathrm{Div}(f \cdot g) | \mathrm{Div}(f) \cdot \mathrm{Div}(g)$.
   6. $\mathcal{P}(f \cdot g) \subseteq \mathcal{P}(f) \cup \mathcal{P}(g)$.

b) *Let σ be a bijective rcwa mapping of R. Then σ^{-1} is one as well. If the restriction of σ to a residue class $r(m)$ is given by $n \mapsto (a_{r(m)} \cdot n + b_{r(m)})/c_{r(m)}$, then the following hold:*

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

c) *Let f, σ, σ_1 and σ_2 be rcwa mappings of R and let σ, σ_1 and σ_2 be bijective. Then the following hold:*

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

Proof:

a) Let f and g be rcwa mappings of the ring R. Further let $m_f := \mathrm{Mod}(f)$ and $m_g := \mathrm{Mod}(g)$.

The compositum of an affine partial mapping of f and an affine partial mapping of g is affine as well. Which of the two affine partial mappings of f and g are applied one after another when evaluating $n^{f \cdot g}$ depends only on n mod $(m_f \cdot \mathrm{Div}(f) \cdot m_g)$. Further the product $m_f \cdot \mathrm{Div}(f) \cdot m_g$ is nonzero, since by definition, the ring R does not contain divisors of zero. Consequently, $f \cdot g$ is an rcwa mapping as well.

Let $a, b, c \in R$. Further let $r(m_f) \in R/m_f R$. By Lemma 1.1.8, Assertion (1), the image of $r(m_f)$ under the mapping $n \mapsto a \cdot n + b$ is the residue class $a \cdot r + b(a \cdot m_f)$. This residue class can only be a subset of $0(c)$ if $c | a \cdot m_f$. If a and c are coprime, this requires $c | m_f$. This is Assertion (1).

Let $m_{fg} := \mathrm{Mod}(f \cdot g)$. We have to prove the divisibility relations $m_{fg} | (m_f \cdot m_g)$ and $m_{fg} | \mathrm{Div}(f) \cdot \mathrm{lcm}(m_f, m_g)$ (2). An element $m \in R$ is a multiple of m_{fg} if $m_f | m$, and if it depends only on n mod m which residue class (mod m_g) the image of n under f belongs to. By definition, the value n mod m_f determines the affine partial mapping of f which is applied to n. Which residue class (mod m_g) the image of n under a fixed affine partial mapping of f belongs to is determined by n mod $(\mathrm{Div}(f) \cdot m_g)$. Thus we have $m_{fg} | \mathrm{lcm}(m_f, \mathrm{Div}(f) \cdot m_g)$, and thus the second of the claimed divisibility relations. Due to $\mathrm{Div}(f) | m_f$ (Assertion (1)) the first relation holds as well. In case $g = f$, from $m_{fg} | \mathrm{Div}(f) \cdot \mathrm{lcm}(m_f, m_g)$ we can inductively conclude Assertion (3).

Assume that the mappings f and g are given by

$$n^f = \frac{a_{r(m_f)} \cdot n + b_{r(m_f)}}{c_{r(m_f)}} \quad \text{for } n \in r(m_f), \text{ where } r(m_f) \in R/m_f R, \text{ and}$$

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

We have

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

for $r_1(m_f) \in R/m_f R$ and $r_2(m_g) \in R/m_g R$ depending on n mod m_{fg}. From this we can immediately read off the assertions $\mathrm{Mult}(f \cdot g) | \mathrm{Mult}(f) \cdot \mathrm{Mult}(g)$ (4) and $\mathrm{Div}(f \cdot g) | \mathrm{Div}(f) \cdot \mathrm{Div}(g)$ (5). Now, Assertion (6) concerning the prime set of $f \cdot g$ follows immediately from the definition.

b) Let σ be a bijective rcwa mapping of R, and let $m := \mathrm{Mod}(\sigma)$.

The inverse of σ is composed from the inverses of the restrictions $\sigma|_{r(m)}$ of σ to the residue classes (mod m). The sources of these mappings are the images of the residue classes $r(m) \in R/mR$ under σ. Due to (a.1), Lemma 1.1.8, Assertion (1) tells us that they are residue classes as well. Thus the mapping σ^{-1} is residue class-wise affine, as claimed.

Obviously, the modulus of σ^{-1} divides the least common multiple of the moduli of the residue classes $r(m)^\sigma$. If we have

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

then Lemma 1.1.8, Assertion (1) tells us that

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

Thus we get Assertion (1). Further we have

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

From this we can immediately read off that inversion interchanges multiplier and divisor (Assertions (3) and (4)). Assertion (2) is an immediate consequence of (4) and (a.1). It follows also immediately that $\mathcal{P}(\sigma^{-1}) \subseteq \mathcal{P}(\sigma)$. Since all of our argumentation remains valid when we interchange the roles of σ and σ^{-1}, we get the equality which is claimed in (5).

c) Let σ, σ_1 and σ_2 be bijective rcwa mappings of the ring R, and let f be an arbitrary rcwa mapping of R. Using (a.2) and (b.1), we get the following chain of divisors:

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

This is Assertion (1). In the same way we get

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

which is Assertion (2). □

1.3.2 Examples Let T be the Collatz mapping and take α from Examples 1.1.3. Then we have

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

The reader can immediately check the validity of the assertions of Lemma 1.3.1 in these examples:

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 Let

- $\mathrm{Rcwa}(R)$ denote the set of all rcwa mappings of the ring R, and
- $\mathrm{RCWA}(R)$ denote the set of all bijective rcwa mappings of the ring R.

1.3.4 Lemma *The following hold:*

1. *The set* $\mathrm{Rcwa}(R)$ *forms a monoid under composition of mappings.*
2. *The set* $\mathrm{RCWA}(R)$ *forms a group under composition of mappings. This group is a proper subgroup of* $\mathrm{Sym}(R)$.
3. *The cardinalities of the sets* R, $\mathrm{Rcwa}(R)$ *and* $\mathrm{RCWA}(R)$ *are the same.*

Proof:

1. Since the identity mapping is an rcwa mapping, this assertion follows immediately from Lemma 1.3.1a.
2. The fact that $\mathrm{RCWA}(R)$ is a subgroup of $\mathrm{Sym}(R)$ is an immediate consequence of Lemma 1.3.1. This subgroup is proper for reasons of cardinality: By Assertion (3), the sets R and $\mathrm{RCWA}(R)$ have the same cardinalities, but it is well-known that the one of $\mathrm{Sym}(R)$ is greater.
3. Given $y \in R$, the mapping $x \mapsto x + y$ is a bijective rcwa mapping. Thus the sets $\mathrm{Rcwa}(R)$ and $\mathrm{RCWA}(R)$ have at least the same cardinality as R. Since any rcwa mapping is determined by a finite number of coefficients from R and since by definition the ring R is infinite, their cardinality is not greater. □

1.4 rcwa Groups and rcwa Monoids

1.4.1 Definition We call a submonoid of $\mathrm{Rcwa}(R)$ a *residue class-wise affine* monoid over R. Accordingly, we call a subgroup of $\mathrm{RCWA}(R)$ a *residue class-wise affine* group over R. For these terms, we also use the abbreviated forms *rcwa monoid* resp. *rcwa group*.

At this point we take the opportunity to recall that any group is in particular also a monoid, hence a semigroup with one. Hence in the following we use the term *monoid* as a generic term.

The terms *modulus*, *multiplier*, *divisor* and *prime set* can be transferred to rcwa groups and -monoids in a natural way:

1.4.2 Definition We define the *modulus*, the *multiplier* and the *divisor* of an rcwa monoid by the least common multiple of the moduli, multipliers resp. divisors of its elements. In case there is no finite least common multiple, we take in the former case the value 0 and in the latter two cases the value ∞. We define the *prime set* $\mathcal{P}(G)$ of an rcwa monoid by the union of the prime sets of its elements.

1.4.3 Lemma *Let $G, H \leqslant \mathrm{Rcwa}(R)$ be rcwa monoids, and let $\sigma \in \mathrm{RCWA}(R)$. Then the following hold:*

1. *G is an rcwa group* $\Rightarrow \mathrm{Mult}(G) | \mathrm{Mod}(G)$,
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 is an rcwa group* $\Rightarrow \mathrm{Mult}(G) = \mathrm{Div}(G)$,
6. *G is an rcwa group* $\Rightarrow \mathcal{P}(G)$ *is the set of prime divisors of* $\mathrm{Mod}(G)$, *and*
7. $\mathrm{Mod}(G^\sigma) | \mathrm{Mult}(\sigma) \cdot \mathrm{Mod}(\sigma)^2 \cdot \mathrm{Mod}(G)$.

In this context, let $0|0$ and $\infty|0$.

Proof: Assertion (2) is an immediate consequence of Lemma 1.3.1a, Assertion (1) and the definition of the divisor and the modulus of an rcwa monoid. We get Assertion (1) when we additionally use Lemma 1.3.1b, Assertion (2). Assertion (3) and (4) are immediate consequences of the definition of the modulus resp. the prime set of an rcwa monoid. Assertion (5) follows from Lemma 1.3.1b, Assertion (3) and (4). Assertion (6) follows from (1) and (2) and the definition of the prime set of an rcwa group. Assertion (7) is an immediate consequence of Lemma 1.3.1c, Assertion (1). □

1.5 rcwa Representations of Groups

Let $\mathbb{K}$ be a category. A $\mathbb{K}$-representation of a group G is an homomorphism

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

for an object X of $\mathbb{K}$. In representation theory, usually $\mathbb{K}$ is the category of finite-dimensional vector spaces over a field or the category of finite-dimensional modules over a ring. The following notion of representation fits seamlessly into this general framework:

1.5.1 Definition Let G be a group. We call an homomorphism $\varphi : G \to \mathrm{RCWA}(R)$ a *residue class-wise affine representation*, or shortly *rcwa representation*, of G over R. In case $R = \mathbb{Z}$, we call φ also an *integral* rcwa representation.

1.5.2 Examples We would like to illustrate this definition by giving a few examples:

1. It is a straightforward calculation to check that a faithful rcwa representation of the Sylow 3 - subgroup

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

   of S_9 is given by

   $$\varphi : \ G \ \longrightarrow \ \mathrm{RCWA}(\mathbb{Z}),$$

   $$(1,2,3)(4,6,5)(7,8,9) \ \longmapsto \ \left(s_1 : \ n \mapsto \begin{cases} n & \text{if } \ n \in 0(3) \cup 2(3), \\ n+6 & \text{if } \ n \in 1(9), \\ n-3 & \text{if } \ n \in 4(9) \cup 7(9). \end{cases} \right),$$

   $$(1,4,7)(2,5,8)(3,6,9) \ \longmapsto \ \left(s_2 : \ n \mapsto \begin{cases} n & \text{if } \ n \in 0(9) \cup 6(9), \\ 3n+18 & \text{if } \ n \in 1(9), \\ n+2 & \text{if } \ n \in 2(9) \cup 5(9), \\ \frac{n+3}{3} & \text{if } \ n \in 3(9), \\ 3n-9 & \text{if } \ n \in 4(9) \cup 7(9), \\ n-7 & \text{if } \ n \in 8(9). \end{cases} \right).$$

   It is $\mathrm{Mod}(G^\varphi) = 27$, $\mathrm{Mult}(G^\varphi) = \mathrm{Div}(G^\varphi) = 3$, and $\mathcal{P}(G^\varphi) = \{3\}$.

2. We define $\nu_{1(4)}, \nu_{3(4)} \in \mathrm{RCWA}(\mathbb{Z})$ by

   $$n \mapsto \begin{cases} n+4 & \text{if } \ n \in 1(4), \\ n & \text{otherwise,} \end{cases} \quad \text{resp.} \quad n \mapsto \begin{cases} n+4 & \text{if } \ n \in 3(4), \\ n & \text{otherwise} \end{cases}$$

and take the mapping α from Examples 1.1.3. Then the rcwa representation

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

is faithful – this can be checked easily using RCWA .

It is $\mathrm{Mod}([\alpha, \nu_{1(4)}\alpha]) = \mathrm{Mod}([\alpha, \nu_{3(4)}\alpha]) = 18$. The commutator $[\alpha, \nu_{1(4)}\alpha]$ is given by

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

We have $\mathrm{Mod}(\mathrm{S}_{10}^{\varphi}) = 18$, $\mathrm{Mult}(\mathrm{S}_{10}^{\varphi}) = \mathrm{Div}(\mathrm{S}_{10}^{\varphi}) = 2$, and $\mathcal{P}(\mathrm{S}_{10}^{\varphi}) = \{2, 3\}$.

3. Let $F := \langle g_i,\ i \in \mathbb{N} \rangle$ be the free abelian group of countably infinite rank. Then

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

is a faithful rcwa representation of F. It is $\mathrm{Mod}(F^{\varphi}) = 0$, $\mathrm{Mult}(F^{\varphi}) = \mathrm{Div}(F^{\varphi}) = 1$, and $\mathcal{P}(F^{\varphi}) = \{2\}$.

1.6 Transition Graphs of rcwa Mappings

In the sequel, we will see that it is very useful to assign directed graphs to rcwa mappings in the following manner:

1.6.1 Definition Let $f \in \mathrm{Rcwa}(R)$ and $m \in R \setminus \{0\}$. We define the *transition graph* $\Gamma_{f,m}$ *of* f *for modulus* m as follows:

- The vertices are the residue classes (mod m).
- 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 $n^f \in r_2(m)$.

Thus $\Gamma_{f,m}$ is a directed graph which may have loops. In case $m = \mathrm{Mod}(f)$ we abbreviate $\Gamma_{f,m}$ by Γ_f.

The following elementary properties can be derived immediately from the definition:

1.6.2 Lemma Let $f \in \mathrm{Rcwa}(R)$, $\sigma \in \mathrm{RCWA}(R)$ and $m, m_1, m_2 \in R$. Then the following hold:

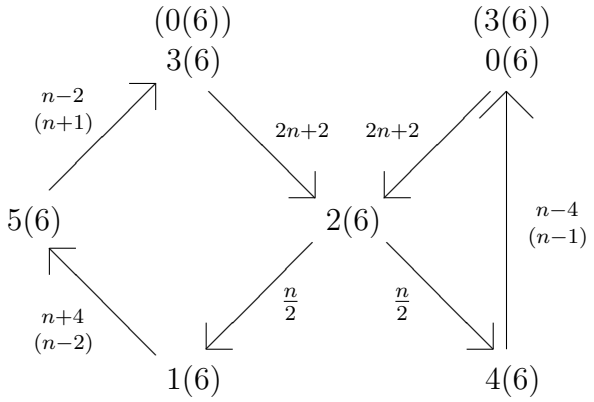
1. Every vertex of the graph $\Gamma_{f,m}$ has an outgoing edge. If f is surjective, then furthermore each vertex of $\Gamma_{f,m}$ has an ingoing edge.

2. The graph Γ_{f,m_1} is the quotient of $\Gamma_{f,m_1 \cdot m_2}$ by the equivalence relation on the set of vertices induced by congruence (mod m_1).

3. The graph $\Gamma_{\sigma^{-1},m}$ can be constructed from $\Gamma_{\sigma,m}$ by reversing all edges.

1.6.3 Example The graph given below is e.g. the transition graph of an rcwa mapping g of order 7 and an rcwa mapping h of order 12 (in both cases for modulus 6).

The vertices and the associated affine partial mappings of h are given in brackets, as far as they are different from those of g. For reasons of nicer typesetting, we abbreviate affine mappings $n \mapsto (an + b)/c$ here and in all further figures showing transition graphs by $(an + b)/c$.



This graph has one cyclus of length 3 and one of length 4. Iterated application of the mapping g to an integer n causes both cycles to be passed consecutively, whereas iterated application of h causes only one of the cycles to be passed – which one depends on n mod 12. Hence the order of g is $3 + 4 = 7$, while the order of h is $\mathrm{lcm}(3, 4) = 12$. In particular we see that it is possible to 'twist' a 7-cycle into an rcwa mapping with modulus 6.

Much more involved examples of transition graphs can be found in Appendix B.

We can not only determine transition graphs of given rcwa mappings. If we would like to construct a mapping with given properties, it is often a good idea first to construct the graph and then to assign affine mappings to its vertices resp. edges:

1.6.4 Example We would like to construct a permutation $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ of order 257 with modulus 32.

For this purpose let $\Gamma_{\sigma,32}$ be a directed graph with the 32 vertices $0(32), \ldots, 31(32)$, 15 cycles of length 16 and one cyclus of length 17. Further, 15 vertices of $\Gamma_{\sigma,32}$ should belong to all cycles, 15 vertices should exclusively belong to one of the cycles of length 16 each and 2 vertices should exclusively belong to the cyclus of length 17.

We get the permutation σ by assigning affine mappings to the edges resp. vertices of this graph. We choose these mappings in such a way that a cycle of the permutation σ always passes all the cycles of $\Gamma_{\sigma,32}$ one after the other. The length of such a cycle is $15 \cdot 16 + 17 = 257$. In this way, we can for example construct the following mapping:

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

We see that the order of an element $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ can be a prime which is considerably greater than $\mathrm{Mod}(\sigma)$.

1.7 Integral, Balanced and Class-Wise Order-Preserving Mappings

1.7.1 Definition We call an rcwa mapping $f \in \mathrm{Rcwa}(R)$

- *integral* if $\mathrm{Div}(f) = 1$,
- *balanced*, if the sets of prime divisors of $\mathrm{Mult}(f)$ and $\mathrm{Div}(f)$ are the same, and
- *class-wise order-preserving* if R is ordered and all affine partial mappings of f are order-preserving.

We call an rcwa monoid *integral*, *balanced* resp. *class-wise order-preserving* if all of its elements have the respective property. We denote the subgroup of $\mathrm{RCWA}(R)$ formed by the bijective class-wise order-preserving mappings by $\mathrm{RCWA}^+(R)$.

1.7.2 Remark An rcwa mapping is integral 'if it does not involve fractions'. Thus integral rcwa mappings have a particularly simple structure. Easy density arguments show that a surjective integral rcwa mapping is even bijective, and that the multiplier of a bijective integral rcwa mapping equals 1 as well. Thus due to Lemma 1.3.1, Assertion (a.4), (a.5), (b.3) and (b.4), the bijective integral rcwa mappings form a subgroup of RCWA(R). By Lemma 1.3.1a, Assertion (3), raising an integral rcwa mapping to some power does not increase its modulus.

Balancedness is a substantially weaker property than integralness. We will see that balancedness is a necessary condition for the boundedness of the moduli of the powers of the respective rcwa mapping.

An rcwa mapping of $\mathbb{Z}$ is class-wise order-preserving if and only if its affine partial mappings are order-preserving, i.e. of the form $n \mapsto (an+b)/c$ with $a > 0$.

1.7.3 Remark The subgroup $\mathrm{RCWA}^+(\mathbb{Z}) < \mathrm{RCWA}(\mathbb{Z})$ is not normal:

For example the mapping $\nu^{\varsigma_{0(2)}}$ where $\nu : n \mapsto n+1$ and $\varsigma_{0(2)} : n \mapsto (-1)^{n+1} \cdot n$ is given by $n \mapsto -n + (-1)^n$. Thus in contrast to ν itself it is not class-wise order-preserving.

1.8 A Notion of Tameness for rcwa Mappings and rcwa Monoids

Some rcwa mappings, -groups, -monoids and -representations have a considerably easier structure than others:

1.8.1 Definition We say that the following objects are *tame*:

1. An rcwa monoid whose modulus is nonzero.

2. An rcwa mapping which generates a tame cyclic monoid.

3. An rcwa representation whose image is tame.

If an rcwa monoid, an rcwa mapping resp. an rcwa representation is not tame, we say that it is *wild*.

1.8.2 Remark A mapping $f \in \mathrm{Rcwa}(R)$ is tame if and only if the set $\{\mathrm{Mod}(f^k) | k \in \mathbb{N}\}$ of the moduli of its powers is bounded. Integral rcwa mappings and finitely generated integral rcwa monoids are always tame.

Tameness is a class invariant:

1.8.3 Lemma *Let $\sigma \in \mathrm{RCWA}(R)$. Then the following hold:*

1. *$f \in \mathrm{Rcwa}(R)$ tame $\Rightarrow$ f^σ tame.*
2. *$G < \mathrm{Rcwa}(R)$ tame $\Rightarrow$ G^σ tame.*
3. *$G < \mathrm{RCWA}(R)$ tame $\Rightarrow$ G^σ tame.*

Proof: Assertion (2) is a consequence of Lemma 1.4.3, Assertion (7). Assertion (3) is a special case of (2), and Assertion (1) follows from (2), since by definition an rcwa mapping is tame if and only if it generates a tame cyclic monoid. □

A tame bijective rcwa mapping generates always even a tame cyclic group:

1.8.4 Lemma *The following hold:*

1. *The multiplier of a bijective rcwa mapping is bounded by a function in its modulus.*
2. *Bijective rcwa mappings generate tame cyclic groups.*

Proof:

1. Let $\sigma \in \mathrm{RCWA}(R)$ and set $m := \mathrm{Mod}(\sigma)$. Since σ is bijective, the images of the residue classes $r(m) \in R/mR$ under σ form a partition of R. By Lemma 1.1.8, Assertion (1) this partition consists of single residue classes and has the form

$$R \;=\; \dot{\bigcup_{r(m)\in R/mR}} r^\sigma \left(\frac{a_{r(m)} \cdot m}{c_{r(m)}} \right),$$

   where we use the notation from Definition 1.1.2. By Lemma 1.3.1a, Assertion (1) we have $\forall r(m) \in R/mR \;\; c_{r(m)} | m$. Thus the multiplier of σ divides the least common multiple of the moduli of the residue classes in this partition. By Lemma 1.1.10 there is a partition

$$1 \;=\; \sum_{r(m)\in R/mR} \frac{1}{|R/a_{r(m)}R| \cdot |R/mR| / |R/c_{r(m)}R|}$$

   of 1 into fractions of the form $1/n$. It is well-known from elementary number theory that an upper bound on the number of fractions in such a sum enforces an upper bound on the denominators. This proves our assertion.

2. From Assertion (1) and Lemma 1.3.1b, Assertion (1) we conclude that there is an upper bound on the modulus of the inverse of a bijective rcwa mapping with a given modulus. □

1.8.5 Examples We would like to illustrate the terms *tame* and *wild* by giving a few examples:

1. The Collatz mapping T is wild. More precisely we have $\forall k \in \mathbb{N}\ \mathrm{Mod}(T^k) = 2^k$. This is a major reason for the difficulty of proving the $3n+1$ Conjecture. If the mapping T would be tame, there would be a upper bound on the number of affine partial mappings of its powers T^k. Therefore, under this circumstance verifying the $3n+1$ Conjecture would be merely a computational task.

2. The groups G^φ and S_{10}^φ from Examples 1.5.2, Part (1) and (2) are finite, thus in particular tame.

   In contrast to this, the representation from Examples 1.5.2, Part (3) is wild, although all elements of its image are tame.

3. The mappings $\beta, \beta^{-1} \in \mathrm{RCWA}(\mathbb{Z})$ given by

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

   are mutually inverse. Assume that $5^k || n$ for some $k \in \mathbb{N}$. Then we obviously have $\forall l \in \{0, \ldots, k\}\ 5^{k-l} || n^{\beta^l}$. Hence the value $n^{\beta^{k-1}} \bmod 5$ is not already determined by $n \bmod 5^{k-1}$. Using Lemma 1.3.1a, Part (2) we can conclude that $\mathrm{Mod}(\beta^k) = \mathrm{Mod}(\beta)^k = 5^k$, thus in particular that β is wild. By Lemma 1.8.4, Part (2) this implies that β^{-1} is wild as well.

4. Let $F := \langle f_1, f_2 \rangle$ be the free abelian group of rank 2. Further let α be as in Examples 1.1.3, and let β be as above. Then

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

   is a wild rcwa representation of F.

5. It is possible to show that the mappings g and h from Example 1.6.3 generate a tame infinite group. The modulus of this group is 12.

CHAPTER 2

Residue Class-Wise Affine Groups

2.1 How 'Large' is RCWA(Z)?

In this section we prove the following assertions:

The group RCWA($\mathbb{Z}$)

- is not finitely generated,
- has finite subgroups of any isomorphism type, and
- acts highly transitively on $\mathbb{Z}$.

As far as this is possible without significant additional efforts, these assertions are generalized to groups RCWA(R) over suitable rings R other than $\mathbb{Z}$.

2.1.1 Theorem *If the ring R contains infinitely many prime elements, then* RCWA(R) *is not finitely generated.*

Proof: For any prime element $p \in R$ there is an element of RCWA(R) with prime set $\{p\}$ – for example

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

Furthermore the prime set of an rcwa mapping is always finite. Now the assertion follows immediately from Lemma 1.3.1, Assertion (a.6) and (b.5). □

Every finite group can be embedded into RCWA($\mathbb{Z}$):

2.1.2 Theorem Assume $R = \mathbb{Z}$ or $R = \mathbb{Z}_{(\pi)}$ for a finite set of primes π. Then, any finite symmetric group S_m has a faithful rcwa representation over R. Given a positive integer $m > 1$, an example of such a representation is

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

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

where in case $R = \mathbb{Z}$ we put $\tilde{m} := m$, and in case $R = \mathbb{Z}_{(\pi)}$ we let $\tilde{m}$ be the least positive integer $\geqslant m$, whose prime divisors are elements of π.

It remains to show that the group RCWA(R) acts highly transitively on R. For this we need two elementary lemmata. The first one is an assertion concerning affine mappings from residue classes onto residue classes:

2.1.3 Lemma *Let $r(m)$ and $\tilde{r}(\tilde{m})$ be residue classes of R. Then there are affine mappings from the quotient field K of R onto itself, which map $r(m)$ bijectively onto $\tilde{r}(\tilde{m})$. These mappings have the form $f = f_1 \cdot f_2(u,k)$ with*

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

and

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

for an $u \in R^\times$ and a $k \in R$. All affine mappings which map the residue class $\tilde{r}(\tilde{m})$ bijectively onto itself can be represented in the form $f_2(u,k)$ for suitable u and k.

Proof: By Lemma 1.1.8, Assertion (1) it is $r(m)^{f_1} = \tilde{r}(\tilde{m})$. It remains to show that the mappings $f_2(u,k)$ map the residue class $\tilde{r}(\tilde{m})$ bijectively onto itself, and that there are no further affine mappings which do the same. For this purpose let

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

be an affine mapping. It holds that $\{\tilde{r}^\alpha, a\tilde{m}/c\} \subset R$, and without loss of generality we can assume that $\gcd(a,b,c) = 1$ and that $c = |c|$. By Lemma 1.1.8, Assertion (1) the image of α is the residue class $(a\tilde{r}+b)/c \bmod a\tilde{m}/c$. Thus source and image of α are equal if and only if $a/c \in R^\times$ and if there is furthermore a $k \in R$ such that $b = \tilde{r}(c-a) + k\tilde{m}$. The standardization $c = |c|$ yields $c = 1$, and we get the assertion since non-constant affine mappings are injective. □

We can put together the affine mappings described in Lemma 2.1.3 and build rcwa mappings from them – this yields the following 'partition transitivity lemma':

2.1.4 Lemma Let S be a union of finitely many residue classes of R, and let k be a positive integer. Further let $R = r_1(m_1) \cup \cdots \cup r_k(m_k)$ and $S = \tilde{r}_1(\tilde{m}) \cup \cdots \cup \tilde{r}_k(\tilde{m})$ be partitions of R resp. S into k residue classes, each, and let $n_i \in r_i(m_i)$ resp. $\tilde{n}_i \in \tilde{r}_i(\tilde{m}_i)$ be arbitrary representatives. Then by Lemma 2.1.3 there are affine mappings whose sources are the residue classes $r_1(m_1), \ldots, r_k(m_k)$ and which can be combined to form an injective mapping $f \in \mathrm{Rcwa}(R)$ such that

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

It follows immediately from this construction that $\mathrm{Mod}(f) | \operatorname{lcm}(m_1, \ldots, m_k)$. If the ring R has the weak residue class decomposability property, then by Remark 1.2.4 we can replace the residue classes $r_i(m_i), \tilde{r}_i(\tilde{m}_i)$ by unions of finitely many residue classes.

Now it is easy to prove the last of the three assertions made above:

2.1.5 Theorem *The group* $\mathrm{RCWA}(R)$ *acts highly transitively on* R.

Proof: Let $k \in \mathbb{N}$. We have to show that given two k-tuples $(n_1, \ldots, n_k)$ and $(\tilde{n}_1, \ldots, \tilde{n}_k)$ of pairwisely different elements of R, there is always a permutation $\sigma \in \mathrm{RCWA}(R)$ such that $(n_1^\sigma, \ldots, n_k^\sigma) = (\tilde{n}_1, \ldots, \tilde{n}_k)$. We choose $a \in R \setminus (R^\times \cup \{0\})$. Further let $e \in \mathbb{N}$ be large enough such that no two n_i, n_j and no two $\tilde{n}_i, \tilde{n}_j$ lie in the same residue class (mod a^e). Finally, we choose $n_{k+1}, \ldots, n_{|R/a^eR|}$ and $\tilde{n}_{k+1}, \ldots, \tilde{n}_{|R/a^eR|}$ in such a way that the sets $\{n_1, \ldots, n_{|R/a^eR|}\}$ and $\{\tilde{n}_1, \ldots, \tilde{n}_{|R/a^eR|}\}$ become sets of representatives for the residue classes (mod a^e). Now the assertion follows from Lemma 2.1.4, applied to the partitions

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

with the requirement $\forall i \in \{1, \ldots, |R/a^eR|\} \ n_i^\sigma = \tilde{n}_i$ for the representatives. □

Theorem 2.1.5 has a considerable impact on the structure of possible nontrivial normal subgroups of $\mathrm{RCWA}(R)$:

2.1.6 Corollary Using [DM96], Corollary 7.2A we can conclude that a nontrivial normal subgroup of $\mathrm{RCWA}(R)$ must act highly transitively on R as well. Since an abelian group can act at most 1-transitively on a set, the centre of $\mathrm{RCWA}(R)$ is trivial. Since any highly transitive permutation group has a subgroup which acts on a set of cardinality 5 as an alternating group of degree 5, the group $\mathrm{RCWA}(R)$ does not even have a solvable nontrivial normal subgroup.

2.2 The Fürstenberg Topology

The group RCWA(R) becomes a group of homoeomorphisms once the ring R is endowed with a suitable topology. Lemma 1.1.9 is a good starting point for this:

2.2.1 Definition We define the *Fürstenberg topology* on R as the topology which is induced by taking the set of all residue classes as a basis. In the following, we always regard the ring R also as a topological space with this topology.

2.2.2 Remark In case $R = \mathbb{Z}$ this is the topology which has been introduced by Harry Fürstenberg in his topological proof [Für55] that there are infinitely many primes.

2.2.3 Theorem The following hold:

1. The topological space R is a Hausdorff space.

2. Residue classes are both open and closed.

3. rcwa mappings are continuous.

4. Preimages of unions of finitely many residue classes of R under rcwa mappings are unions of finitely many residue classes as well.

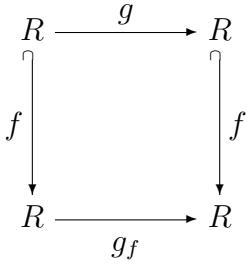
5. The group RCWA(R) is a group of homoeomorphisms.

Proof: Let $n_1, n_2 \in R$ be two distinct points. We choose an $m \in R \setminus \{0\}$ which does not divide $n_1 - n_2$. Then the residue classes $n_1(m)$ and $n_2(m)$ are disjoint open neighbourhoods of n_1 and n_2. This yields Assertion (1). By definition, all nontrivial residue class rings of R are finite. This implies Assertion (2). We get Assertion (3) and (4) just like Lemma 1.2.1, Assertion (2), when we additionally take into consideration that the preimage of a set under a constant affine partial mapping of an rcwa mapping f is either empty or a residue class (mod Mod(f)). We conclude Assertion (5) from Lemma 1.2.1, Assertion (2) and Lemma 1.3.4, Assertion (2). □

2.3 Restriction Monomorphisms

In the following we will see that the groups RCWA(R) have proper subgroups which are isomorphic to the whole of RCWA(R) itself. It will turn out to be convenient to consider isomorphisms from RCWA(R) to such subgroups:

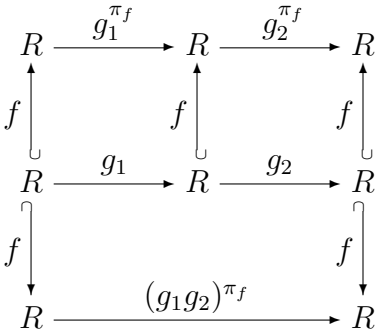
2.3.1 Definition Given an injective rcwa mapping f and an rcwa mapping g of R, let g_f be the uniquely determined rcwa mapping which pointwisely fixes the complement of the image of f and makes the following diagram commutative:



We call the mapping $\pi_f : \mathrm{Rcwa}(R) \to \mathrm{Rcwa}(R),\ g \mapsto g_f$ the *restriction monomorphism associated to* f. Where there is no risk of confusion, we identify the restriction monomorphism π_f with its restriction to $\mathrm{RCWA}(R)$.

2.3.2 Theorem *The restriction monomorphisms π_f are well-defined mappings, and they are indeed monomorphisms. Furthermore, the mappings $\pi_f : \mathrm{RCWA}(R) \to \mathrm{RCWA}(R)^{\pi_f}$ are permutation isomorphisms.*

Proof: Due to the required injectivity of f, restriction monomorphisms are indeed well-defined injective mappings. For this conclusion it is not even necessary that we know that we are dealing with rcwa mappings. Furthermore since f is an rcwa mapping, images of rcwa mappings under the restriction monomorphism associated to f are rcwa mappings as well. It is also easy to see that restriction monomorphisms are homomorphisms – given any two mappings $g_1, g_2 \in \mathrm{Rcwa}(R)$, by definition all three rectangles in the following diagram commute:



This yields $(g_1 g_2)^{\pi_f} = g_1^{\pi_f} g_2^{\pi_f}$. The equality $(g^{-1})^{\pi_f} = (g^{\pi_f})^{-1}$ for bijective g can be obtained directly from the definition by following the horizontal arrows in the reverse direction. Since the mapping f is bijective as a mapping from R onto $\mathrm{im}\, f$, the restriction monomorphism π_f just causes a 'renumbering' $n \mapsto n^f$ of the points. Thus π_f is a permutation isomorphism. □

2.3.3 Corollary Using Theorem 2.3.2 and Theorem 2.1.5, we can conclude that for any possible image $\operatorname{im} f$ of an injective rcwa mapping f, the group $\mathrm{RCWA}(R)$ has a subgroup which is permutation isomorphic to $\mathrm{RCWA}(R)$ itself, acts highly transitively on $\operatorname{im} f$ and fixes $R \setminus \operatorname{im} f$ pointwise. A consequence of this is that the class of groups which have faithful rcwa representations over R is closed under forming direct products: Given $G, H \leqslant \mathrm{RCWA}(R)$, choose $a \in R \setminus (R^\times \cup \{0\})$ and ring elements $b_1, b_2 \in R$ which are not congruent (mod a). Then

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

Assume that R has the weak residue class decomposability property and let $S_1, S_2 \subsetneq R$ be nonempty unions of finitely many residue classes of R. Then, using Lemma 2.1.4 we can conclude that there are injective rcwa mappings f_1 and f_2 of R such that $\operatorname{im} f_1 = S_1$ and $\operatorname{im} f_2 = S_2$. Looking a bit ahead on Theorem 2.4.1 reveals that there further is a permutation $\sigma \in \mathrm{RCWA}(R)$ such that $S_1^\sigma = S_2$. This yields $(\operatorname{im} \pi_{f_1})^\sigma = \operatorname{im} \pi_{f_2}$. Hence in particular all images of restriction monomorphisms which are not inner automorphisms are mutually conjugate in $\mathrm{RCWA}(R)$.

2.4 Transitivity on Sets of Unions of Residue Classes

In Theorem 2.1.5 we have already shown that the group $\mathrm{RCWA}(R)$ acts highly transitively on the underlying ring R. It is similarly easy to prove an assertion concerning the transitivity of the action of $\mathrm{RCWA}(R)$ on the set of unions of residue classes. Of course without making assumptions concerning disjointness of the sets in question, we cannot get more than 1-transitivity:

2.4.1 Theorem *If the ring R has the weak residue class decomposability property, then the group* $\mathrm{RCWA}(R)$ *acts transitively on the set of unions of finitely many residue classes distinct from $\emptyset$ and R itself.*

Proof: Let $\emptyset \neq S_1, S_2 \subsetneq R$ be unions of finitely many residue classes. We have to show that $\exists \sigma \in \mathrm{RCWA}(R) : S_1^\sigma = S_2$. Since R has the weak residue class decomposability property, and since by Lemma 1.1.9, complements of unions of finitely many residue classes are unions of finitely many residue classes as well, we get the claimed assertion by applying Lemma 2.1.4 to the partitions $R = S_1 \cup (R \setminus S_1) = S_2 \cup (R \setminus S_2)$. □

2.4.2 Example We would like to construct a mapping $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ which maps the residue class $1(2)$ onto the union of the residue classes $2(5)$ and $3(5)$.

For this purpose we write $1(2)$ as union of $1(4)$ and $3(4)$, and the complement $\mathbb{Z} \setminus 1(2)$ as union of $0(6)$, $2(6)$ and $4(6)$.

Using Lemma 2.1.3 we construct affine mappings which map $1(4)$ onto $2(5)$, $3(4)$ onto $3(5)$, $0(6)$ onto $0(5)$, $2(6)$ onto $1(5)$ resp. $4(6)$ onto $4(5)$. Putting these mappings together yields the desired mapping

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

The condition in Theorem 2.4.1 that R has the weak residue class decomposability property is essential:

2.4.3 Remark If the ring R does not have the weak residue class decomposability property, the group $\mathrm{RCWA}(R)$ acts in general not transitively on the set of nonempty unions of residue classes of R distinct from R itself. In case $R = \mathbb{Z}_{(3)}$ for example it is not possible to write a union of an even number of residue classes as a union of an odd number of residue classes and vice versa. Furthermore, in this case the parity of the number of residue classes in such a union is invariant under rcwa mappings. Hence the action of $\mathrm{RCWA}(\mathbb{Z}_{(3)})$ on the set of unions of residue classes is intransitive.

Apart from considering the action of $\mathrm{RCWA}(R)$ on the set of unions of residue classes, we can also consider the action of this group act on an element of this set. At this point it is convenient to introduce the notion of a *Jordan set*. Since this term might not be well-known to every reader, we give the commonly used definition (cp. e.g. [DM96], Chapter 7, Section 4):

2.4.4 Definition Let G be a group which acts on a set S. The set S_J is called a *Jordan set* and the complement $S_C := S \setminus S_J$ is called a *Jordan complement* if the action of the pointwise stabilizer $G_{(S_C)}$ on S_J is transitive and if $|S_J| > 1$. If S_C is finite and if G acts at least $|S_C| + 1$-fold transitively on S, then S_J and S_C are called *improper*. In this case, S_C is a Jordan complement already for reasons of cardinality. The Jordan set S_J and the Jordan complement S_C are called *proper* if S_C is infinite or G does not act $|S_C| + 1$-fold transitively on S. The group G is called a *Jordan group* if it acts transitively on S and if it has at least one proper Jordan complement. If $G_{(S_C)}$ acts k-fold transitively resp. highly transitively on S_J, the Jordan set S_J is called k-fold transitive resp. highly transitive as well.

2.4.5 Remark If R has the weak residue class decomposability property, then we conclude from Corollary 2.3.3 that RCWA(R) is a Jordan group. Further we see that all nonempty unions of finitely many residue classes of R are both highly transitive Jordan sets and highly transitive Jordan complements.

2.4.6 Theorem *Assume that the ring R has the weak residue class decomposability property. Then the Jordan sets for* RCWA(R) *in R are precisely the open sets and the Jordan complements are precisely the closed sets. All Jordan sets are highly transitive.*

Proof: We know from Theorem 2.2.3, Assertion (5) that RCWA(R) is a group of homoeomorphisms of R. By Theorem 2.2.3, Assertion (2) the Fürstenberg topology has a basis consisting of sets which are both open and closed. Further, Theorem 2.1.5 tells us that RCWA(R) acts transitively on R. Hence we can conclude from [BMMN98], Section 11.1.2, that the Jordan sets resp. the Jordan complements for RCWA(R) in R are at most the open sets resp. closed sets. It remains to show that all open sets are indeed highly transitive Jordan sets.

By Remark 2.4.5 unions of finitely many residue classes are highly transitive Jordan sets. Let $S \subset R$ be open. Without loss of generality, we can assume that $S = \cup_{i=1}^{\infty} r_i(m_i)$. This can be rewritten as $S = \cup_{i=1}^{\infty}(r_i(m_i) \cup r_{i+1}(m_{i+1}))$. Thus the set S is a union of a connected family of highly transitive Jordan sets, and as is such due to [BMMN98], Corollary 10.10 a highly transitive Jordan set as well. □

Ben Green and Terence Tao have shown in in [GT04] that the set of primes contains arithmetic progressions of arbitrary length. This motivates the following considerations.

2.4.7 Definition The elements of the orbits $\{1, 2, \ldots, l\}^{\mathrm{Aff}(\mathbb{Z})}$, $l \in \mathbb{N}$ are called *arithmetic progressions of length l*. Accordingly, saying that a set $S \subseteq \mathbb{Z}$ *contains arithmetic progressions of arbitrary length* means

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

2.4.8 Theorem *The property of a set that it contains arithmetic progressions of arbitrary length is invariant under the action of* RCWA($\mathbb{Z}$). *This means that given $S \subseteq \mathbb{Z}$ and $\sigma \in$ RCWA($\mathbb{Z}$), the set S^σ has this property if and only if also S has it.*

Proof: Let $S \subseteq \mathbb{Z}$ be a set which contains arithmetic progressions of arbitrary length, and let $\sigma \in$ RCWA($\mathbb{Z}$). Further let $l \in \mathbb{N}$. It is sufficient to show that S^σ contains an arithmetic progression of length l. If we set $m := \mathrm{Mod}(\sigma)$, then the set S contains an arithmetic progression of length $m \cdot l$. We denote this progression by A. Obviously, there is a residue class $r(m) \in \mathbb{Z}/m\mathbb{Z}$ such that $|A \cap r(m)| \geqslant l$. This intersection is an arithmetic progression as well, just like its image $(A \cap r(m))^{\sigma|_{r(m)}} \subseteq S^\sigma$ under the affine mapping $\sigma|_{r(m)}$. □

A further invariant is the following:

2.4.9 Theorem *The property of a set $S \subseteq \mathbb{Z} \setminus \{0\}$ that the series $\sum_{n\in S} \frac{1}{|n|}$ diverges is invariant under the action of the point stabilizer* $\mathrm{RCWA}(\mathbb{Z})_0$ *in the same sense as in Theorem 2.4.8.*

Proof: The assertion holds since given $\sigma \in \mathrm{RCWA}(\mathbb{Z})_0$, the quotients $|n|/|n^\sigma|$ and $|n^\sigma|/|n|$ are defined for $n \in \mathbb{Z} \setminus \{0\}$ and bounded. □

2.4.10 Remark G. Szekeres has conjectured that even any set $S \subseteq \mathbb{Z} \setminus \{0\}$ such that the series $\sum_{n\in M} \frac{1}{|n|}$ diverges contains arithmetic progressions of arbitrary length (cp. [ET36]). This conjecture is still open today (cp. [GT04]). Theorem 2.4.9 reduces this problem to a set of representatives under the action of $\mathrm{RCWA}(\mathbb{Z})_0$.

2.5 Tame Groups and Respected Partitions

In the following we begin with considerations concerning the action of suitable rcwa groups on partitions of R into single residue classes. In the next section they will lead to a complete classification of tame rcwa groups.

First of all, we give a lemma about the orbits of certain residue classes under the action of tame groups:

2.5.1 Lemma *Let $G < \mathrm{RCWA}(R)$ be tame and let m be a multiple of* $\mathrm{Mod}(G)$*. Then the orbit of a residue class $r(m)$ under the action of G is a set of finitely many disjoint residue classes.*

Proof: By the choice of m, the restriction of an element $g \in G$ to $r(m)$ is always affine. From this we can conclude that the restriction of an element of G to any element of the orbit Ω of $r(m)$ under the action of G is affine as well: Let $\tilde{r}(\tilde{m}) \in \Omega$ and $g \in G$ be chosen arbitrarily. We have to show that $g|_{\tilde{r}(\tilde{m})}$ is affine. Due to our assumption, there is an $h \in G$ such that $r(m)^h = \tilde{r}(\tilde{m})$. As we already know, the mappings $h|_{r(m)}$ and $(hg)|_{r(m)}$ are affine. Since $\mathrm{AFF}(K)$ is a group, this implies that the mappings $h^{-1}|_{\tilde{r}(\tilde{m})}$ and $h^{-1}|_{\tilde{r}(\tilde{m})} \cdot (hg)|_{r(m)} = (h^{-1}hg)|_{\tilde{r}(\tilde{m})} = g|_{\tilde{r}(\tilde{m})}$ are affine as well. Since by Lemma 1.1.8 the image of a residue class under a bijective affine mapping is also a residue class provided that it is a subset of R, the orbit Ω contains only single residue classes. Lemma 1.4.3, Assertion (1) tells us that $\mathrm{Mult}(G)|m$, i.e. that $\forall g \in G\ \ \mathrm{Mult}(g)|m$. Thus due to Lemma 1.1.8, Assertion (1), the moduli of all of the residue classes in Ω divide m^2. Counting the residue classes of R which satisfy this requirement yields $|\Omega| \leqslant \sum_{t|m^2} |R/tR| < \infty$. Assume that the orbit Ω contains two residue classes which intersect nontrivially, i.e. that there is an $\tilde{r}(\tilde{m}) \in \Omega$ and a $g \in G$ such that $\tilde{r}(\tilde{m})^g \cap \tilde{r}(\tilde{m}) \notin \{\emptyset, \tilde{r}(\tilde{m})\}$. Further assume that $g|_{\tilde{r}(\tilde{m})}$ is given by $n \mapsto (an + b)/c$ for certain $a, b, c \in R$. Then, Lemma 1.1.8, Assertion (3) tells us that at

least one of the coefficients a, c is not a unit. Finally, Lemma 1.1.8, Assertion (2) yields a contradiction to the finiteness of Ω. □

2.5.2 Definition Let $\mathcal{P}$ be a partition of R into finitely many residue classes. We say that an rcwa group $G < \mathrm{RCWA}(R)$ *respects* the partition $\mathcal{P}$, if it naturally acts on $\mathcal{P}$ as a permutation group, and if all restrictions of elements of G to residue classes in $\mathcal{P}$ are affine. We say that a mapping $\sigma \in \mathrm{RCWA}(R)$ *respects* the partition $\mathcal{P}$, if the cyclic group generated by σ does so.

In this situation, we denote the permutation which is induced by σ on $\mathcal{P}$ by $\sigma_{\mathcal{P}}$. Similarly, we denote the permutation group which is induced by G on $\mathcal{P}$ by $G_{\mathcal{P}}$.

We take the symbol $\mathrm{Sym}(\mathcal{P})$ to denote an arbitrary rcwa group which respects the partition $\mathcal{P}$ and acts on it as full symmetric group. Accordingly, we write $\mathrm{Sym}(\mathcal{P}) < G$ to denote that G has a subgroup which respects the partition $\mathcal{P}$ and acts on it as full symmetric group.

Let S be a set of sets. Then we denote the union of the elements of S by $\cup S$. Analogously, we denote the intersection of the elements of S by $\cap S$.

2.5.3 Example Let $g, h \in \mathrm{RCWA}(\mathbb{Z})$ be the permuttions of order 7 resp. 12 defined in Example 1.6.3. They are given by

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

The group $G := \langle g, h \rangle$ respects the partition

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

of $\mathbb{Z}$, and we have

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

The order of $G_{\mathcal{P}}$ is $322560 = 2^{10} \cdot 3^2 \cdot 5 \cdot 7$, and the derived subgroup $G'_{\mathcal{P}}$ is perfect and has index 2. The kernel of the action of G on $\mathcal{P}$ is a free abelian group of rank 6. The computations for this and all following examples have been carried out using GAP [GAP04] and RCWA [Koh05].

2.5.4 Lemma *A tame rcwa group $G < \mathrm{RCWA}(R)$ is integral if and only if it respects the partition $R/\mathrm{Mod}(G)R$ of R.*

Proof: Let $m := \mathrm{Mod}(G) \neq 0$ and choose an arbitrary element $g \in G$. It is sufficient to show that the mapping g is integral if and only if it permutes the residue classes (mod m). The latter assertion holds since by Lemma 1.1.8, Assertion (1) the image of a residue class (mod m) under an affine mapping $\alpha \in \mathrm{AFF}(K)$ is a residue class (mod m) as well if and only if $\alpha \in \mathrm{AFF}(R)$. □

2.5.5 Example Let $m \in \mathbb{N}$ and let φ_m as in Theorem 2.1.2. Then Lemma 2.5.4 tells us that the group $G := \mathrm{S}_m{}^{\varphi_m}$ respects the partition

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

Further it holds $G_{\mathbb{Z}/m\mathbb{Z}} \cong \mathrm{S}_m$, hence the action of G on $\mathbb{Z}/m\mathbb{Z}$ is faithful.

2.5.6 Lemma *Let $G, H < \mathrm{RCWA}(R)$ be rcwa groups, let $\mathcal{P}$ be a partition of R which is respected by G and H and let $\sigma \in \mathrm{RCWA}(R)$ be affine on any element of $\mathcal{P}$. Then the following hold:*

1. *The group $\langle G, H\rangle < \mathrm{RCWA}(R)$ respects $\mathcal{P}$ as well.*
2. *The group G^σ respects the partition $\mathcal{P}^\sigma$, and the groups $G_\mathcal{P}$ and $G^\sigma_{\mathcal{P}^\sigma}$ are permutation isomorphic to each other.*

Proof:

1. By assumption, all elements of G and all elements of H permute the residue classes in the partition $\mathcal{P}$, and are furthermore affine on all residue classes in $\mathcal{P}$. This implies the same for arbitrary products of elements of G with elements of H, or in different words, for arbitrary elements of the subgroup of $\mathrm{RCWA}(R)$ which is generated by G and H.
2. We have assumed that $\sigma \in \mathrm{RCWA}(R)$ is affine on any element of $\mathcal{P}$. Hence by Lemma 1.1.8, Assertion (1), $\mathcal{P}^\sigma$ is also a partition of R into single residue classes. The group G^σ acts on it, and even respects it due to our assumption concerning σ. The mapping σ induces a permutation isomorphism from $G_\mathcal{P}$ to $G^\sigma_{\mathcal{P}^\sigma}$. □

2.5.7 Example We consider the group G which is given in Example 2.5.5. The mapping $\nu : n \mapsto n+1$ has infinite order, and $\varsigma : n \mapsto -n$ is not class-wise order-preserving. Since the group G is finite and class-wise order-preserving, it contains neither ν nor ς. The group $H := \langle \nu, \varsigma\rangle$ respects the partition $\mathbb{Z}/m\mathbb{Z}$ as well. By Lemma 2.5.6, Assertion (1) the same holds for the group $\langle G, H\rangle$ generated by G and H.

The following theorem will turn out to be important for obtaining a classification of those groups which have faithful tame rcwa representations over R:

2.5.8 Theorem *A group $G < \mathrm{RCWA}(R)$ is tame if and only if it respects a partition of R into finitely many residue classes.*

Proof: First assume that G is tame. Let $m := \mathrm{Mod}(G)$ and denote the residue classes (mod m) by $r_i(m)$, $i = 1, \ldots, |R/mR|$. We construct the desired partition $\mathcal{P}$ of R using the following algorithm:

1. Put $i := 1$ and $\mathcal{P} := \emptyset$.
2. If $r_i(m) \not\subseteq \cup\mathcal{P}$, put $D := r_i(m) \setminus \cup\mathcal{P}$, otherwise continue with step 4.
3. By Lemma 1.1.9, the set D is a union of finitely many residue classes. Put $\tilde{m} := \mathrm{lcm}(m, \mathrm{Mod}(D))$, and assume that $D = \tilde{r}_1(\tilde{m}) \cup \cdots \cup \tilde{r}_k(\tilde{m})$. For $j = 1, \ldots, k$, put $\mathcal{P} := \mathcal{P} \cup \tilde{r}_j(\tilde{m})^G$ – by Lemma 2.5.1, the orbits of the residue classes $\tilde{r}_j(\tilde{m})$ under the action of G are finite sets of disjoint single residue classes.
4. If $i < |R/mR|$, put $i := i + 1$ and continue with step 2. Otherwise done.

We have to form at most $|R/mR| < \infty$ difference sets D, and all of them are unions of finitely many residue classes. Further the orbits of the residue classes in these unions are finite as well. This yields $|\mathcal{P}| < \infty$.

Proving the other direction is trivial, since obviously the modulus of the group divides the least common multiple of the moduli of the residue classes in a respected partition. □

2.5.9 Remark By Theorem 2.5.8, a tame group $G < \mathrm{RCWA}(R)$ respects a partition $\mathcal{P}$ of R. If the action of G on R is transitive, then $\mathcal{P}$ is a block system. Hence the action of G on R is imprimitive, thus at most 1-transitive. Using Corollary 2.1.6, we can conclude that a nontrivial tame group cannot be a normal subgroup of $\mathrm{RCWA}(R)$.

2.5.10 Corollary *A mapping $\sigma \in \mathrm{RCWA}(R)$ is tame if and only if there is a $k \in \mathbb{N}$ such that σ^k is integral.*

Proof: First assume that $\sigma \in \mathrm{RCWA}(R)$ is tame. Then, Theorem 2.5.8 tells us that the cyclic group $\langle\sigma\rangle$ respects a partition $\mathcal{P}$. If k is the order of the permutation which is induced by σ on $\mathcal{P}$, then σ^k fixes and respects the partition $\mathcal{P}$. We conclude that σ is tame. Proving the opposite direction is trivial. □

2.5.11 Example Let g, h and $\mathcal{P}$ be as in Example 2.5.3. Then we have $\mathrm{ord}((gh)_{\mathcal{P}}) = 20$. Accordingly, $(gh)^{20}$ fixes the partition $\mathcal{P}$, hence the mapping $(gh)^{20}$ is integral.

From Theorem 2.5.8 we can derive an easy criterion for deciding whether a given bijective rcwa mapping is wild:

2.5.12 Conclusion *Let $\sigma \in \mathrm{RCWA}(R)$ be not balanced. Then σ is wild.*

Proof: Assume that the mapping σ is not balanced, but tame. Then by Theorem 2.5.8, σ respects a partition $\mathcal{P}$ of R into finitely many residue classes. Since the mapping σ is not balanced, there is a prime element $p \in \mathbb{P}(R)$ which divides $\mathrm{Div}(\sigma)$, but not $\mathrm{Mult}(\sigma)$ or vice versa. Due to Lemma 1.3.1b, Assertion (3) and (4), without loss of generality we can assume the former. Using Lemma 1.1.8, Assertion (1), we conclude that there is a cycle $(r_0(m_0), \ldots, r_{l-1}(m_{l-1})) \subseteq \mathcal{P}$ such that $\exists i \in \{0, \ldots, l-1\} : \ p | (m_i / m_{(i+1) \bmod l})$, but $\nexists j \in \{0, \ldots, l-1\} : \ p | (m_{(j+1) \bmod l} / m_j)$. Obviously this yields a contradiction. □

2.5.13 Examples By Conclusion 2.5.12, the mappings α and ξ from Examples 1.1.3 are both wild. However, by far not all balanced bijections are tame – see e.g. the example

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

with $\nu : n \mapsto n+1$. In the same time, the mapping $\nu\nu^{\alpha}$ is an example of a product of tame mappings which itself is *not* tame.

In Conclusion 2.5.12, at least the condition that σ is surjective cannot simply be omitted – see the example $f \in \mathrm{Rcwa}(\mathbb{Z}), \ n \mapsto 2n$.

The knowledge about respected partitions we have assembled so far permits us to reveal a strong relationship between tame and integral rcwa groups:

2.5.14 Theorem *Assume that R has the strong residue class decomposability property. Then exactly those mappings $g \in \mathrm{RCWA}(R)$ and exacty those finitely generated groups $G < \mathrm{RCWA}(R)$ are tame which are conjugate to an integral mapping resp. group.*

Proof: It is sufficient to prove the assertion for rcwa groups. Due to Remark 1.8.2 and Lemma 1.8.3, Assertion (3), finitely generated rcwa groups which are conjugate to integral groups are tame. Hence it is sufficient to prove that tame rcwa groups are always conjugate to integral groups. Thus let $G < \mathrm{RCWA}(R)$ be tame. By Theorem 2.5.8, the group G respects a partition $\mathcal{P}$ of R into finitely many residue classes. Due to our condition on R, we can choose an $m \in R$ such that $|R/mR| = |\mathcal{P}|$. By Lemma 2.1.4, there is now a mapping $\sigma \in \mathrm{RCWA}(R)$ which is affine on all residue classes in $\mathcal{P}$ and which induces a bijection from $\mathcal{P}$ to R/mR. Lemma 2.5.6, Assertion (2) tells us that the group G^{σ} respects the image of this bijection, and Lemma 2.5.4 reveals that G^{σ} is integral. □

2.5.15 Example Let G be the group from Example 2.5.3. As we have seen there, the group G respects a partition $\mathcal{P}_G$ of length 14. Just as described in the proof of Theorem 2.5.14, we can construct a mapping σ which maps the partition $\mathcal{P}_G$ onto the partition $\mathbb{Z}/14\mathbb{Z} = \{0(14), \ldots, 13(14)\}$:

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

Then G^σ is integral, and we have $\mathrm{Mod}(G^\sigma) = 14$.

Once we know how orbits under the action of affine groups look like, it is straightforward to give a description of the orbits under the action of tame rcwa groups on the underlying ring:

2.5.16 Theorem *Let $G < \mathrm{RCWA}(R)$ be tame and let $\Omega \subseteq R$ be an orbit on R under the action of G. Then there is a residue class $r(m) \subseteq R$ and a subgroup $U \leqslant \mathrm{AFF}(R)$ which acts on $r(m)$, such that Ω is the union of the images of an orbit of U on $r(m)$ under finitely many non-constant affine mappings.*

Proof: By Theorem 2.5.8, there is a partition $\mathcal{P}$ of R into finitely many residue classes such that G acts naturally on $\mathcal{P}$ and such that the restriction of an arbitrary element of G to one of the elements of $\mathcal{P}$ is always affine. Let N be the kernel of the action of G on $\mathcal{P}$. Due to Lemma 2.1.3, the group N acts on an arbitrary residue class in $\mathcal{P}$ as a subgroup of $\mathrm{AFF}(R)$. The quotient G/N is isomorphic to a subgroup of $\mathrm{Sym}(\mathcal{P})$, hence in particular finite. Thus any orbit of N on R has only finitely many images under elements of G. Due to the choice of $\mathcal{P}$, this yields the claimed assertion. □

In case $R = \mathbb{Z}$ this has the following consequences:

2.5.17 Conclusion The orbits under the action of subgroups of

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

on residue classes of $\mathbb{Z}$ are either sets of cardinality 1 or 2 or unions of one or two residue classes. Thus Theorem 2.5.16 tells us that an orbit on $\mathbb{Z}$ under the action of a tame group is either finite or a union of finitely many residue classes.

In general, the orbits on R under the action of a tame group can be computed easily. In particular, it is usually easy to decide whether a given tame group acts transitively on the underlying ring. We would like to illustrate this by giving an example:

2.5.18 Example Using RCWA , it is easy to check that the group $G = \langle g, h \rangle$ from Example 2.5.3 acts transitively on $\mathbb{Z}$. For example the cyclic group $\langle [g,h] \rangle$ acts transitively on the residue class $2(6)$, the orbit of this residue class under the action of G is

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

and the union of the 21 elements of Ω is $\mathbb{Z}$. By the way, it should be remarked that the action of G on Ω is primitive and that the induced permutation group is isomorphic to S_7.

2.6 Tame rcwa Representations of Groups

The following theorem gives a complete classification of those groups which have faithful tame rcwa representations over R. In order to prove the existence of such representations of the respective groups, we use an enhanced version of the construction which is shown in Theorem 2.1.2. The proof of the other direction, i.e. that indeed all tame rcwa groups have the given structure, is based on the use of respected partitions.

2.6.1 Theorem *A group G has a faithful tame rcwa representation over R if and only if there is an $m \in \mathbb{N}$ such that G is isomorphic to a subgroup of the wreath product* $\mathrm{AFF}(R) \wr \mathrm{S}_m$.

Proof:

a) We have to show that a subgroup of $\mathrm{AFF}(R) \wr \mathrm{S}_m$, $m \in \mathbb{N}$ has always a tame rcwa representation over R. Obviously it is sufficient to construct such a representation of the group $\mathrm{AFF}(R) \wr \mathrm{S}_m$ itself. We choose $a \in R \setminus (R^\times \cup \{0\})$, and set

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

and

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

Then we have already $\langle \sigma, \tau \rangle \cong \mathrm{S}_m$, since an m-cycle and a transposition on the partition $\mathcal{P}$ of $R \setminus 0(a^m)$ into the sets $S_k := \{n \in R \mid a^k | n,\ a^{k+1} \nmid n\}$, $k = 0, \ldots, m-1$ generate the full symmetric group on $\mathcal{P}$. Now we have to 'incorporate' the affine group of R. For this purpose we make use of the monomorphism

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

where $\alpha(u, k)$ is given by

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

(cp. Lemma 2.1.3). The support of the image of ϕ is S_0. This is one of the m sets which are permuted by $\langle \sigma, \tau \rangle$. Consequently we have $\langle \sigma, \tau, \alpha(u, k) \rangle \cong \mathrm{AFF}(R) \wr \mathrm{S}_m$, where u runs through a set of generators of $R^\times$ and k runs through a set of generators of $(R, +)$.

Further we see that the modulus of this group is a^m, hence that it is indeed tame.

b) Let $G < \mathrm{RCWA}(R)$ be tame. We have to show that there is an $m \in \mathbb{N}$ such that G is isomorphic to a subgroup of $\mathrm{AFF}(R) \wr \mathrm{S}_m$. By Theorem 2.5.8, there is a partition $\mathcal{P}$ of R into finitely many residue classes, such that G acts naturally on $\mathcal{P}$ as a permutation group, and that the restriction of an element of G to an element of $\mathcal{P}$ is always affine. The kernel of the action of G on $\mathcal{P}$ is obviously isomorphic to a subgroup of $\mathrm{AFF}(R)^{|\mathcal{P}|}$. Hence G itself is isomorphic to a subgroup of $\mathrm{AFF}(R) \wr \mathrm{S}_{|\mathcal{P}|}$, as claimed. □

In order to handle the case $\mathrm{char}(R) \neq 0$ as well, we have built the construction of a faithful representation of S_m in the first part of the proof upon the multiplicative instead of upon the additive structure of R. In Theorem 2.1.2 we have used the 1 as a non-torsion element of $(R,+)$. Here we have used a non-torsion element a of the monoid $(R,\cdot)$ instead.

Theorem 2.6.1 gives rise to a method for determining matrix representations of tame groups over K. Before discussing this, we have to introduce some notation which will sometimes be useful in the sequel:

2.6.2 Definition In the following, we call the faithful representation

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

the *standard representation* of $\mathrm{AFF}(K)$.

2.6.3 Corollary *Any tame group $G < \mathrm{RCWA}(R)$ has a faithful matrix representation over K.*

Proof: By Theorem 2.6.1, any tame group $G < \mathrm{RCWA}(R)$ is isomorphic to a subgroup of $\mathrm{AFF}(R) \wr \mathrm{S}_m$ for sufficiently large m. Hence it is sufficient to show that the group $\mathrm{AFF}(R) \wr \mathrm{S}_m$ itself has a faithful matrix representation over K. It is well-known that $\mathrm{AFF}(R)$ has a faithful K-representation of degree 2 (cp. Definition 2.6.2) and that S_m has one of degree m – for example take the 'natural' representation via permutation matrices. Hence the obvious bijection from the wreath product of these groups to the group of all $2m \times 2m$ block permutation matrices whose nonzero blocks lie in the image of the standard representation of $\mathrm{AFF}(R)$ is the desired faithful representation. □

2.6.4 Example The group G in Example 2.5.3 respects a partition of length 14. Hence it has a faithful matrix representation of degree $2 \cdot 14 = 28$ over $\mathbb{Q}$.

In conjunction with Theorem 2.6A in [DM96], Theorem 2.6.1 permits the following conclusion:

2.6.5 Corollary Let $k \in \mathbb{N}$. Then a finite extension $G \trianglerighteq N$ of a subgroup $N \leqslant \mathrm{AFF}(R)^k$ can always be embedded into $\mathrm{AFF}(R) \wr \mathrm{S}_m$, provided that m is at least equal to the product of k and the least degree of a faithful permutation representation of G/N. Hence such a group has always a tame rcwa representation over R.

Over certain rings, finitely generated tame rcwa groups are even finite:

2.6.6 Corollary *If finitely generated subgroups of* $\mathrm{AFF}(R)$ *are finite, then finitely generated tame rcwa groups* $G < \mathrm{RCWA}(R)$ *are finite as well.*

Proof: If finitely generated subgroups of $\mathrm{AFF}(R)$ are even finite, then the same holds for finitely generated subgroups of $\mathrm{AFF}(R) \wr \mathrm{S}_m$ for any $m \in \mathbb{N}$: Assume that there would be an infinite finitely generated subgroup. Then the kernel N of the action of this subgroup on the set of the m blocks would have finite index, hence would be infinite as well. However, according to Theorem 1.6.11 in [Rob96], N would also be finitely generated. Since not all projections of the infinite group N onto one of the m blocks can be finite, this yields a contradiction. Using Theorem 2.6.1 completes the proof. □

The polynomial rings $\mathbb{F}_q[x]$ satisfy the requirements of Corollary 2.6.6. This holds since they have nonzero characteristic, since their group of units is finite and since the partition which is induced by the degree mapping is invariant under multiplication with units. Obviously, Corollary 2.6.6 is not applicable to rings of characteristic 0 – on these for example the tame mapping $\nu : n \mapsto n + 1$ has infinite order.

In the following, we would like to classify the rcwa representations of certain 'suitable' groups over R up to conjugation:

2.6.7 Theorem *Assume that* R *has the weak residue class decomposability property. Further suppose that* G *is a finite group whose order is coprime to the orders of the torsion elements of* $\mathrm{AFF}(R)$*. Then the rcwa representations of the group* G *over* R *are parametrized up to conjugacy by the nonempty subsets of the set of all equivalence classes of its transitive finite-degree permutation representations.*

Proof: We have to show that there is a one-to-one correspondence between conjugacy classes of rcwa representations of G over R and sets of non-equivalent transitive finite-degree permutation representations of G. Since G is finite we only have to consider tame representations. Let $\varphi_i : G \to H_i < \mathrm{RCWA}(R),\ i \in \{1, 2\}$ be such representations, and let $\mathcal{P}_1$ and $\mathcal{P}_2$ be respected partitions of H_1 resp. H_2 (cp. Theorem 2.5.8).

In the following, let $i \in \{1, 2\}$. Due to the coprimality condition and due to the finiteness of G, the kernel of the action of H_i on $\mathcal{P}_i$ is trivial. Hence we have $(H_i)_{\mathcal{P}_i} \cong H_i$. Let $\Omega_{i,j}$ be the orbits of $(H_i)_{\mathcal{P}_i}$ on $\mathcal{P}_i$, and let $H_{i,j}$ be the transitive permutation groups which are induced by H_i on $\Omega_{i,j}$. Since the action of H_i on $\mathcal{P}_i$ is faithful, the groups $H_{i,j}$ induce on the sets $\cup\Omega_{i,j} \subseteq R$ infinite series of finite permutation groups which are permutation-isomorphic to $H_{i,j}$. We have to show that H_1 and H_2 are conjugate in $\mathrm{RCWA}(R)$ if and only if the sets of pairwisely not permutation-isomorphic groups $H_{1,j}$ and $H_{2,j}$ are the same.

This condition is obviously necessary, since non-isomorphic permutation groups are not even conjugate in the full symmetric group $\mathrm{Sym}(R)$. This means that the correspondence

to be established is at least well-defined, if read from the left to the right. In order to check that the condition is also sufficient, we have to think about how different numbers of mutually permutation-isomorphic groups $H_{1,j}$ and $H_{2,j}$ can be 'conjugated one upon the other'. For this purpose we refine the partitions $\mathcal{P}_i$ as follows, to obtain partitions $\tilde{\mathcal{P}}_i$ which are respected by the groups H_i as well and such that the groups $(H_i)_{\tilde{\mathcal{P}}_i}$ are permutation-isomorphic:

1. Let $\mathcal{H}_i$ be the set of the groups $H_{i,j}$, and initialize $\tilde{\mathcal{P}}_i$ by $\mathcal{P}_i$.
2. Choose an $H_{1,j} \in \mathcal{H}_1$.
3. Let $j_{i,1}, \ldots, j_{i,k_i}$ be the indices of the groups in $\mathcal{H}_1 \cup \mathcal{H}_2$ with are permutation-isomorphic to $H_{1,j}$. If $k_1 = k_2$, continue with step (5).
4. Put $t_i := \mathrm{lcm}(k_1, k_2)/k_i$, and for any $\Omega \in \{\Omega_{i,j_{i,1}}, \ldots, \Omega_{i,j_{i,k_i}}\}$ do the following:
   - Choose a residue class $r(m) \in \Omega$.
   - Write $r(m)$ as a disjoint union of t_i residue classes $r_1(m_1), \ldots, r_{t_i}(m_{t_i})$ – this is possible due to the condition that R has the weak residue class decomposability property.
   - Put $\tilde{\mathcal{P}}_i := \tilde{\mathcal{P}}_i \setminus \Omega$.
   - For $l \in \{1, \ldots, t_i\}$ put $\tilde{\mathcal{P}}_i := \tilde{\mathcal{P}}_i \cup r_l(m_l)^{H_i}$.

   Obviously, the groups H_i still respect the partitions $\tilde{\mathcal{P}}_i$. Since the kernel of the action of H_i on $\mathcal{P}_i$ is trivial, furthermore the permutation isomorphy types of the transitive permutation groups induced on subsets of these partitions remain invariant.

   Now, H_1 induces on $\tilde{\mathcal{P}}_1$ the same number $\mathrm{lcm}(k_1, k_2)$ of images which are permutation-isomorphic to $H_{1,j}$ as H_2 does on $\tilde{\mathcal{P}}_2$.
5. Put $\mathcal{H}_i := \mathcal{H}_i \setminus \{H_{i,j_{i,1}}, \ldots, H_{i,j_{i,k_i}}\}$.
6. If $\mathcal{H}_i \neq \emptyset$, continue with step (2), otherwise done.

Due to Lemma 2.1.4 and Lemma 2.5.6, Assertion (2) there is a $\sigma \in \mathrm{RCWA}(R)$ such that H_1^σ respects the partition $\tilde{\mathcal{P}}_2$, and such that $(H_1^\sigma)_{\tilde{\mathcal{P}}_2}$ is permutation-isomorphic to $(H_1)_{\tilde{\mathcal{P}}_1}$. The groups $(H_1^\sigma)_{\tilde{\mathcal{P}}_2}$ and $(H_2)_{\tilde{\mathcal{P}}_2}$ are now conjugate in in $\mathrm{Sym}(\tilde{\mathcal{P}}_2) < \mathrm{RCWA}(R)$. This means that also $(H_1)_{\tilde{\mathcal{P}}_1}$ and $(H_2)_{\tilde{\mathcal{P}}_2}$ are conjugate in $\mathrm{RCWA}(R)$. Due to the faithfulness of their action on the given respected partitions, the groups H_1 and H_2 are conjugate in $\mathrm{RCWA}(R)$ as well. This shows the injectivity of our correspondence.

It is always possible to embed a direct product of transitive finite-degree permutation groups into $\mathrm{Sym}(\mathcal{P}) < \mathrm{RCWA}(R)$ without fixed points, provided that its degree equals the cardinality of $\mathcal{P}$. Due to the condition that R has the weak residue class decomposability property, there is always a partition $\mathcal{P}$ of R of suitable length. Thus our correspondence is surjective as well. □

2.6.8 Example We would like to count the equivalence classes of rcwa representations of the non-abelian group G_{21} of order 21 over $\mathbb{Z}$. The faithful transitive permutation representations of this group are the regular representation of degree 21 and a representation of degree 7 on the cosets of a cyclic subgroup of order 3. Further there is a transitive representation of degree 3, whose kernel is the normal subgroup of G_{21} of order 7. Finally as always there is of course the trivial representation. Thus there are in total 4 non-equivalent transitive permutation representations. Since a set of cardinality 4 has exactly $2^4 - 1 = 15$ nonempty subsets, we conclude from Theorem 2.6.7 that the number of non-equivalent rcwa representations of G_{21} over $\mathbb{Z}$ equals 15. The faithful ones are (not in general, but in this case) the ones which belong to those sets which contain at least one of the faithful representations. These sets can be counted easily – there are exactly 12 of them. Of course instead of $\mathbb{Z}$ we could also have taken any other base ring which satisfies the conditions of the theorem, hence e.g. $\mathbb{F}_2[x]$ or $\mathbb{Z}_{(2)}$, and would have gotten the same results.

2.7 Conjugacy Classes of RCWA(R)

The following corollary of Theorem 2.6.7 tells us the number of conjugacy classes of RCWA(R) of elements of a given finite order:

2.7.1 Corollary *(Number of conjugacy classes of torsion elements in* RCWA(R)*.) Assume that the ring R has the weak residue class decomposability property, and let $r \in \mathbb{N}$. Then the following hold:*

a) *If the ring R has a torsion unit whose order is not coprime to r, then* RCWA(R) *has infinitely many conjugacy classes of elements of order r.*

b) *If r is coprime to the orders of all torsion elements of* AFF(R)*, then* RCWA(R) *has exactly as many conjugacy classes of elements of order r as there are subsets of the set of divisors of r whose least common multiple is r.*

Proof:

a) It is sufficient to describe how to construct an rcwa mapping of order r which has exactly a given number k of fixed points. We can even restrict ourselves to those k which are one more than the cardinality of a suitably chosen residue class ring of R. In this context we recall that permutations with different numbers of fixed points are not even conjugate in the full symmetric group.

   Let $u \neq 1$ be a torsion unit of R whose order divides r. Further let $a \in R \setminus (R^\times \cup \{0\})$.

We choose $m \in R$ such that $|R/mR| = k-1$, and set

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

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

The permutation σ_u has the same order as u. Its fixed points are the $k-1$ elements of $\mathfrak{R}(m)$. The permutation σ_r has order r, and the single fixed point 0.

Now let $f_1, f_2 \in \mathrm{Rcwa}(R)$ be injective mappings, whose images form a partition of the ring R – such mappings exist by Lemma 2.1.4. Since we have $\mathrm{ord}(u)|r$, the mapping $\sigma := \sigma_u^{\pi_{f_1}} \cdot \sigma_r^{\pi_{f_2}}$ is a permutation of order r which has exactly k fixed points, as desired.

b) Here we can apply Theorem 2.6.7. This only requires using the well-known formula for the number of transitive permutation representations of cyclic groups. □

2.7.2 Conclusion By Corollary 2.7.1, the group RCWA($\mathbb{Z}$) has

- infinitely many conjugacy classes of elements of a given even order, but only
- finitely many conjugacy classes of elements of a given odd order.

If R has characteristic 0, Corollary 2.7.1 is always applicable. Over rings of characteristic p, it still covers the element orders which are not divisible by p.

2.8 More About Respected Partitions

In the preceding three sections, we have already seen that the concept of a respected partition plays a key role in the proofs of various assertions concerning the structure of rcwa groups.

In this section these investigations will be continued. Concretely, we will investigate how to take influence on the permutation which a tame mapping induces on a respected partition by choosing that partition suitably. This is interesting in the context of looking for normal subgroups of RCWA(R). Further we investigate under which conditions on R all tame mappings even have finite order. Finally we derive a criterion when there is a tame mapping which maps a given partition of R into finitely many residue classes onto a given other partition of R into the same number of residue classes.

First of all, we need a lemma concerning the refinability of respected partitions:

2.8.1 Lemma *Let $G < \mathrm{RCWA}(R)$ be tame, let $\mathcal{P}$ be a respected partition of G and let $t \in \mathbb{N}$ be the cardinality of a residue class ring of R. Then $\mathcal{P}$ can be refined to another respected partition $\tilde{\mathcal{P}}$ of G of length $t \cdot |\mathcal{P}|$.*

Proof: Due to the condition that R has a residue class ring of cardinality t, we can always write a residue class $r(m) \in \mathcal{P}$ as a union of t residue classes $r_1(\tilde{m}), \ldots, r_t(\tilde{m})$ with equal moduli. This yields a partition $\tilde{\mathcal{P}}$ of R into $t \cdot |\mathcal{P}|$ residue classes. Since G respects $\mathcal{P}$, the restrictions of the elements of G to residue classes $r(m) \in \mathcal{P}$ are all affine. Hence the images of the residue classes $r_1(\tilde{m}), \ldots, r_t(\tilde{m})$ in a partition of $r(m)$ under an element $g \in G$ form always a partition of the image of $r(m)$ under g into residue classes with equal moduli. We conclude that the group G acts on the partition $\tilde{\mathcal{P}}$ as well. □

It is obviously not true that two given tame groups have always a common tame supergroup. But we can show the following:

2.8.2 Lemma *If R has the strong residue class decomposability property, then two given tame groups $G, H < \mathrm{RCWA}(R)$ have always conjugate tame supergroups.*

Proof: Let $\mathcal{P}_G$ and $\mathcal{P}_H$ be respected partitions of G resp. H. Due to the condition that R has residue class rings of any nonzero finite cardinality, Lemma 2.8.1 tells us that $\mathcal{P}_G$ and $\mathcal{P}_H$ can be refined to respected partitions $\tilde{\mathcal{P}}_G$ and $\tilde{\mathcal{P}}_H$ of G of the same length $l := \mathrm{lcm}(|\mathcal{P}_G|, |\mathcal{P}_H|)$. By Lemma 2.1.4, there is a mapping $\sigma \in \mathrm{RCWA}(R)$ which is affine on any element of $\tilde{\mathcal{P}}_G$, such that $\tilde{\mathcal{P}}_G^{\sigma} = \tilde{\mathcal{P}}_H$. If we set $\tilde{G} := G^{\sigma}$ and $\tilde{H} := H^{\sigma^{-1}}$, then by Lemma 2.5.6, Assertion (2) the group $\tilde{G}$ respects the partition $\tilde{\mathcal{P}}_H$ and the group $\tilde{H}$ respects the partition $\tilde{\mathcal{P}}_G$. By Lemma 2.5.6, Assertion (1), the two groups $\hat{G} := \langle G, \tilde{H} \rangle > G$ and $\hat{H} := \langle \tilde{G}, H \rangle > H$ respect the partitions $\tilde{\mathcal{P}}_G$ resp. $\tilde{\mathcal{P}}_H$ as well. Hence by Theorem 2.5.8 they are tame. Further we have $\hat{G}^{\sigma} = \hat{H}$. □

An immediate consequence is the following:

2.8.3 Conclusion Assume that the ring R has the strong residue class decomposability property, and let $g, h \in \mathrm{RCWA}(R)$ be tame. Then there is a $\sigma \in \mathrm{RCWA}(R)$ such that the group generated by g and h^{σ} is tame, thus in particular that the mapping $g \cdot h^{\sigma}$ is tame.

2.8.4 Remark It it not easily possible to assign a sign to a tame rcwa mapping g. A simple-minded idea would be just to set the sign of g equal to the sign of the induced permutation on a respected partition.

The problem with this is that the respected partition is not determined uniquely. Often a tame mapping respects partitions on which it induces odd permutations as well as partitions on which it induces even permutations.

For example, the mapping $\nu \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto n+1$ respects the trivial partition and the partitions $\{0(2), 1(2)\}$ and $\{0(3), 1(3), 2(3)\}$ of $\mathbb{Z}$. The corresponding induced partitions are the identity, a transposition and a 3-cycle.

Anyway, we can prove the following lemma:

2.8.5 Lemma *Assume that* $\mathrm{char}(R) = 0$*, that* R *has the weak residue class decomposability property and that the exponent of the group of units of* R *is finite. Then for any tame mapping* $\sigma \in \mathrm{RCWA}(R)$ *of infinite order there is an* $e \in \mathbb{N}$ *and a respected partition* $\mathcal{P}$ *of* σ^e *on which* σ^e *induces a transposition. Given* $l \in \mathbb{N}$*, it is further possible to choose* e *and* $\mathcal{P}$ *such that* $|\mathcal{P}| \geqslant l$*.*

Proof: By Theorem 2.5.8 and Lemma 2.8.1, the mapping σ respects a partition $\tilde{\mathcal{P}}$ of length $\geqslant l$. Let $e_1 := \mathrm{ord}(\sigma_{\mathcal{P}})$, $e_2 := \exp(R^\times)$ and $e := e_1 \cdot e_2$. Then σ^{e_1} respects and fixes the partition $\tilde{\mathcal{P}}$. Hence by Lemma 2.1.3, the affine partial mappings of σ^{e_1} on the residue classes $r(m) \in \tilde{\mathcal{P}}$ have the form $n \mapsto u_r n + r(1-u_r) + \tilde{k}_r m$ for some $u_r \in R^\times$ and $\tilde{k}_r \in R$. By computing powers in $\mathrm{AFF}(R)$, we see that the affine partial mappings of $\sigma^e = \sigma^{e_1 e_2}$ on the same residue classes have the form $n \mapsto n + k_r m$ with $k_r \in R$. Due to $\mathrm{ord}(\sigma) = \infty$ we have $\sigma^e \neq 1$. Hence we can choose a residue class $r(m) \in \tilde{\mathcal{P}}$ such that $k_r \neq 0$. Now $\tilde{\mathcal{P}}$ can be refined to a new partition $\mathcal{P}$ which is respected by σ^e as well. We do this as follows: Firstly, we choose a residue class $r(m) \in \tilde{\mathcal{P}}$ and split it into residue classes (mod $k_r m$). Secondly, we further split one of the latter residue classes into two residue classes. This is possible due to the condition that R has the weak residue class decomposability property. By Lemma 1.1.10, these two residue classes have necessarily the same modulus $\tilde{m}$ with $|R/\tilde{m}R| = 2 \cdot |R/k_r m R|$, since the only partition of 1 into exactly two fractions of the form $1/n$ is $1 = 1/2 + 1/2$. The affine partial mapping $n \mapsto n + k_r m$ maps the residue classes (mod k_r m) onto themselves and interchanges the two residue classes mentioned before. Since by construction the permutation $(\sigma^e)_{\mathcal{P}}$ fixes the 'rest' of $\mathcal{P}$, it induces a transposition on this partition as desired. □

It should be mentioned that the condition $\mathrm{char}(R) = 0$ has not been used anywhere in the proof. But this condition is redundant, i.e. leaving it away would not make the assertion anything stronger:

2.8.6 Theorem *Assume that* $\mathrm{char}(R) \neq 0$ *and* $\exp(R^\times) < \infty$*. Then all tame mappings* $\sigma \in \mathrm{RCWA}(R)$ *have finite order.*

Proof: Let $p := \mathrm{char}(R)$, let $\sigma \in \mathrm{RCWA}(R)$ be tame and let $\mathcal{P}$ be a respected partition of σ. Further let $e := \mathrm{ord}(\sigma_{\mathcal{P}}) \cdot \exp(R^\times)$. Then σ^e respects and fixes the partition $\mathcal{P}$, and the affine partial mappings of σ^e have the form $n \mapsto n + k \cdot \mathrm{Mod}(\sigma^e)$ for certain $k \in R$. We can immediately conclude that the affine partial mappings of $(\sigma^e)^p$ have the form $n \mapsto n + p \cdot k \cdot \mathrm{Mod}(\sigma^e) = n$, which completes the proof of our assertion. □

The construction used in the proof of Lemma 2.8.5 should be illustrated in an example:

2.8.7 Example Assume that the mappings g and h and the partition $\mathcal{P}$ are the same as in Example 2.5.3. The ring of integers obviously satisfies the conditions, and the product $\sigma := gh$ is a tame mapping of infinite order. Thus Lemma 2.8.5 can be applied to σ. Hence there is an $e \in \mathbb{N}$ and a refinement $\mathcal{P}'$ of $\mathcal{P}$ such that σ^e induces a transposition on $\mathcal{P}'$. An easy calculation yields $\mathrm{ord}(\sigma_{\mathcal{P}}) = 20 =: e_1$, and we have $\exp(\mathbb{Z}^\times) = 2 =: e_2$. Hence $e_1 e_2 = 40 =: e$. Another easy calculation shows that σ^e is given by

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

We now decide to split the residue class $3(12)$ into 4 residue classes (mod 48), and set $\mathcal{P}' := (\mathcal{P} \setminus \{3(12)\}) \cup \{3(48), 15(48), 27(48), 39(48)\}$. Further we choose among the residue classes (mod 48) the residue class $3(48)$ and split it into 2 residue classes (mod 96), thus we set $\mathcal{P}' := (\mathcal{P}' \setminus \{3(48)\}) \cup \{3(96), 51(96)\}$. Now we have

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

and the mapping σ^e induces on $\mathcal{P}'$ the transposition $(3(96), 51(96))$.

By Lemma 2.1.4, given two partitions of R into the same number of residue classes there is always a bijective rcwa mapping which maps the one onto the other. We would like to investigate under which circumstances the latter mapping can be chosen to be tame. The resulting condition can likely best be formulated using a property of certain weighted graphs:

2.8.8 Definition Let Γ be a finite simple graph with vertices $v_i,\ i \in \{1, \ldots, k\}$. Further assume that the vertices v_i have weights $n_i \in \mathbb{N}$. We call the graph Γ *balancable* if it is possible to reach a state in which all n_i are equal in a finite number of steps as follows:

1. Choose a pair of adjacent vertices (v_i, v_j) of Γ.

2. Put $n_i := n_i + 1$ and $n_j := n_j + 1$.

3. If not all n_i are equal then continue with step (1), otherwise done.

The author does not know whether the question if a given graph is balancable is algorithmically decidable or not.

2.8.9 Theorem *Assume that the ring R has the weak residue class decomposability property, let $k \in \mathbb{N}$ and let*

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

be partitions of R into k residue classes, each. Further let Γ be the bipartite graph with the $2k$ vertices $r_{i,j}(m_{i,j})$, where two of these are adjacent if and only if their intersection as sets is nonempty. Let m be the least common multiple of the moduli of the residue classes in $\mathcal{P}_1$ and $\mathcal{P}_2$. To the vertices $r_{i,j}(m_{i,j})$ of Γ, we assign the weights $n_{i,j} := |R/mR|/|R/m_{i,j}R|$. Assume that the graph Γ is balancable and that $G \leqslant \mathrm{RCWA}(R)$ is an rcwa group such that $\mathrm{Sym}(\mathcal{P}) < G$ for any partition $\mathcal{P}$ of R into a sufficiently large finite number of residue classes. Then there is a tame element $\sigma \in G$ such that $\mathcal{P}_1^\sigma = \mathcal{P}_2$.

Proof: Due to Lemma 2.1.4, Theorem 2.5.8 and Lemma 2.8.1 it is sufficient to show that the partitions $\mathcal{P}_1$ and $\mathcal{P}_2$ have a common refinement $\mathcal{P} = \{r_1(m_1), r_2(m_2), \ldots, r_l(m_l)\}$ such that for any j, the residue classes $r_{1,j}(m_{1,j})$ and $r_{2,j}(m_{2,j})$ are unions of the same number of residue classes $r_i(m_i)$ from $\mathcal{P}$. Let $m := \mathrm{lcm}_{i,j}\, m_{i,j}$. Now a vertex $r_{i,j}(m_{i,j})$ of Γ is the union of exactly $n_{i,j}$ residue classes (mod m). Since Γ is balancable and since R has the weak residue class decomposability property, the desired partition $\mathcal{P}$ can be obtained from the partition R/mR using the method described in Definition 2.8.8 – adding 1 to $n_{i,j}$ corresponds to splitting a residue class in $r_{i,j}(m_{i,j})$ into two disjoint other residue classes. Note in this context that the splitted residue class lies also in exactly one vertex $r_{3-i,\tilde{\jmath}}(m_{3-i,\tilde{\jmath}})$ of Γ adjacent to $r_{i,j}(m_{i,j})$. Note also that the vertex $r_{3-i,\tilde{\jmath}}(m_{3-i,\tilde{\jmath}})$ can be chosen freely among the vertices adjacent to $r_{i,j}(m_{i,j})$ by making a suitable choice of the residue class to be splitted. □

2.8.10 Example As a little example, we construct a tame mapping $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ such that $\mathcal{P}_1^\sigma = \mathcal{P}_2$, where $\mathcal{P}_1 := \{0(2), 1(4), 3(4)\}$ and $\mathcal{P}_2 := \{0(3), 1(3), 2(3)\}$. It is easy to see that in this example Γ is the complete bipartite graph with 6 vertices. The vertices $0(2), 1(4), 3(4), 0(3), 1(3), 2(3)$ of Γ have the weights $6, 3, 3, 4, 4, 4$ (cp. Theorem 2.8.9). We check that Γ is balancable by using the method given in Definition 2.8.8. For this we consecutively increment the weights for the pairs $(1(4), 0(3))$, $(1(4), 0(3))$, $(1(4), 1(3))$, $(3(4), 1(3))$, $(3(4), 2(3))$ and $(3(4), 2(3))$ of vertices of Γ. Further we have $m = \mathrm{lcm}(2,3,4) = 12$, thus we start with the partition $\mathbb{Z}/12\mathbb{Z}$. Refining the partitions $\mathcal{P}_1$ and $\mathcal{P}_2$ correspondingly yields

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

resp.

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

Decompositions of residue classes corresponding to the mentioned manipulations of the weights of the vertices of Γ are for example (in an order consistent with the above specifications)

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

This yields the partition

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

Now using Lemma 2.1.4 it is easy to construct a mapping σ which has the desired properties. We get e.g.

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

By the way, the mapping σ is not only tame but even has finite order – it is easy to check that $\mathrm{ord}(\sigma) = 30$. If we would not have required the resulting mapping to be tame, we simply could have taken the mapping α from Examples 1.1.3 – it is also $\mathcal{P}_1^\alpha = \mathcal{P}_2$.

2.9 The Group Generated by the Tame Mappings in RCWA(Z)

In the preceding sections we have investigated the structure of tame rcwa mappings and -groups. It is natural to ask for the structure of the subgroup N of $\mathrm{RCWA}(\mathbb{Z})$ which is generated by *all* tame mappings.

Due to Lemma 1.8.3 this subgroup is normal. In this section, an elegant set of generators of this normal subgroup will be given.

Apart from this, Collatz' permutation α from Examples 1.1.3 is factored into 73 factors from the mentioned set of generators and an integral mapping. This shows constructively that $\alpha \in N$.

2.9.1 Definition Let $\nu \in \mathrm{RCWA}(R) : n \mapsto n+1$, $\varsigma \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto -n$ and $\tau \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto n + (-1)^n$. Using the restriction monomorphisms introduced in Definition 2.3.1, we derive from these three mappings certain basic 'building blocks' for tame rcwa mappings:

1. Given a residue class $r(m)$ of R, we define the *class shift* $\nu_{r(m)} \in \mathrm{RCWA}(R)$ by $\nu^{\pi_{n \mapsto mn+r}}$.

2. Given a residue class $r(m)$ of $\mathbb{Z}$, we define the *class reflection* $\varsigma_{r(m)} \in \mathrm{RCWA}(\mathbb{Z})$ by $\varsigma^{\pi_{n \mapsto mn+r}}$.

3. Given two disjoint residue classes $r_1(m_1)$ and $r_2(m_2)$ of $\mathbb{Z}$, we define the *class transposition* $\tau_{r_1(m_1),r_2(m_2)} \in \mathrm{RCWA}(\mathbb{Z})$ by τ^{π_μ}, where

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

   maps the residue class $0(2)$ resp. $1(2)$ onto $r_1(m_1)$ resp. $r_2(m_2)$ (cp. Lemma 2.1.3).

To ensure uniqueness, in this context we always assume that for any residue class $r(m)$ we have $r \in \mathfrak{R}(m)$. In case $R = \mathbb{Z}$, let $\mathfrak{R}(m) := \{0, 1..m-1\}$.

2.9.2 Remark As can be seen easily and as is suggested by the terms, a class shift $\nu_{r(m)} \in \mathrm{RCWA}(R)$ and a class reflection $\varsigma_{r(m)} \in \mathrm{RCWA}(\mathbb{Z})$ are given by

$$n \longmapsto \begin{cases} n+m & \text{if } \ n \in r(m), \\ n & \text{otherwise,} \end{cases} \quad \text{resp.} \quad n \longmapsto \begin{cases} -n+2r & \text{if } \ n \in r(m), \\ n & \text{otherwise.} \end{cases}$$

A class transposition $\tau_{r_1(m_1),r_2(m_2)}$ is an involution which interchanges the disjoint residue classes $r_1(m_1)$ and $r_2(m_2)$. Concretely: It is

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

It is immediate that $\tau_{r_1(m_1),r_2(m_2)} = \tau_{r_2(m_2),r_1(m_1)}$.

Due to Corollary 2.3.3, the mappings $\nu_{r(m)}$, $\varsigma_{r(m)}$ resp. $\tau_{r_1(m_1),r_2(m_2)}$ distinct from ν, ς resp. τ are conjugate to all other members of the respective class. Thus if a normal subgroup of $\mathrm{RCWA}(\mathbb{Z})$ contains such a mapping, it already contains the whole class.

2.9.3 Theorem *All tame mappings in* $\mathrm{RCWA}(\mathbb{Z})$ *can be written as products of class shifts* $\nu_{r(m)}$*, class reflections* $\varsigma_{r(m)}$ *and class transpositions* $\tau_{r_1(m_1),r_2(m_2)}$*.*

Proof: Since finite symmetric groups are generated by transpositions and since the mappings $\nu_{r(m)}$ and $\varsigma_{r(m)}$ generate the largest subgroup of $\mathrm{AFF}(\mathbb{Z})$ which acts on the residue class $r(m)$, the assertion follows immediately from Theorem 2.5.8. □

An obvious consequence is the following:

2.9.4 Theorem The normal subgroup $N \trianglelefteq \mathrm{RCWA}(\mathbb{Z})$ is generated by class shifts, class reflections and class transpositions.

Hence the group N is in particular generated by images of the three mappings ν, ς and τ under restriction monomorphisms. Due to $\nu = (n \mapsto -n) \cdot (n \mapsto -n+1)$ this implies also that all elements of N can be written as products of involutions.

2.9.5 Example Let g be the mapping of order 7 given in Example 2.5.3. Then it is straightforward to check that $g = \tau_{0(6),1(6)} \cdot \tau_{0(6),5(6)} \cdot \tau_{0(6),3(6)} \cdot \tau_{0(6),4(6)} \cdot \tau_{1(3),2(6)}$ is a factorization of g into class transpositions.

On a first glance it looks like a plausible conjecture that the mappings $\nu_{r(m)}$, $\varsigma_{r(m)}$ and $\tau_{r_1(m_1),r_2(m_2)}$ would generate a balanced subgroup of $\mathrm{RCWA}(\mathbb{Z})$. This would imply that $N \neq \mathrm{RCWA}(\mathbb{Z})$. But the following example shows that N is *not* balanced:

2.9.6 Example Products of class transpositions are not necessarily balanced. Even more: multiplier and divisor of such a product can also be coprime. For example let $\sigma_1 := \tau_{1(6),0(8)} \cdot \tau_{5(6),4(8)}$, $\sigma_2 := \tau_{0(4),1(6)} \cdot \tau_{2(4),5(6)}$ and $\sigma_3 := \tau_{2(6),1(12)} \cdot \tau_{4(6),7(12)}$. Then it is

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

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

The mappings σ_1, σ_2 and σ_3 are involutions whose product is given by

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

This example yields

2.9.7 Remark The following hold:

- Balancedness is not a class invariant. For example $\sigma_1\sigma_2\sigma_3$ is not balanced, but it is $\mathrm{Mult}((\sigma_1\sigma_2\sigma_3)^{\sigma_2}) = \mathrm{Div}((\sigma_1\sigma_2\sigma_3)^{\sigma_2}) = 36$.

- Also wild mappings can be conjugate to their inverse via an involution. For example it is $(\sigma_1\sigma_2)^{\sigma_2} = (\sigma_1\sigma_2)^{-1}$, and it is easy to check that $\sigma_1\sigma_2$ is wild.

- The group $\langle \sigma_1, \sigma_2 \rangle$ is wild and isomorphic to D_∞. Hence the infinite dihedral group has a faithful wild rcwa representation over $\mathbb{Z}$.

It seems reasonable to conjecture that Definition 2.9.1 gives in fact a set of generators for the whole of RCWA($\mathbb{Z}$):

2.9.8 Conjecture It is $N = \mathrm{RCWA}(\mathbb{Z})$.

2.9.9 Example As mentioned above, the permutation α from Examples 1.1.3 has already been investigated by other people. Günther Wirsching [Wir96] for example cites an article of Jeffrey C. Lagarias [Lag85], which states that Lothar Collatz has mentioned the mapping α^{-1} in his notebook under the date July 1, 1932. Further he states that it would be unknown so far whether the cycle

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

of this permutation is finite or infinite.

Here we would like to factor the permutation α into the generators $\nu_{r(m)}$, $\varsigma_{r(m)}$ and $\tau_{r_1(m_1),r_2(m_2)}$ of the normal subgroup $N \trianglelefteq \mathrm{RCWA}(\mathbb{Z})$. The fact that all affine partial mappings of α have a factor 3 in their numerator and a power of 2 in their denominator makes factoring this mapping much harder than factoring a balanced mapping.

Let $\sigma_1, \sigma_2, \sigma_3$ be defined as in Example 2.9.6. If we set $\sigma := \sigma_1\sigma_2\sigma_3$ and

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

then $\alpha\theta^{-1}$ is integral, thus in particular tame. Hence according to Theorem 2.9.3, it is a product of mappings $\nu_{r(m)}$, $\varsigma_{r(m)}$ and $\tau_{r_1(m_1),r_2(m_2)}$. Now the given factorization of θ tells us that α can be written as a product of such mappings as well.

The mapping σ with multiplier 3 and divisor 2 plays a key role in this example, since a division of α by a suitable power of σ yields a quotient in which the powers of 2 and 3 are relatively evenly distributed on the numerators and denominators of the affine partial mappings. The next step in the construction was the elimination of the prime factor 3 from multiplier and divisor. The final step was the reduction of a mapping with multiplier 4, divisor 4 and modulus 288 to an integral mapping $\alpha\theta^{-1}$ of order 101616.

The above factorization of α has been obtained using a trial-and-error approach in multiple interactive sessions with the RCWA package. The task can be compared with solving the Rubik's Cube – the analogue to the moves of the latter are multiplications by class transpositions and class shifts. A major difference is that the Rubik's Cube is finite. This example has lead to the development of a general factorization method for elements of RCWA($\mathbb{Z}$) and its implementation in RCWA. This method so far has not been proven to terminate always, thus has not yet led to a proof of Conjecture 2.9.8.

Transpositions in finite symmetric groups cannot be written as commutators. For class transpositions in RCWA($\mathbb{Z}$) things look different:

2.9.10 Lemma *Class transpositions can be written as commutators. Thus in particular they are elements of* RCWA($\mathbb{Z}$)′.

Proof: It is easy to check that $\tau = [\tau_1, \tau_2]$, where

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

This decomposition can be transferred to a given class transposition $\tau_{r_1(m_1),r_2(m_2)}$ by switching to images under the restriction monomorphism associated to the mapping $\mu_{r_1(m_1),r_2(m_2)}$ from the definition of a class transposition in 2.9.1. □

The representation of τ as a commutator which is given in the proof of Lemma 2.9.10 can be obtained from the equation $(12)(34) = [(123), (124)]$ by switching to images under the rcwa representation φ_4 of S_4 given in Theorem 2.1.2.

There are not many possible values for the order of the commutator of two class shifts:

2.9.11 Lemma *Assume that* $\mathrm{char}(R) = 0$. *Then the following holds:*

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

Proof: Obviously we have $\mathrm{supp}([\nu_{r_1(m_1)}, \nu_{r_2(m_2)}]) \subseteq r_1(m_1) \cup r_2(m_2)$. The case that the residue classes $r_1(m_1)$ and $r_2(m_2)$ are either disjoint or equal is trivial. We consider the case that a proper subset relation holds. Without loss of generality we can assume that $r_1(m_1) \subsetneq r_2(m_2)$ – otherwise we simply switch to considering the inverse of the commutator. An easy calculation yields

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

hence due to our condition that $\mathrm{char}(R) = 0$ we are done. In the remaining case we set $r(m) := r_1(m_1) \cap r_2(m_2)$ and get

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

It is easy to check that this permutation has order 3. □

The attempt to obtain a comparable result for products of two class transpositions yields a larger amount of different cases which presently do not seem like being reasonably easy to distinguish. For example one gets mappings of different finite orders (vague conjecture: exactly those dividing 60, except of 5 – in any case, all of these orders are possible and no further ones have been found so far) and mappings of infinite order either with infinite cycles or only with finite cycles.

2.10 Conditions on Normal Subgroups of RCWA(R)

In this section we will derive conditions on normal subgroups of RCWA(R). In particular we will investigate whether a normal subgroup of RCWA(R) must have a nontrivial tame subgroup, and if so, how 'large' it must be.

First of all, we need the following lemmata:

2.10.1 Lemma *Let $\sigma \in \mathrm{RCWA}(R)$. Further let $m := \mathrm{Mod}(\sigma)$, and let $\nu \in \mathrm{RCWA}(R)$ be an integral mapping which respects and fixes the partition R/mR of R. Then the commutator $c := [\sigma, \nu]$ is integral.*

Proof: Let α be an arbitrary affine partial mapping of c. By definition and due to Lemma 2.1.3, the mapping α is the product of

- an affine partial mapping $\alpha_{\sigma^{-1}} : n \mapsto (c_1 n - b_1)/a_1$ of σ^{-1},
- an affine partial mapping $\alpha_{\nu^{-1}} : n \mapsto u_1 n + r_1(1 - u_1) + k_1 m$ of ν^{-1},
- an affine partial mapping $\alpha_\sigma : n \mapsto (a_2 n + b_2)/c_2$ of σ and
- an affine partial mapping $\alpha_\nu : n \mapsto u_2 n + r_2(1 - u_2) + k_2 m$ of ν

for certain coefficients $a_1, a_2, b_1, b_2, c_1, c_2, r_1, r_2, k_1, k_2 \in R$ and $u_1, u_2 \in R^\times$. Since the mapping ν respects and fixes the partition R/mR, we have $a_1 = a_2$, $b_1 = b_2$ and $c_1 = c_2$. Let φ be the standard representation of AFF(K). Since the determinant of a product of matrices is the product of the determinants of the factors, we have

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

Thus since $R^\alpha \cap R \neq \emptyset$ we also know that $\alpha \in \mathrm{AFF}(R)$. But this means that the mapping c is integral, as claimed. □

2.10.2 Lemma *In the situation of Lemma 2.10.1, the commutator $[\sigma, \nu\sigma]$ is tame.*

Proof: It is $[\sigma, \nu\sigma] = \sigma^{-1}(\nu\sigma)^{-1}\sigma\nu\sigma = \sigma^{-2}\sigma^\nu\sigma = (\sigma^{-1}\sigma^\nu)^\sigma = [\sigma, \nu]^\sigma$. We get the claimed assertion by Lemma 2.10.1 and Lemma 1.8.3, Assertion (1). □

2.10.3 Example Lemma 2.10.2 is the reason why the two commutators $[\alpha, \nu_{1(4)}\alpha]$ and $[\alpha, \nu_{3(4)}\alpha]$ in Examples 1.5.2 are tame.

There is no normal subgroup which except of 1 contains only wild elements:

2.10.4 Lemma *If $N \lhd \mathrm{RCWA}(R)$ is a nontrivial normal subgroup, then N contains an integral element $g \neq 1$.*

Proof: Let $\sigma \in N \setminus \{1\}$ and let $m := \mathrm{Mod}(\sigma)$. Without loss of generality we can assume that there is a residue class $r(m)$ such that $r(m)^\sigma \neq r(m)$ – otherwise σ already would be integral. Put $\nu := \nu_{r(m)}$ and $g := [\sigma, \nu] = \sigma^{-1}\sigma^\nu$. By definition of a normal subgroup, we have $g \in N$. Further since $r(m)^\sigma \neq r(m)$, it is $g \neq 1$. However by Lemma 2.10.1, the mapping g is integral. □

Furthermore, provided that the group $(R, +)$ is not periodic we can show that a normal subgroup must even have tame elements of infinite order:

2.10.5 Lemma *Assume that $\mathrm{char}(R) = 0$ and that $N \lhd \mathrm{RCWA}(R)$ is a nontrivial normal subgroup. Then N has an integral element g of infinite order.*

Proof: By Lemma 2.10.4, N has an integral element $\tilde{g} \neq 1$. Without loss of generality we can assume that $\mathrm{ord}(\tilde{g}) < \infty$ – otherwise g would already be the desired element. Put $m := \mathrm{Mod}(\tilde{g})$. By Lemma 2.5.4, the mapping $\tilde{g}$ respects the partition R/mR. We choose a residue class $r(m)$ such that $\tilde{g}|_{r(m)} \neq 1$, and set $\nu := \nu_{r(m)}$. Finally we set $g := [\tilde{g}, \nu] = \tilde{g}^{-1}\tilde{g}^\nu$. By definition of a normal subgroup, it is $g \in N$. Further since $\tilde{g}$ and ν are integral, g is integral as well. Lemma 2.5.6, Assertion (1) tells us that g respects the partition R/mR also. Hence it suffices to show that $r(m)^g = r(m)$ and that $\mathrm{ord}(g|_{r(m)}) = \infty$. We have to distinguish two different cases:

1. It is $r(m)^{\tilde{g}} = r(m)$. Then due to Lemma 2.1.3 the restriction $\tilde{g}|_{r(m)}$ is given by $n \mapsto un + r(1-u) + km$ for certain $k \in R$ and $u \in R^\times$. Given $n \in r(m)$ we have

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

   hence $n^g = n + (1-u)m \equiv r\ (m)$. Assume that we would have $u = 1$. Then by the choice of $r(m)$ at least k must be nonzero. This contradicts with the condition $\mathrm{char}(R) = 0$ and our assumption that $\mathrm{ord}(\tilde{g}) < \infty$. Thus we have $u \neq 1$. Since $\mathrm{char}(R) = 0$, the permutation g is the desired element.

2. It is $r(m)^{\tilde{g}} \neq r(m)$. In this case, given $n \in r(m)$ it holds that

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

   since $n^{\tilde{g}^{-1}} \notin r(m)$. Hence the affine partial mapping $g|_{r(m)}$ is given by $n \mapsto n + m$. Thus since $\mathrm{char}(R) = 0$, the permutation g is the desired element. □

By Lemma 2.8.5, a tame rcwa mapping of infinite order induces a transposition on a suitably chosen partition. Together with the preceding lemma we can conclude that a nontrivial normal subgroup of RCWA(R) must have 'pretty large' tame subgroups:

2.10.6 Theorem *Assume that* $\mathrm{char}(R) = 0$. *Further suppose that the exponent of the group of units of* R *is finite and that* R *has the weak residue class decomposability property. 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.*

Proof: Let $l' \in \mathbb{N}$ be arbitrary. By Lemma 2.10.5, N has an integral element g of infinite order. By Lemma 2.8.5 there is an exponent $e \in \mathbb{N}$ and a respected partition $\tilde{\mathcal{P}}$ of g^e such that $l' \leqslant |\tilde{\mathcal{P}}| =: l$, on which g^e induces a transposition. Since a finite symmetric group does not have a proper normal subgroup which contains a transposition, $\mathrm{Sym}(\tilde{\mathcal{P}}) < \mathrm{RCWA}(R)$ implies already $\mathrm{Sym}(\tilde{\mathcal{P}}) < N$. If $\mathcal{P}$ is an arbitrary partition of R into l residue classes, then by Lemma 2.1.4 there is a $\sigma \in \mathrm{RCWA}(R)$ such that $\tilde{\mathcal{P}}^\sigma = \mathcal{P}$. By Lemma 2.5.6, Assertion (2) this implies that $\mathrm{Sym}(\tilde{\mathcal{P}})^\sigma = \mathrm{Sym}(\mathcal{P})$. Due to the condition that N is a normal subgroup of RCWA(R), we can conclude that $\mathrm{Sym}(\mathcal{P}) < N$, as claimed. □

It should be emphasized that the theorem does *not* claim 'Then there is an $l_0 \in \mathbb{N}$ such that for any partition $\mathcal{P}$ of R into $l > l_0$ residue classes the following holds: ...'. Furthermore, so far we cannot tell anything about partitions of 'small' length in this context.

Theorem 2.10.6 shows by other means than Corollary 2.1.6 that the group RCWA($\mathbb{Z}$) does not have nontrivial solvable normal subgroups.

2.11 A Normal Subgroup of RCWA+(Z)

The group $\mathrm{RCWA}^+(\mathbb{Z})$ of class-wise order-preserving bijective rcwa mappings of $\mathbb{Z}$ has a nontrivial normal subgroup. In this section we will construct this normal subgroup as the kernel of an epimorphism from $\mathrm{RCWA}^+(\mathbb{Z})$ to $(\mathbb{Z}, +)$.

2.11.1 Definition Let $r(m)$ be a residue class and let $\alpha : n \mapsto (an + b)/c$ be an order-preserving affine mapping whose source is $r(m)$. We define the *determinant* of α by

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

Further we define the *determinant* of an rcwa mapping $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ with modulus m by the sum of the determinants of its affine partial mappings, i.e. it is

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

It is not intuitive that this yields an homomorphism. It is not even obvious that the determinant of an element $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ is always an integer. In fact, evaluating the above expression for an arbitrary rcwa mapping usually does not yield an integer – injectivity, surjectivity and class-wise order-preservingness are all crucial. The author got the idea to consider this mapping during computational investigations with RCWA.

2.11.2 Remark Let $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ and $m := \mathrm{Mod}(\sigma)$. As in the definition of an rcwa mapping, we denote the coefficients of σ by $a_{r(m)}$, $b_{r(m)}$ and $c_{r(m)}$, i.e. the restriction $\sigma|_{r(m)}$ of σ to a residue class $r(m) \in \mathbb{Z}/m\mathbb{Z}$ is given by $n \mapsto (a_{r(m)}n + b_{r(m)})/c_{r(m)}$. Then the following holds:

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

In the sequel it will turn out to be useful to consider residue classes with distinguished representatives:

2.11.3 Definition We denote a residue class $r(m)$ with distinguished representative r by $[r/m]$. The image $[r/m]^\alpha$ of such a residue class under an affine mapping α is defined as the residue class $r(m)^\alpha$ with distinguished representative r^α. Let $k \in \mathbb{N}$. We call a decomposition

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

of a residue class $[r/m]$ *representative stabilizing*.

Let $\mathcal{P}$ be a partition of $\mathbb{Z}$ into finitely many residue classes with distinguished representatives. We call a refinement of $\mathcal{P}$ *representative stabilizing* if it is obtained by representative stabilizing decomposition of residue classes in $\mathcal{P}$.

We assign rational numbers to residue classes with distinguished representatives:

2.11.4 Definition Given a residue class $[r/m]$, we set

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

Given a partition $\mathcal{P}$ of $\mathbb{Z}$ into finitely many residue classes with distinguished representatives we set

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

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

It has to be shown that $\delta(\mathbb{Z})$ is well-defined:

2.11.5 Lemma *The value $\delta(\mathbb{Z})$ is independent of the choice of the partition $\mathcal{P}$.*

Proof: We have to show that $\delta(\mathcal{P}) \bmod 1$ is invariant under representative stabilizing refinement of $\mathcal{P}$ as well as under changes of the distinguished representatives of the residue classes in $\mathcal{P}$. For a residue class $[r/m]$ and $k \in \mathbb{N}$, we have

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

It follows that $\delta(\mathcal{P})$ is invariant under representative stabilizing refinement of the partition $\mathcal{P}$. Furthermore, for a residue class $[r/m]$ and $k \in \mathbb{Z}$ we have

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

Hence changes of the choice of the distinguished representatives of the residue classes can change $\delta(\mathcal{P})$ only by an integer. □

2.11.6 Remark We can explicitly determine $\delta(\mathbb{Z})$ – it is $\delta(\mathbb{Z}) = \delta([0/1]) = 0/1 - 1/2 - \lfloor 0/1 - 1/2 \rfloor = 1/2$. However, we will not need this value in the sequel.

2.11.7 Definition Let $\sigma \in \mathrm{RCWA}(\mathbb{Z})$. We call a partition $\mathcal{P}$ of $\mathbb{Z}$ into finitely many residue classes with distinguished representatives a *base* for σ if all restrictions of σ to residue classes $[r/m] \in \mathcal{P}$ are affine.

2.11.8 Lemma Let $\alpha : n \mapsto (an+b)/c$ be an order-preserving affine mapping whose source is a residue class $[r/m]$. Then we have

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

Let $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$, and let $\mathcal{P}$ be a base for σ. From the above we get

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

and from this by inserting into the definition, that

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

Now we have all necessary prerequisites for being able to prove that the determinant mapping is indeed an epimorphism from $\mathrm{RCWA}^+(\mathbb{Z})$ to $(\mathbb{Z}, +)$:

2.11.9 Theorem *The mapping*

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

is an epimorphism.

Proof: Let $\sigma_1,\sigma_2,\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$. We have to show that $\det(\sigma)$ is an integer, that $\det(\sigma^{-1}) = -\det(\sigma)$, that $\det(\sigma_1\sigma_2) = \det(\sigma_1)+\det(\sigma_2)$, and that there is a class-wise order-preserving bijective rcwa mapping of $\mathbb{Z}$ with determinant 1.

1. We would like to show that $\det(\sigma) \in \mathbb{Z}$. By Lemma 2.11.8 we have

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

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

2. We would like to show that $\det(\sigma^{-1}) = -\det(\sigma)$. Let $m := \mathrm{Mod}(\sigma)$, and denote the coefficients of σ by $a_{r(m)}$, $b_{r(m)}$ and $c_{r(m)}$. By definition, the restriction of σ to a residue class $r(m)$ contributes the summand $b_{r(m)}/(m \cdot a_{r(m)})$ to the determinant of σ. The image of $r(m)$ under σ is $r^\sigma(m \cdot a_{r(m)}/c_{r(m)})$. Since we have $a_{r(m)} > 0$, the restriction of σ^{-1} to this residue class contributes the summand

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

   to the determinant of σ^{-1}. This in turn is the additive inverse of the contribution of $\sigma|_{r(m)}$ to the determinant of σ, and we get the claimed assertion.

3. We want to show that $\det(\sigma_1\sigma_2) = \det(\sigma_1) + \det(\sigma_2)$. Let $m := \mathrm{Mod}(\sigma_1) \cdot \mathrm{Mod}(\sigma_2)$. By construction, the partition $\mathcal{P} := \{[0/m], [1/m], \ldots, [(m-1)/m]\}$ is a base for σ_1 and σ_2. Furthermore it is easy to see that it is a base for $\sigma_1\sigma_2$ as well, and that $\mathcal{P}^{\sigma_1}$ is a base for σ_2. Hence by Lemma 2.11.8, we have

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

   Subtracting $\delta(\mathcal{P})$ from the leftmost and the rightmost term yields the claimed assertion.

4. We have already shown that the determinant mapping is an homomorphism from $\mathrm{RCWA}^+(\mathbb{Z})$ onto $(\mathbb{Z},+)$. It is indeed even an epimorphism, since the mapping $\nu \in \mathrm{RCWA}^+(\mathbb{Z}) :\; n \mapsto n+1$ lies in the preimage of 1. □

2.11.10 Remark Wolfgang Rump has contributed the idea to assign the value $r/m-1/2$ to a residue class $[r/m]$, and to determine how this invariant changes when one applies an affine mapping to $[r/m]$.

2.11.11 Examples Class shifts obviously have determinant 1. Mappings of finite order, commutators and their products lie in the kernel of the determinant mapping. As an example that inversion does not change the absolute value of the determinant, we have a look at the mapping σ from Example 2.5.15: It is

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

For purposes of illustrating the additivity of the determinant mapping, we have a look at the mappings α and β from 1.1.3 resp. 1.8.5 and their product: It is

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

We can easily determine the maximal subgroups of $\mathrm{RCWA}^+(\mathbb{Z})$ containing the kernel of the determinant epimorphism:

2.11.12 Remark Let K be the kernel of the determinant epimorphism, p be a prime number and $\nu : n \mapsto n+1$. Then the subgroup $K_p := \langle K, \nu^p \rangle < \mathrm{RCWA}^+(\mathbb{Z})$ has index p, hence is maximal. The intersection of all subgroups K_p is K. This implies that the Frattini subgroup of $\mathrm{RCWA}^+(\mathbb{Z})$ is a subgroup of K.

2.12 A Normal Subgroup of RCWA(Z)

In this section we will construct an epimorphism from RCWA($\mathbb{Z}$) onto $\mathbb{Z}^\times$.

Reflecting the common term for the epimorphism $S_n \to \mathbb{Z}^\times$, we will call it the *sign* mapping.

Transpositions in the symmetric group S_n cannot be written as products of two transpositions. In contrast, class transpositions in RCWA($\mathbb{Z}$) can be written as products of two other class transpositions. For this reason the sign mapping considered here cannot be derived directly from the one of finite symmetric groups. It is rather derived from an epimorphism AFF($\mathbb{Z}$) $\to \mathbb{Z}^\times$ by a lift from AFF($\mathbb{Z}$) to the whole of RCWA($\mathbb{Z}$).

Anyway, for argumentational purposes it is more convenient to use the determinant mapping as a starting point for our construction:

2.12.1 Definition We set $\exp : z \mapsto e^{2\pi i z}$. Further let $r(m) \subseteq \mathbb{Z}$ be a residue class. We define the *sign* of an affine mapping $\alpha : n \mapsto (an+b)/c$ with source $r(m)$ by

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

where $\det(\alpha) := b/(|a|m)$. Further we define the *sign* of a mapping $\sigma \in$ RCWA($\mathbb{Z}$) with modulus m by

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

2.12.2 Remark Let $\sigma \in$ RCWA($\mathbb{Z}$), and let $m := \operatorname{Mod}(\sigma)$. Using the same notation for the coefficients of σ as in Remark 2.11.2, we have

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

where we extend the determinant mapping via

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

to the whole of RCWA($\mathbb{Z}$).

The generalized notion of a 'determinant' in Definition 2.12.1 and Remark 2.12.2 does not make much sense itself. It is introduced here merely for purposes of illustrating relations between the determinant mapping and the sign mapping and of helping in the proof that the sign mapping is indeed an epimorphism.

In the proof of the assertion that the determinant mapping is an epimorphism, we have introduced an invariant $\delta([r/m])$ of residue classes $[r/m]$ with distinguished representatives. A similar construction is useful in the proof of the assertion that the sign mapping has the claimed properties. However, in this context it is not sufficient to fix representatives only:

2.12.3 Definition From now on, we assume that the residue classes $[r/m]$ are also *oriented*, i.e. that their moduli carry signs. By definition, applying an affine mapping to such a residue class changes this sign if and only if the mapping is order-reversing. Let $k \in \mathbb{N}$. We call a decomposition

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

of a residue class $[r/m]$ *representative stabilizing* and *orientation-preserving*.

Let $\mathcal{P}$ be a partition of $\mathbb{Z}$ into finitely many oriented residue classes with distinguished representatives. Then we call a refinement of $\mathcal{P}$ *representative stabilizing* and *orientation-preserving* if it is obtained by representative stabilizing and orientation-preserving decomposition of residue classes in $\mathcal{P}$.

We assign complex numbers with absolute value 1 to residue classes $[r/m]$:

2.12.4 Definition Let $[r/m]$ be an oriented residue class with distinguished representative. Then we set

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

For residue classes $r(m)$ without distinguished representative and without fixed orientation, we always assume $m > 0$ and $r \in \{0, \ldots, m-1\}$, and set $\varrho(r(m)) \;:=\; \varrho([r/m])$. Given a partition $\mathcal{P}$ of $\mathbb{Z}$ into finitely many oriented residue classes with distinguished representatives, we set

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

Further we set $\varrho(\mathbb{Z}) := (-1)^{\epsilon} \cdot \varrho(\mathcal{P})$, where we choose $\epsilon \in \{0,1\}$ such that $\varrho(\mathbb{Z}) = \exp(t)$ with $t \in [0, \frac{1}{2}[$.

We have to show that $\varrho(\mathbb{Z})$ is well-defined:

2.12.5 Lemma *Let $\mathcal{P}$ be a partition of $\mathbb{Z}$ into finitely many oriented residue classes with distinguished representatives. Then the following hold:*

1. *The value $\varrho(\mathcal{P})$ is invariant under representative stabilizing and orientation-preserving refinements of $\mathcal{P}$.*
2. *Changes of the distinguished representatives of the residue classes in $\mathcal{P}$ can only change the sign of $\varrho(\mathcal{P})$.*
3. *Changes of the orientations of the residue classes in $\mathcal{P}$ affect only the sign of $\varrho(\mathcal{P})$.*

In particular, the value $\varrho(\mathbb{Z})$ does not depend on the choice of the partition $\mathcal{P}$, hence is well-defined.

Proof:

1. For any residue class $[r/m]$ with positive modulus m and any $k \in \mathbb{N}$ the following holds:

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

   If $m < 0$, just the signs of all exponents are changed. This does not affect the validity of the given chain of equalities. It follows that $\varrho(\mathcal{P})$ is invariant under representative stabilizing and orientation-preserving refinements of $\mathcal{P}$.

2. For any $m > 0$ and $k \in \mathbb{Z}$, the following holds:

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

   If $m < 0$, again just the signs of all exponents are changed, and again this does not affect the validity of the given chain of equalities. Thus changing the distinguished representative of a residue class in $\mathcal{P}$ can at most change the sign of $\varrho(\mathcal{P})$.

3. Changing the orientation of a residue class $[r/m] \in \mathcal{P}$ changes $\varrho(\mathcal{P})$ by a factor of

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

   as claimed. □

2.12.6 Remark In fact we can explicitly determine $\varrho(\mathbb{Z})$: It is

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

However, we will not need this value in the sequel.

Similar assertions hold as for $\det(\alpha)$ and $\delta([r/m])$:

2.12.7 Lemma *Let α be an affine mapping with source $r(m)$. Then we have*

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

Let $\sigma \in \mathrm{RCWA}(\mathbb{Z})$, and let $\mathcal{P}$ be a partition of $\mathbb{Z}$ into finitely many oriented residue classes with distinguished representatives. Then it holds that

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

thus

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

for suitable $\epsilon \in \{0, 1\}$.

Proof: We assume that the mapping α is given by $n \mapsto (an+b)/c$ for certain coefficients $a, b, c \in \mathbb{Z}$. In case $a > 0$ we get the assertion directly from Lemma 2.11.8. Hence we can assume without loss of generality that $a < 0$. It holds that

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

thus our first assertion.

We get the corresponding assertion for an rcwa mapping σ and a partition $\mathcal{P}$, when we refine $\mathcal{P}$ to a base for σ by representative stabilizing and orientation-preserving decomposition of residue classes in $\mathcal{P}$, and apply the assertion proven above to the restrictions of σ to the residue classes in $\mathcal{P}$. This is permitted due to Lemma 2.12.5. □

2.12.8 Theorem *The mapping*

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

is an epimorphism.

Proof: Let $\sigma_1, \sigma_2, \sigma \in \mathrm{RCWA}(\mathbb{Z})$. We have to show that $\mathrm{sgn}(\sigma)$ is a unit of $\mathbb{Z}$, that $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1}$, that $\mathrm{sgn}(\sigma_1\sigma_2) = \mathrm{sgn}(\sigma_1) \cdot \mathrm{sgn}(\sigma_2)$ and that there is a bijective rcwa mapping of $\mathbb{Z}$ with sign -1.

1. We would like to show that the sign of σ is indeed a unit of $\mathbb{Z}$. By Lemma 2.12.7, we have $\varrho(\mathbb{Z}) = \varrho(\mathbb{Z}^\sigma) = (-1)^\epsilon \cdot \varrho(\mathbb{Z}) \cdot \mathrm{sgn}(\sigma)$ for a suitable $\epsilon \in \{0, 1\}$. Division of the leftmost and the rightmost term by $\varrho(\mathbb{Z})$ yields the claimed assertion.

2. We would like to show that $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1}$. Obviously it is sufficient to show this for the restriction of σ to some residue class $r(m)$. Thus let

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

   be such a restriction. Then we have

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

   If $a > 0$, we have $\mathrm{sgn}(\alpha^{-1}) = \exp(-b/(2am)) = \mathrm{sgn}(\alpha)^{-1}$, and if $a < 0$, we have

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

   as claimed.

3. We would like to show that $\mathrm{sgn}(\sigma_1\sigma_2) = \mathrm{sgn}(\sigma_1) \cdot \mathrm{sgn}(\sigma_2)$. Let $\mathcal{P}$ be a partition of $\mathbb{Z}$ into finitely many oriented residue classes with distinguished representatives. By Lemma 2.12.7, we have

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

   Dividing the leftmost and the rightmost term by $\varrho(\mathcal{P})$ yields the claimed assertion.

4. The sign of the mapping $\varsigma \in \mathrm{RCWA}(\mathbb{Z}): \; n \mapsto -n$ is -1. □

In Definition 2.9.1 we have seen three infinite classes of bijective rcwa mappings of $\mathbb{Z}$, which either generate RCWA($\mathbb{Z}$) or a proper normal subgroup thereof (cp. Theorem 2.9.4). We would like to determine the signature of these mappings:

2.12.9 Lemma *Given a residue class $r(m)$ of $\mathbb{Z}$, we have* $\mathrm{sgn}(\nu_{r(m)}) = \mathrm{sgn}(\varsigma_{r(m)}) = -1$. *Given two disjoint residue classes $r_1(m_1)$ and $r_2(m_2)$ of $\mathbb{Z}$, we have* $\mathrm{sgn}(\tau_{r_1(m_1),r_2(m_2)}) = 1$.

Proof: Insertion into the expression given in Remark 2.12.2 yields

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

and

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

as well as

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

In the last-mentioned case we use that the modulus of the class transposition $\tau_{r_1(m_1),r_2(m_2)}$ divides m_1m_2, and that $r_i(m_i)$ ($i \in \{1,2\}$) can be written as a union of m_{3-i} residue classes (mod m_1m_2). □

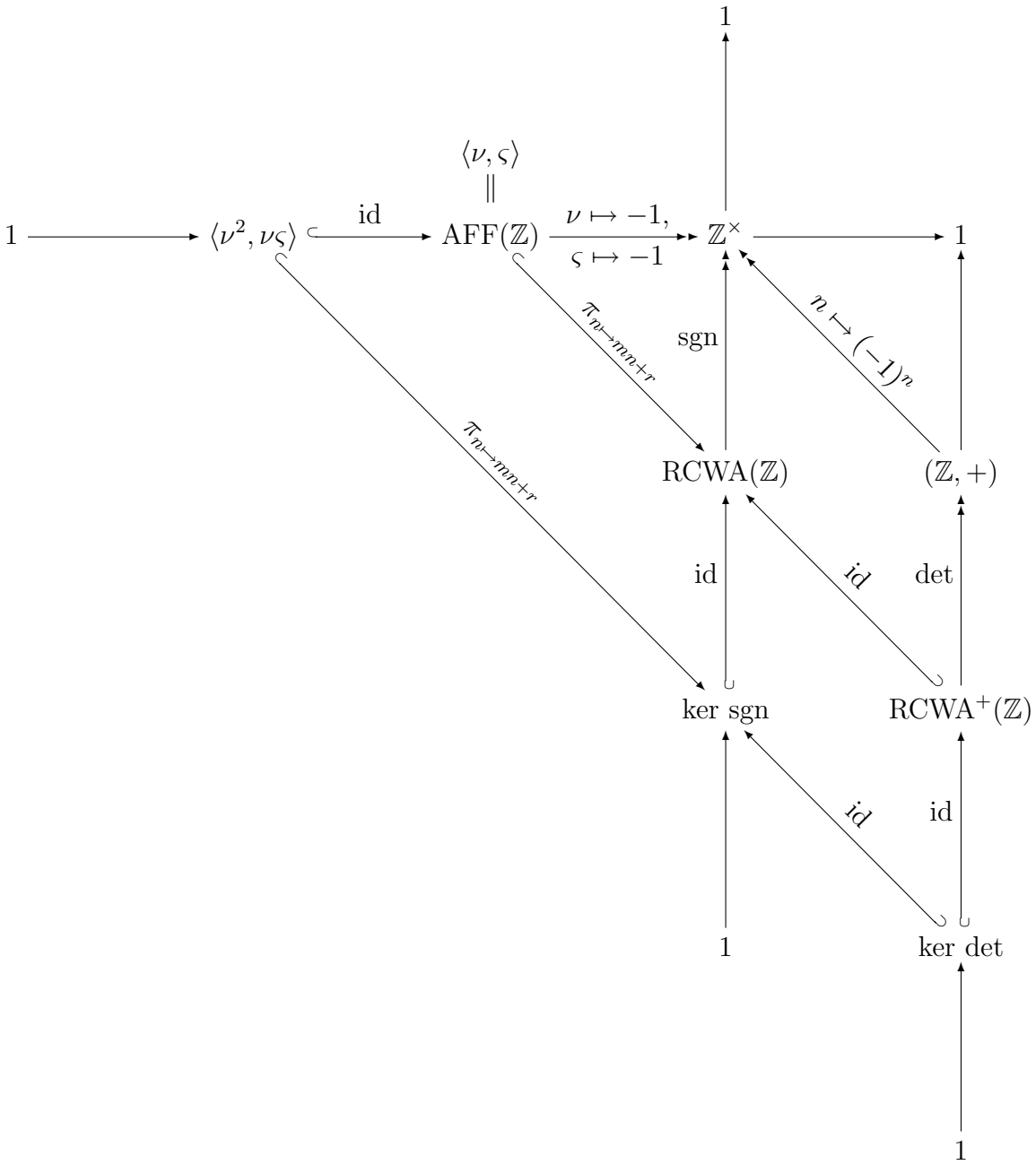
2.12.10 Example Collatz' permutation α given in Examples 1.1.3 has determinant 0, and thus the sign $(-1)^0 = 1$. By Lemma 2.12.9, the sign of the class reflection $\varsigma_{1(5)}$ is -1. Theorem 2.12.8 tells us that $\mathrm{sgn}(\alpha\cdot\varsigma_{1(5)}) = -1$. Fur purposes of illustration, we will check this directly: It is

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

Insertion into the expression given in Remark 2.12.2 yields $\det(\alpha\cdot\varsigma_{1(5)}) = \frac{2}{5}$ and the 'correcting term' $\frac{1}{20}((20-2\cdot 1)+(20-2\cdot 4)+(20-2\cdot 14)+(20-2\cdot 15)) = \frac{3}{5}$ in the exponent. From this we get – as expected – the sign $(-1)^{2/5+3/5} = -1$.

By Remark 2.12.2, the sign of a mapping $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ equals $(-1)^{\det(\sigma)}$. Further due to Lemma 2.12.9, class shifts and class reflections have sign -1. Hence the following holds:

2.12.11 Corollary Let $m \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then the following diagram commutes:



The vertical and horizontal sequences are short exact.

2.12.12 Remark Which other values could an epimorphism from RCWA($\mathbb{Z}$) to $\mathbb{Z}^\times$ take for class shifts, class reflections and class transpositions?

Under the assumption that our epimorphism is invariant under restriction monomorphisms, the image of a class transposition must be 1 since $\tau = \tau_{0(4),1(4)} \cdot \tau_{2(4),3(4)}$. The equality $\varsigma \cdot \varsigma_{0(2)} \cdot \varsigma_{1(2)} \cdot \nu_{1(2)}^{-1} = 1$ enforces furthermore that class shifts and class reflections must have the same image.

Consequently, the sign mapping is the only epimorphism from RCWA($\mathbb{Z}$) to $\mathbb{Z}^\times$ which is invariant under restriction monomorphisms, and whose kernel does not contain the mormal subgroup which is generated by all class shifts, class reflections and class transpositions (cp. Theorem 2.9.4).

2.13 Open Questions

The following questions remain open:

- Is the normal series RCWA($\mathbb{Z}$) $\rhd \ker \operatorname{sgn} \rhd 1$ already a composition series?

  Does the group RCWA($\mathbb{Z}$) have further normal subgroups?

  If yes: How do the corresponding factor groups look like?

- Is the kernel of the sign mapping resp. the kernel of the determinant mapping simple?

  If not: Which normal subgroups do these groups have?

- Is the group RCWA($\mathbb{Z}$) generated by the tame mappings?

  If so: Does it have finite diameter with respect to this set of generators, and if yes, which diameter?

- Does the group RCWA($\mathbb{Z}$) have nontrivial outer automorphisms?

- Are finitely generated subgroups of RCWA($\mathbb{Z}$) even finitely presented?

- Given $k \in \mathbb{N}$, is there always an rcwa group which acts k-transitively, but not $k+1$-transitively on one of its infinite orbits?

- Do the groups $\mathrm{GL}(n, \mathbb{Z})$ resp. the free group of rank 2 have monomorphic images in RCWA($\mathbb{Z}$)?

- Is the membership- and / or conjugacy problem in finitely generated subgroups of RCWA($\mathbb{Z}$) algorithmically decidable? For both problems, RCWA provides methods which cover certain cases.

CHAPTER 3

Trajectories and Monotonizations

The $3n+1$ Conjecture makes an assertion about the sequence $n, n^T, n^{T^2}, \ldots$ produced by iterated application of the Collatz mapping T to a positive integer n.

It is natural to ask what happens when we replace the Collatz mapping by some other mapping. In order to get interesting results, it is inevitable to restrict the class of mappings to consider. It seems to be a suitable choice to decide to investigate the class of rcwa mappings in this context.

So far, questions of this kind have not been touched in this thesis. In this chapter they should be addressed in short.

3.1 Definition Let $f : R \to R$ be a mapping, and let $n \in R$. Then the sequence $(n^{f^k})_{k\in\mathbb{N}_0}$ is called the *trajectory* of f *starting at* n.

For purposes of illustration, we list a few examples of trajectories of the Collatz mapping:

3.2 Examples The trajectories of T starting at 15, 27, -5 resp. -17 are

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

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

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

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

where we have stopped at 1 resp. at the end of a cycle.

3.3 Remark During the past half century, many people have tried to prove the $3n+1$ Conjecture. The methods these people have used for this purpose vary very much. In any case, dynamical systems and analytical density estimates have to be mentioned in this context. Lagarias' annotated bibliography [Lag05] provides undoubtedly the best overview on the work done so far on this problem.

A very nice discussion of the $3n+1$ Conjecture under the aspect of the underlying dynamical system and a detailed elementary discussion of further aspects can be found in Günther Wirsching's *Habilitationsschrift* [Wir96]. Wirsching's thesis has also appeared as a *Springer Lecture Notes* volume [Wir98]. Wirsching's work is focussed on trying to prove that all numbers $n_0 \in \mathbb{N} \setminus 0(3)$ have *positive predecessor density*, i.e. that

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

This assertion is closely related to the $3n+1$ Conjecture, but it neither implies it nor is implied by it. A sketch of a proof with three gaps formulated as conjectures is given in [Wir03].

The $3n+1$ Conjecture essentially claims that any trajectory of the Collatz mapping intersects nontrivially with a certain finite set of integers. In different words this means that it is contracting in the following sense:

3.4 Definition Let $f : R \to R$ be an arbitrary mapping from the ring R to itself. We call an ascending sequence $S_0 \subsetneq S_1 \subseteq S_2 \subseteq \ldots$ of subsets of R such that

1. S_0 is a finite set which satisfies $S_0^f = S_0$, that

2. for any $k \in \mathbb{N}$, the set S_k is the whole preimage of S_{k-1} under f, and that

3. $R = \bigcup_{k=0}^{\infty} S_k$.

a *contraction sequence* of f. If there is such a sequence we call f *contracting* and call the set S_0 the *contraction centre* of f.

3.5 Remark Contraction sequence and -centre of a contracting mapping $f \in \mathrm{Rcwa}(R)$ are determined uniquely. Thus we can talk about *the* contraction sequence and *the* contraction centre of f. If f is contracting and $\sigma \in \mathrm{Sym}(R)$, then f^σ is contracting as well – if $(S_k)_{k\in\mathbb{N}_0}$ is a contraction sequence of f, then $(S_k^\sigma)_{k\in\mathbb{N}_0}$ is a contraction sequence of f^σ.

3.6 Examples These definitions should be illustrated in a few examples.

1. The author conjectures that the Collatz mapping T is contracting, and that its contraction centre is

$$S_0 = \{ -136, -91, -82, -68, -61, -55, -41, \\ -37, -34, -25, -17, -10, -7, -5, -1, 0, 1, 2 \}.$$

   Showing this would prove the $3n+1$ Conjecture. The sets $S_1, S_2, \ldots, S_{25}$ then would have the cardinalities 30, 42, 66, 95, 138, 187, 258, 345, 467, 627, 848, 1138, 1529, 2041, 2731, 3646, 4865, 6485, 8651, 11529, 15384, 20506, 27312, 36379 resp. 48497.

2. The author conjectures that the mapping

$$T_7 \in \mathrm{Rcwa}(\mathbb{Z}), \quad n \longmapsto \begin{cases} \frac{7n+1}{2} & \text{if } \gcd(n,6) = 1, \\ \frac{n}{\gcd(n,6)} & \text{otherwise} \end{cases}$$

   is contracting and that its contraction centre is

$$S_0 = \{ -360, -206, -103, -66, -60, -59, -38, -19, -17, -11, -10, -5, -3, -1, 0, \\ 1, 2, 4, 19, 38, 65, 67, 143, 167, 195, 228, 235, 429, 501, 585, 823, 1103, 1287, \\ 2206, 2521, 2881, 3861, 4412, 5042, 8824, 10084 \}.$$

   This is not obvious – e.g. the 4361th number in the trajectory of T_7 starting at 9595 is the first one which lies in S_0, and the maximum of this sequence which is taken at position 1855 is 45266766717824274611851780017733940744283387822 72.

3. The author conjectures that the mapping

$$f_6 \in \mathrm{Rcwa}(\mathbb{Z}): \quad n \longmapsto \begin{cases} \frac{n}{6} & \text{if } n \in 0(6), \\ \frac{5n+1}{6} & \text{if } n \in 1(6), \\ \frac{7n-2}{6} & \text{if } n \in 2(6), \\ \frac{11n+3}{6} & \text{if } n \in 3(6), \\ \frac{11n-2}{6} & \text{if } n \in 4(6), \\ \frac{11n-1}{6} & \text{if } n \in 5(6) \end{cases}$$

   is contracting as well, and that its contraction centre has at least cardinality 443. The trajectory starting at 3224 approaches the fixed point 2 only after 19949562 steps and after ascending to approx. $3 \cdot 10^{2197}$. Note that the product of the coefficients in the numerators ($5 \cdot 7 \cdot 11^3 = 46585$) is only a bit smaller than the product of the coefficients in the denominators ($6^6 = 46656$). A consequence of this is that the absolute value of the image of an integer n under the mapping f_6 is 'on average' smaller than $|n|$ by a factor of $\sqrt[6]{46585/46656} \approx 0.999746$. It is obvious that the last consideration is purely heuristic.

4. A further mapping which the author conjectures to be contracting is

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

It holds $\forall n \in \mathbb{Z}\ (-n)^{f_5} = -(n^{f_5})$. Provided its existence, the contraction centre of f_5 has at least cardinality $3659 = 1 + 2 \cdot (1 \cdot 1 + 5 \cdot 5 + 1 \cdot 141 + 6 \cdot 277)$: Fixed points of f_5 are 0 and ± 1, cycles of length 5 are $\pm$(4 6 8 5 7), $\pm$(10 14 20 28 17), $\pm$(29 41 57 34 48), $\pm$(35 49 69 97 58) and $\pm$(50 70 98 59 83), members of least absolute value of 141-cycles are ± 89 and members of least absolute value of 277-cycles are ± 2536, ± 3199, ± 12571, ± 13075, ± 16564 and ± 27589. It is not clear whether the mentioned 6 pairs of 277-cycles just arise 'by random' or whether there is some deeper reason for their existence.

Already in the Summary it has been mentioned that for proving the $3n+1$ Conjecture it would be enough to find a permutation $\sigma \in (\mathrm{Sym}(\mathbb{Z})_{\{\mathbb{N}\}})_1$ such that $\forall n \in \mathbb{N} \setminus \{1\}\ n^{T^\sigma} < n$. Since T is surjective, it is equivalent to require that T^σ is monotonous 'almost everywhere'. This motivates the following definition:

3.7 Definition Let R be ordered, e.g. $R \in \{\mathbb{Z}, \mathbb{Z}_{(\pi)}\}$. We call a mapping $f \in \mathrm{Rcwa}(R)$ *monotonizable* if there is a permutation $\sigma \in \mathrm{Sym}(R)$ such that f^σ is monotonous. We call it *rcwa-monotonizable* if σ can even be chosen to be an rcwa mapping. Further we call f *nearly (rcwa-)monotonizable* if there is a $\sigma \in \mathrm{Sym}(R)$ ($\sigma \in \mathrm{RCWA}(R)$) and a finite set $S \subsetneq R$ such that f^σ is monotonous on $R \setminus S$.

In order to get information on dependencies between these properties of an rcwa mapping, we need the following lemma:

3.8 Lemma *Assume that $f \in \mathrm{Rcwa}(R)$ is not injective and that $\mathrm{Mult}(f) \neq 0$. Then there is a residue class $r_0(m_0)$ and two disjoint residue classes $r_1(m_1)$ and $r_2(m_2)$ of R such that $r_0(m_0) = r_1(m_1)^f = r_2(m_2)^f$.*

Proof: Let $m := \mathrm{Mod}(f)$. Due to our condition that the mapping f is not injective, there are two residue classes $\tilde{r}_1(m)$ and $\tilde{r}_2(m)$ whose images under f are not disjoint. Due to the condition that $\mathrm{Mult}(f) \neq 0$, by Lemma 1.1.8, Assertion (1), $\tilde{r}_1(m)^f$ and $\tilde{r}_2(m)^f$ are residue classes as well. Therefore $r_0(m_0) := \tilde{r}_1(m)^f \cap \tilde{r}_2(m)^f$ is also a residue class. The preimages $r_1(m_1)$ and $r_2(m_2)$ of $r_0(m_0)$ under the affine partial mappings of f on $\tilde{r}_1(m)$ resp. $\tilde{r}_2(m)$ are residue classes by Lemma 1.1.8, Assertion (1). Further they are disjoint, since they are subsets of distinct residue classes (mod m). □

3.9 Lemma *Let $f \in \mathrm{Rcwa}(\mathbb{Z})$ be surjective, not injective and nearly monotonizable. Then f is contracting.*

Proof: Let $S \subset \mathbb{Z}$ be a finite set and $\sigma \in \mathrm{Sym}(\mathbb{Z})$ such that f^σ is monotonous on $\mathbb{Z} \setminus S$. Like f also f^σ is surjective and not injective. Consequently, the application of f^σ decreases the absolute value of all except of finitely many $n \in \mathbb{Z}$ (look at the graph of the function f^σ!). This implies that f^σ is contracting, and using Remark 3.5 completes the proof of our assertion. □

In the proof of the main theorem of this section, we need the following lemma:

3.10 Lemma *The following holds:* $\forall f \in \mathrm{Rcwa}(R)\ \exists c \in R:\ |x^f| \leqslant \mathrm{Mult}(f) \cdot |x| + c$.

Proof: We get the assertion by taking upper bounds on the absolute values of the images under affine partial mappings of f. □

We get a quite restrictive condition for rcwa-monotonizability:

3.11 Theorem *Assume that $f \in \mathrm{Rcwa}(\mathbb{Z}) \setminus \mathrm{RCWA}(\mathbb{Z})$ is surjective and (nearly) rcwa-monotonizable. Suppose further that* $\mathrm{Mult}(f) \neq 0$. *Then there is a $k \in \mathbb{N}$ such that there are at most finitely many $n \in \mathbb{Z}$ such that $|n^{f^k}| \geqslant |n|$.*

Proof: By assumption we can choose a mapping $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ and a finite subset $S \subset \mathbb{Z}$ such that $\mu := f^\sigma \in \mathrm{Rcwa}(\mathbb{Z})$ is monotonous on $\mathbb{Z} \setminus S$. Surjectivity and non-injectivity are inherited from f to μ, and due to Lemma 1.3.1, Assertion (a.4) and (b.3) it is $\mathrm{Mult}(\mu) \neq 0$. Consequently, by Lemma 3.8 there is a residue class $r(m) \subset \mathbb{Z}$ such that each $n \in r(m)$ has at least two distinct preimages under μ. From the surjectivity of μ, the monotonity of μ on $\mathbb{Z} \setminus S$ and the finiteness of S we conclude that there is a constant $c \in \mathbb{N}$ such that

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

and induction over $k \in \mathbb{N}$ yields

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

For arbitrary $k \in \mathbb{N}$ we have $n^{f^k} = n^{\sigma^{-1}\mu^k\sigma}$. If we choose k such that

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

then by Lemma 1.3.1b, Assertion (3) and Lemma 3.10 it holds that

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

for some constant c' depending on σ. Since neither k nor c nor c' depends on n, this completes our proof. □

Is there a $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ such that T^σ is monotonous? – No, things are not that easy!:

3.12 Remark Using Theorem 3.11 we can conclude that the Collatz mapping T is not nearly rcwa-monotonizable: The mapping T is surjective and not injective, and it is $\mathrm{Mult}(T) \neq 0$. But if $n = 2^k m - 1$ for arbitrary $k, m \in \mathbb{N}$, we have

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

In order to get a conjugate T^σ which is monotonous almost everywhere we thus would have to look at mappings $\sigma \in \mathrm{Sym}(\mathbb{Z}) \setminus \mathrm{RCWA}(\mathbb{Z})$. In particular the quotient n^σ/n must not be bounded – its boundedness for rcwa mappings is in fact what the proof of Theorem 3.11 is based on.

At the end of this short chapter we would like to show that the Collatz mapping can be extended to a permutation of $\mathbb{Z}^2$ in a natural way:

3.13 Example The mapping

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

is a permutation which acts on the x-coordinate just like the Collatz mapping T. Its inverse σ_T^{-1} is given by

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

The mapping σ_T is affine on the residue classes $r(m) \in \mathbb{Z}^2/\langle (6,0),(0,1)\rangle\mathbb{Z}^2$, and σ_T^{-1} is affine on the residue classes $r(m) \in \mathbb{Z}^2/\langle (3,0),(0,2)\rangle\mathbb{Z}^2$.

APPENDIX A

Wildness Criteria

In this appendix we would like to discuss the question how to recognize whether a given rcwa mapping is tame or wild.

One criterion whose application is algorithmically very cheap has already been mentioned before (non-balancedness, cp. Conclusion 2.5.12).

In the following we will obtain two further such criteria:

A surjective rcwa mapping is wild if

1. it is not injective, or if
2. one of its transition graphs has a weakly connected component which is not strongly connected.

The proofs are essentially based on lemmata concerning the density of images and preimages of open sets under rcwa mappings.

The *asymptotic* density of a set $S \subseteq \mathbb{N}$ of positive integers is defined by

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

The asymptotic density is also called *natural* density provided that the sequence $(d_n)_{n\in\mathbb{N}}$ converges.

It is easy to see that given a positive integer k, the asymptotic resp. natural density of $k \cdot S$ is $\frac{1}{k}$-times the asymptotic resp. natural density of S itself. Furthermore, adding a constant to the elements of a set does not change its density.

These facts are very convenient w.r.t. considerations concerning rcwa mappings. This motivates the following definition:

A.1 Definition Given a residue class $r(m) \subseteq R$, we set $\mu(r(m)) := 1/|R/mR|$. Given $S \subseteq R$ we further set $\mu(R \setminus S) := 1 - \mu(S)$, and given two subsets $S_1, S_2 \subseteq R$, we set $\mu(S_1 \cup S_2) := \mu(S_1) + \mu(S_2) - \mu(S_1 \cap S_2)$.

These settings induce a notion of density for open and closed subsets of R. We call $\mu(S)$ the *natural density* of S.

By the *modulus* $\mathrm{Mod}(S)$ of an open or closed subset $S \subseteq R$ we denote the least $|m|$ such that S can be written as union of residue classes (mod m). If there is no such m, we set $\mathrm{Mod}(S) := 0$.

This notion of density complies in a natural way with the generally used definition of the natural density of a set of integers given above.

For convenience we use the following shorthand for preimages:

A.2 Convention In the following, we write $n^{f^{-1}}$ resp. $S^{f^{-1}}$ to denote the full preimage of an element n resp. a set S under a mapping f.

We need a few basic lemmata concerning density and modulus of images and preimages of open sets under rcwa mappings:

A.3 Lemma *Let $S \subseteq R$ be open. Further let $\alpha \in \mathrm{AFF}(K) : n \mapsto (an + b)/c$ and $f \in \mathrm{Rcwa}(R)$. Then the following hold:*

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

In this context, let $0|0$.

Proof: By definition, the set of residue classes is a basis for our topology on R. Consequently, the open set S is a union of residue classes.

1. This assertion follows from Lemma 1.1.8, Assertion (1), applied to the elements of a partition of S into residue classes.

2. This assertion follows from (1), applied to the affine partial mappings of f and to the intersections of S with the residue classes (mod $\mathrm{Mod}(f)$). Images under constant affine partial mappings have natural density 0, thus can be ignored in this context.

3. The case $\mathrm{Mod}(S) = 0$ is trivial. Hence without loss of generality we can assume that $\mathrm{Mod}(S) \neq 0$. Let $m := \mathrm{Mod}(f)$ and $n \in R$. By definition, $n^f \bmod \mathrm{Mod}(S)$ determines whether n^f is in S or not. This value in turn is determined by $n \bmod m$ and $n^{f|_{n(m)}} \bmod \mathrm{Mod}(S)$, hence by $n \bmod \mathrm{lcm}(m, \mathrm{Div}(f) \cdot \mathrm{Mod}(S))$. Applying Lemma 1.3.1a, Assertion (1) finishes the proof. □

We need a term which denotes the sum of the densities of the images of the affine partial mappings of an affine mapping:

A.4 Definition Let $f \in \mathrm{Rcwa}(R)$ and let $m := \mathrm{Mod}(f)$. Further suppose that the restrictions of f to the residue classes $r(m) \in R/mR$ are given by $n \mapsto (a_{r(m)}n+b_{r(m)})/c_{r(m)}$. Then we define the *image density* $\mu_{\mathrm{img}}(f)$ of f by

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

The right '=' is justified by Lemma A.3, Assertion (1).

From Definition A.4 we immediately read off that the image density of an rcwa mapping with given multiplier and divisor can neither be arbitrary large nor arbitrary small, and that the denominator of the fraction is bounded as well:

A.5 Lemma Given $f \in \mathrm{Rcwa}(R)$, we have $1/|R/\mathrm{Mult}(f)R| \leqslant \mu_{\mathrm{img}}(f) \leqslant |R/\mathrm{Div}(f)R|$ and $|R/\mathrm{Mod}(f)R| \cdot |R/\mathrm{Mult}(f)R| \cdot \mu_{\mathrm{img}}(f) \in \mathbb{N}_0$.

Stronger assertions hold under the assumption that the corresponding mapping is injective, surjective or even bijective:

A.6 Lemma *Let $f \in \mathrm{Rcwa}(R)$. Then the following hold:*

1. *f is injective $\Rightarrow \mu_{\mathrm{img}}(f) \leqslant 1$.*
2. *f is surjective $\Rightarrow \mu_{\mathrm{img}}(f) \geqslant 1$.*
3. *f is bijective $\Rightarrow \mu_{\mathrm{img}}(f) = 1$.*

In Assertion (1) and (2), equality holds for mappings f without constant affine partial mappings if and only if f is bijective.

Proof: The assertions follow from the additivity of the density function and from the setting $\mu(R) := 1$. □

Multiplying by a surjective, but not injective mapping increases the image density:

A.7 Lemma *Let $f, g \in \mathrm{Rcwa}(R)$ be surjective rcwa mappings without constant affine partial mappings, and assume that f is not injective. Then $\mu_{\mathrm{img}}(f \cdot g) > \mu_{\mathrm{img}}(g)$.*

Proof: By Lemma 3.8, there is a residue class $r_0(m_0)$ and two disjoint residue classes $r_1(m_1)$ and $r_2(m_2)$ of R such that $r_1(m_1)^f = r_2(m_2)^f = r_0(m_0)$. Let $m_g := \mathrm{Mod}(g)$. Then the residue classes $r_0(m_g)$ and $r_0(m_0)$ intersect nontrivially. Let $r_0(m)$ be their intersection. Due to the surjectivity of f it is $\mu_{\mathrm{img}}(f \cdot g) \geqslant \mu_{\mathrm{img}}(g) + \mu(r_0(m)^g) > \mu_{\mathrm{img}}(g)$, which had to be shown. □

Now we can show the validity of the first-mentioned criterion:

A.8 Theorem *If $f \in \mathrm{Rcwa}(R)$ is surjective but not injective, then f is wild.*

Proof: Assume that f is tame. Let $m := \mathrm{Mod}(\langle f \rangle)$. Then the restrictions $f^k|_{r(m)}$ $(k \in \mathbb{N})$ of powers of f to residue classes (mod m) are affine. Due to Lemma 1.1.8, Assertion (1) the images of the residue classes $r(m)$ under the powers f^k are either single residue classes as well, or (caused by constant partial mappings) sets of cardinality 1. We have to distinguish two different cases:

1. The mapping f has a constant partial mapping $f|_{r_1(m)} \equiv n$. In this case, due to the surjectivity of the mapping f and the choice of m there is an infinite sequence $r_2(m), r_3(m), r_4(m), \ldots$ of pairwisely distinct residue classes (mod m) such that $\forall k \in \mathbb{N}\ f^k|_{r_k(m)} \equiv n$. Since R/mR is finite this yields a contradiction.

2. The mapping f does not have a constant partial mapping. In this case, we know from Lemma A.7 that $\forall k \in \mathbb{N}\ \mu_{\mathrm{img}}(f^{k+1}) > \mu_{\mathrm{img}}(f^k)$. By Lemma A.5, $|R/\mathrm{Div}(f^k)R|$ is an upper bound on $\mu_{\mathrm{img}}(f^k)$. From Lemma 1.3.1a, Assertion (1) we know that $|R/\mathrm{Div}(f^k)R| \leqslant |R/mR|$. Using the 'denominator bound' from Lemma A.5, we conclude that the sequence $(\mathrm{Mult}(f^k))_{k\in\mathbb{N}}$ is not bounded.

   If we set $d := |R/mR| + 2$, then we can choose a $k_0 \in \mathbb{N}$ and a residue class $r_1(m) \in R/mR$ such that $\mu(r_1(m)^{f^{k_0}}) < 1/|R/mR|^d$. According to the above, $r_1(m)^{f^{k_0}} =: r_0(\tilde{m})$ is a residue class as well, and from Lemma A.3, Assertion (2) and Lemma 1.3.1a, Assertion (1) we conclude that $\forall k \in \mathbb{N}\ \mu(r_0(\tilde{m})^{f^k}) < 1/|R/mR|^{d-1}$. Using the method described below, we show that there is an exponent $e \in \mathbb{N}$ such that for any $k \in \mathbb{N}$ and any $r(m) \in R/mR$ we have $\mu(r(m)^{f^{e+k}}) < 1/|R/mR|$:

   1. Put $i := 2$.
   2. Since the mapping f^{k_0} is surjective, there is a residue class $r_i(m) \in R/mR$ such that $\mu(r_i(m)^{f^{k_0}} \cap r_{i-1}(m)) \geqslant 1/|R/mR|^2$. By the choice of m, for any $k \in \mathbb{N}_0$ the mappings $f^{(i-1)k_0+k}\big|_{r_i(m)^{f^{k_0}}}$ and $f^{(i-1)k_0+k}|_{r_{i-1}(m)}$ are affine and differ at most by their sources. Hence using this inequality one can conclude inductively that

$$\mu(r_i(m)^{f^{ik_0}}) \leqslant |R/mR|^{i-1} \cdot \mu(r_1(m)^{f^{k_0}}) < 1/|R/mR|^{d-(i-1)}$$

      and that $\mu(r_i(m)^{f^{ik_0+k}}) < 1/|R/mR|^{d-i}$. Thus in particular for $i \leqslant |R/mR|$ no image of $r_i(m)^{f^{ik_0}}$ under a power of f can have an intersection of density $\geqslant 1/|R/mR|^2$ with any residue class $r_{\tilde{i}}(m)$ $(*)$.
   3. If $i < |R/mR|$, put $i := i + 1$ and continue with step (2), otherwise done.

   Due to $(*)$ the $|R/mR|$ residue classes $r_i(m) \in R/mR$ which we get this way are pairwisely distinct. Hence the above-mentioned inequality for the density holds for $e := |R/mR| \cdot k_0$. This is a contradiction to the assumption that f is surjective. □

A.9 Examples Three of the four possible combinations of (non-) injectivity and (non-) surjectivity do not permit a conclusion whether the respective rcwa mapping is tame or wild – examples over $\mathbb{Z}$:

	tame	wild
¬injective, ¬surjective	$f \in \mathrm{Rcwa}(\mathbb{Z})$: $n \mapsto \begin{cases} 2n & \text{if } n \in 0(2), \\ 2n+2 & \text{if } n \in 1(2). \end{cases}$	$f \in \mathrm{Rcwa}(\mathbb{Z})$: $n \mapsto \begin{cases} \frac{3n}{2} & \text{if } n \in 0(2), \\ 2n+2 & \text{if } n \in 1(2). \end{cases}$
injective, ¬surjective	$f \in \mathrm{Rcwa}(\mathbb{Z}) : \ n \mapsto 2n$.	$f \in \mathrm{Rcwa}(\mathbb{Z})$: $n \mapsto \begin{cases} \frac{3n}{2} & \text{if } n \in 0(2), \\ 3n+2 & \text{if } n \in 1(2). \end{cases}$
¬injective, surjective	Does not exist, see Theorem A.8.	$T \in \mathrm{Rcwa}(\mathbb{Z})$: $n \mapsto \begin{cases} \frac{n}{2} & \text{if } n \in 0(2), \\ \frac{3n+1}{2} & \text{if } n \in 1(2) \end{cases}$ (cp. Examples 1.1.3).
bijective	$\nu \in \mathrm{RCWA}(\mathbb{Z}) : \ n \mapsto n+1$.	$\alpha \in \mathrm{RCWA}(\mathbb{Z})$: $n \mapsto \begin{cases} \frac{3n}{2} & \text{if } n \in 0(2), \\ \frac{3n+1}{4} & \text{if } n \in 1(4), \\ \frac{3n-1}{4} & \text{if } n \in 3(4) \end{cases}$ (cp. Examples 1.1.3).

A.10 Lemma *Let $f \in \mathrm{Rcwa}(R)$. Assume that there is a union of finitely many residue classes of R which is a proper subset of its image and a proper superset of its preimage under f. Then f is wild.*

Proof: Let S_0 be such a union of finitely many residue classes, and let S_1 be the preimage of S_0 under f. By Theorem 2.2.3, Assertion (4), the set S_1 is a union of finitely may residue classes as well, and hence has a strictly smaller natural density than S_0. Our conditions imply that images of elements outside S_1 lie outside S_0, hence in particular outside S_1. Thus since the image of S_1 under f is a proper superset of S_1, the preimage S_2 of S_1 under f is a proper subset of S_1. We can iterate this argumentation and get a

descending chain $S_0 \supsetneq S_1 \supsetneq S_2 \supsetneq \ldots$ of unions of finitely many residue classes such that S_{k+1} is always the full preimage of S_k under f.

Assume that f is tame, and set $m := \mathrm{Mod}(\langle f \rangle)$. By Lemma 1.4.3, Assertion (2) we have $\forall k \in \mathbb{N}\ \mathrm{Div}(f^k) | m$. Since S_0 is the image of S_k under f^k, the quotients $\mu(S_0)/\,\mu(S_k)$ hence are bounded by $|R/mR|$ due to Lemma A.3, Assertion (2). Now we can easily conclude that $\lim_{k\to\infty} \mu(S_k)/\,\mu(S_{k+1}) = 1$, and hence $\lim_{k\to\infty} \mathrm{Mod}(S_k) = \infty$. But since S_k is the preimage of S_0 under f^k, we know from Lemma A.3, Assertion (3) that it holds also that $\forall k \in \mathbb{N}\ \mathrm{Mod}(S_k) | m \cdot \mathrm{Mod}(S_0)$. This is a contradiction. □

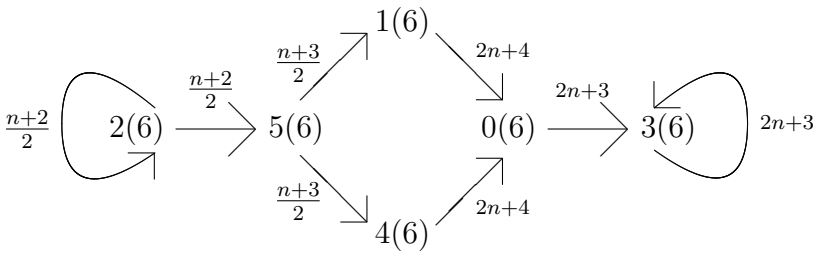
Using Lemma A.10 we can show the validity of the second criterion:

A.11 Theorem *Let $f \in \mathrm{Rcwa}(R)$ be surjective, and assume that there is an $m \in \mathbb{N}$ such that the transition graph $\Gamma_{f,m}$ of f for modulus m has a weakly connected component which is not strongly connected. Then f is wild.*

Proof: According to the conditions, for suitable m we can choose a strongly connected component Γ_0 of $\Gamma_{f,m}$ which is a proper subgraph of a weakly connected component $\overline{\Gamma}_0$. Since $\overline{\Gamma}_0$ is a finite graph, we can assume without loss of generality that Γ_0 is connected to the rest of $\overline{\Gamma}_0$ by outgoing edges only: Otherwise we could follow an ingoing edge in reverse direction and would enter another strongly connected component and so on, until reaching a 'source' which satisfies our condition after a finite number of steps.

Let $S \subsetneq R$ be the union of the vertices of Γ_0. Since f is surjective, the image of S under f is a proper superset of S. By the choice of Γ_0 this implies further that the preimage of S under f is a proper subset of S. Now, Lemma A.10 tells us that f is wild, as claimed. □

A.12 Example We take the mapping α from Examples 1.1.3, and set $\nu : n \mapsto n+1$. The transition graph of the mapping $\nu\nu^\alpha$ for modulus 6 looks as follows:



This graph is weakly connected but not strongly connected. A strongly connected component without ingoing edges is $\{2(6)\}$. Consequently, by Theorem A.11 the mapping $\nu\nu^\alpha$ is wild.

APPENDIX B

Examples

In this appendix we would like to discuss several examples of residue class-wise affine mappings and -groups in detail.

The structure of tame rcwa groups has been completely determined in Theorem 2.6.1. In contrast, the question for the structure of wild rcwa groups is difficult. The same holds for the question how orbits under their action on the underlying ring may look like. The following examples should illustrate this. However, in the same time they should demonstrate that wild rcwa groups are accessible to computational investigations as well.

B.1 Structure of a Wild rcwa Group

Let α be Collatz' permutation given in Examples 1.1.3. Further let β be defined as in Examples 1.8.5, Part (3), and let $\nu : n \mapsto n+1$. We investigate the group $G := \langle \alpha, \beta, \nu \rangle$.

Maybe the permutations α and β generate a free group of rank 2. In any case, adding the generator ν yields a multitude of nontrivial relations. For example it is easy to check with RCWA that $\mathrm{ord}([\alpha\beta, \nu^2]) = 396 = 2^2 \cdot 3^2 \cdot 11$, $\mathrm{ord}([\alpha\beta, \nu^4]) = 182 = 2 \cdot 7 \cdot 13$, $\mathrm{ord}([\alpha\beta, \nu^6]) = 24$, $\mathrm{ord}([\alpha\beta, \nu^{184}]) = \mathrm{ord}([\alpha\beta, \nu^{356}]) = 25$, $\mathrm{ord}([\beta^2, \nu^{17}]) = 5256 = 72 \cdot 73 = 2^3 \cdot 3^2 \cdot 73$ and $\mathrm{ord}([\beta^2, \nu^{20}]) = 29$. For illustrational purposes we explicitly write down one of these commutators:

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

Further, computational investigations suggest the following relations:

1. Given $k \in \mathbb{Z}$ it holds that

$$[\alpha, \nu^k] \text{ wild } \Leftrightarrow \gcd(k, 6) = 1, \text{ and}$$

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

2. Given $k \in \mathbb{Z}$ it holds that

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

3. It holds $\forall k \in \mathbb{N} \setminus \{2, 4, 6, 12, 24, 184, 356\}$ $\operatorname{ord}([\alpha\beta, \nu^k]) \in \{10, 15, \infty\}$.

4. Given $k \in \mathbb{Z}$ it holds that

$$\operatorname{ord}([\alpha^2, \nu^k]) = \begin{cases} 1 & \text{if } k = 0, \\ 4 & \text{if } k \in 9(18), \\ 5 & \text{if } k \in \{-6, 6\}, \\ 7 & \text{if } k \in 61(144) \cup 83(144), \\ 9 & \text{if } k \in 16(48) \cup 32(48) \cup 8(144) \cup 136(144), \\ 17 & \text{if } k \in 134(288) \cup 154(288), \\ 70 & \text{if } k \in \{-10, 10\}, \\ 90 & \text{if } k \in \{-14, 14\}, \\ \infty & \text{otherwise.} \end{cases}$$

The naturally arising question whether the group G is finitely presented remains open.

B.2 On Automorphisms of RCWA(Z)

Both of the mappings ν and α from the preceding section have infinite order. Is there an automorphism of RCWA($\mathbb{Z}$) which maps ν to α?

The mapping ν is tame, while α is wild. Hence by Lemma 1.8.3, Assertion (1) such an automorphism cannot be inner. So far, nothing is known about possible outer automorphisms of RCWA($\mathbb{Z}$). Our question can be answered anyway:

We have $\nu^{n\mapsto -n} = \nu^{-1}$, thus in RCWA($\mathbb{Z}$) the mapping ν is conjugate to its inverse. Further it is

$$\lim_{k\to\infty} \frac{\mathrm{Mod}(\alpha^k)}{\mathrm{Mod}(\alpha^{-k})} = \lim_{k\to\infty} \frac{4^k}{3^k} = \infty.$$

Hence by Lemma 1.3.1c, Assertion (1) the mappings α and α^{-1} are not conjugate in RCWA($\mathbb{Z}$). This implies a negative answer to our question.

B.3 Orbits Under the Action of a Wild rcwa Group

Conclusion 2.5.17 gives a complete description of orbits under the action of tame rcwa groups on $\mathbb{Z}$. But how do orbits under the action of wild rcwa groups look like?

Obviously there are finite and infinite orbits under the action of such groups. This section focusses on those groups whose orbits are all finite.

On the polynomial rings $\mathbb{F}_q[x]$ the degree mapping induces a partition into finite subsets, which is fixed by suitable wild rcwa mappings and -groups (cp. Examples 1.1.3, Part (3)). In contrast, it is not at all obvious whether there are wild rcwa groups over $\mathbb{Z}$ whose orbits on $\mathbb{Z}$ are all finite. Here we would like to describe an example of a wild group $G < \mathrm{RCWA}(\mathbb{Z})$ which seems to have this property. Let the generators σ_1 and σ_2 of G be given by

$$n \longmapsto \begin{cases} n & \text{if } n \in 0(4), \\ n+1 & \text{if } n \in 1(4) \cup 2(4), \\ n-2 & \text{if } n \in 3(4) \end{cases} \quad \text{resp.} \quad n \longmapsto \begin{cases} \frac{3n+3}{2} & \text{if } n \in 1(\ 6), \\ 2n & \text{if } n \in 3(\ 9), \\ \frac{n-3}{3} & \text{if } n \in 6(18), \\ n & \text{otherwise.} \end{cases}$$

The product of these two mappings is wild. This can be seen by looking at the restriction of the mapping $\sigma := \sigma_1\sigma_2$ to the residue class 3(12): It is $\sigma|_{3(12)} = \sigma_1|_{3(12)} \cdot \sigma_2|_{3(12)^{\sigma_1}} = \sigma_1|_{3(12)} \cdot \sigma_2|_{1(12)} = (n \mapsto n-2) \cdot (n \mapsto (3n+3)/2) = n \mapsto (3n-3)/2$. It is easy to check that for $\alpha \in \mathrm{AFF}(\mathbb{Q}) : n \mapsto (3n-3)/2$ it is $\forall k \in \mathbb{N}\ \ 3(12) \cap 3(12)^{\alpha^k} = 3(12 \cdot 3^k)$. Consequently, $12 \cdot 3^k$ is a lower bound on the modulus of the mapping σ^k. This implies that σ is wild.

Both of the mappings σ_1 and σ_2 have order 3, and both have fixed points. Thus as a consequence of Theorem 2.6.7 they are conjugate in RCWA($\mathbb{Z}$). It is $\sigma_1^\theta = \sigma_2$, where

$$\theta \in \mathrm{RCWA}(\mathbb{Z}): \quad n \longmapsto \begin{cases} \frac{3n-1}{2} & \text{if } n \in 1(4), \\ \frac{9n-6}{4} & \text{if } n \in 2(4), \\ \frac{9n-15}{2} & \text{if } n \in 3(4), \\ \frac{3n+32}{16} & \text{if } n \in 0(16), \\ \frac{3n+20}{8} & \text{if } n \in 4(16), \\ \frac{9n-72}{16} & \text{if } n \in 8(16), \\ \frac{9n+12}{8} & \text{if } n \in 12(16). \end{cases}$$

The group G acts on the set $\{1, 2, 3, 5, 6, 7, 12, 24\}$ as $\mathrm{E}(8) : \mathrm{F}_{21}$ (GAP notation, order $8 \cdot 21 = 168$) and on $\{17, 18, 19, 29, 30, 31, 48, 60, 96\}$ as $\mathrm{P\Gamma L}(2, 8)$.

Further, results of computational investigations suggest that all orbits under the action of G on $\mathbb{Z}$ are finite, and that G is isomorphic to the free product of two cyclic groups of order 3.

It is however not even clear that the permutation σ indeed has only finite cycles. Trying to answer this question, we restrict σ to the 'relevant' connected component of the transition graph $\Gamma_{\sigma,36}$ and remove vertices which are superfluous in the given context. 'Removing' a vertex $r(m)$ means that we take it away, and if there were vertices $r_1(m_1)$ and $r_2(m_2)$ such that there was an ingoing edge from $r_1(m_1)$ to $r(m)$ and an outgoing edge from $r(m)$ to $r_2(m_2)$, then we join these two edges to an edge from $r_1(m_1)$ to $r_2(m_2)$. The affine mapping corresponding to the vertex $r_1(m_1)$ is in turn multiplied by the one corresponding to $r(m)$.

This yields a permutation which has only finite cycles if and only if the same holds for σ itself. In this way for example we can construct the mapping

$$\sigma' \in \mathrm{RCWA}(\mathbb{Z}): \quad n \longmapsto \begin{cases} \frac{3n-3}{2} & \text{if } n \in 3(12), \\ \frac{3n+6}{2} & \text{if } n \in 6(12), \\ \frac{n+1}{3} & \text{if } n \in 5(36), \\ \frac{n-9}{3} & \text{if } n \in 24(36), \\ 2n & \text{if } n \in 12(36) \cup 21(36), \\ 2n+2 & \text{if } n \in 2(36) \cup 29(36), \\ n+1 & \text{if } n \in 14(36) \cup 17(36) \cup 26(36), \\ n & \text{otherwise,} \end{cases}$$

whose transition graph for modulus 36 is depicted in Figure B.3.1. The numbers in brackets denote the minimal length of a cycle passing the respective vertex. Cycles which are not members of an infinite series are not considered.

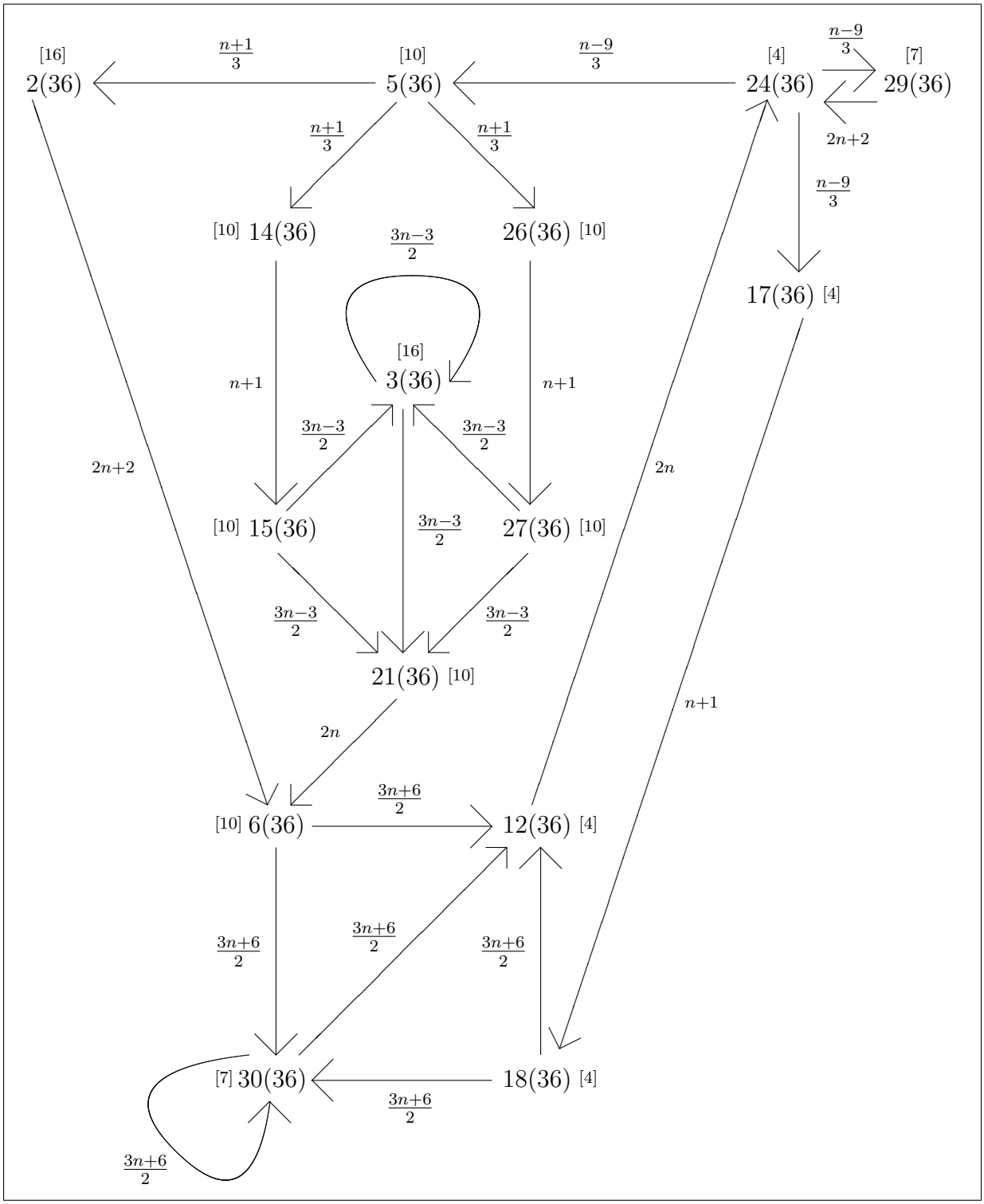


Figure B.3.1: Transition graph of σ' for modulus 36.

B.4 A Wild rcwa Mapping Without Infinite Cycles

The mapping σ' in the previous section is still relatively complicate. Also rather than in this particular case, we are interested in the general question whether there are wild rcwa mappings of $\mathbb{Z}$ without infinite cycles at all. Thus in this section we will try to construct a 'least complicate' such mapping.

One possible approach is to take a closer look at the mapping σ' and to think about reasons why this mapping seems to have only finite cycles, and in which way one could construct a similar, but simpler-structured mapping. These considerations are mostly heuristic, and describing them in detail would be lengthy. For this reason we give and discuss only the result in form of the mapping

$$\kappa := \tau_{2(4),3(4)} \cdot \tau_{3(4),8(12)} \cdot \tau_{4(6),8(12)} : \quad n \longmapsto \begin{cases} \frac{3n+2}{2} & \text{if } n \in 2(4), \\ \frac{n+1}{3} & \text{if } n \in 8(12), \\ 2n & \text{if } n \in 4(12), \\ 2n-2 & \text{if } n \in 11(12), \\ n-1 & \text{if } n \in 3(12) \cup 7(12), \\ n & \text{otherwise.} \end{cases}$$

The transition graph $\Gamma_{\kappa,12}$ of κ for modulus 12 looks as follows:

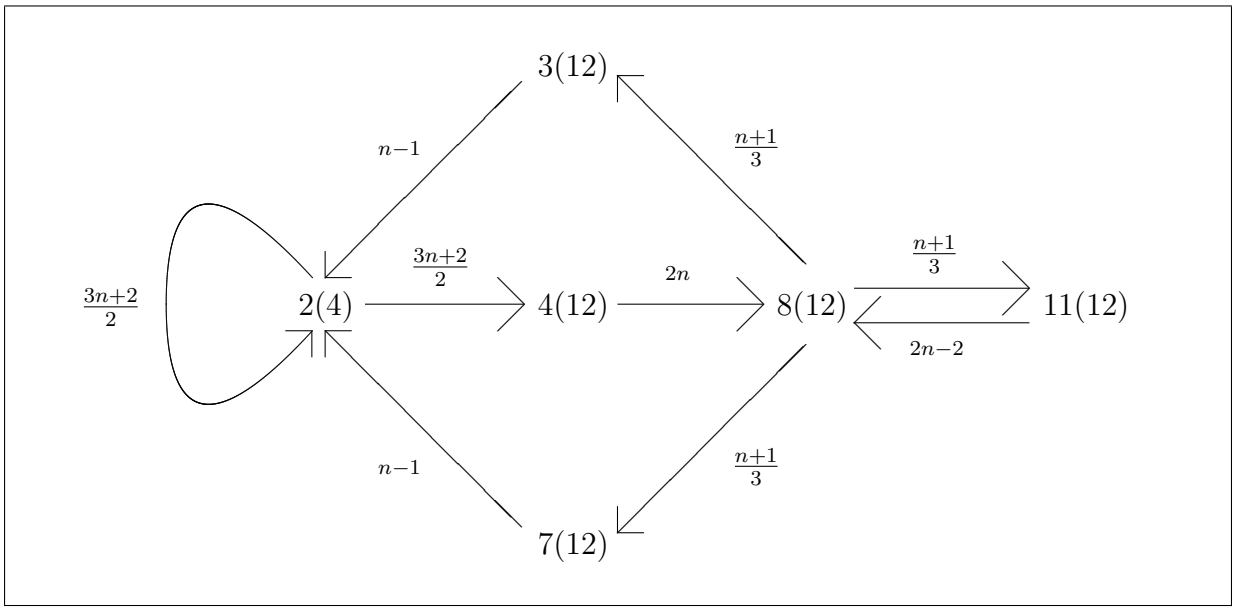


Figure B.4.1: Transition graph of κ.

For reasons of clarity, we have bundled the vertices 2(12), 6(12) and 10(12) into one vertex 2(4). In order to shed a light on the relation to the transition graph of σ' given in Figure B.3.1, we list which vertices of the one graph correspond to which vertices of the other:

- $2(4) \leftrightarrow 6(36) \cup 18(36) \cup 30(36)$
- $3(12) \leftrightarrow 2(36)$
- $4(12) \leftrightarrow 12(36)$
- $7(12) \leftrightarrow 17(36)$
- $8(12) \leftrightarrow 24(36)$
- $11(12) \leftrightarrow 29(36)$
- All other vertices of $\Gamma_{\sigma',36}$ have turned out to be not needed and have been left away.

Due to the loop around the vertex 2(4) it is obvious that κ is wild, and checking bijectivity is straightforward. But why do all cycles of κ have finite length?

For $r(m) \in \{2(4), 3(12), 4(12), 7(12), 8(12), 11(12)\}$ we set $\alpha_{r(m)} := \kappa|_{r(m)}$, and convince ourselves that $\alpha_{2(4)}\alpha_{4(12)}\alpha_{8(12)}\alpha_{7(12)} = 1$ and $\alpha_{8(12)}\alpha_{11(12)} = {\alpha_{2(4)}}^{-1}$. Now it is possible to figure out that except of (-1,-4), the permutation κ has only cycles of length $l \equiv 1\ (3)$, and that for any $k \in \mathbb{N}_0$ the set of integers belonging to cycles of length $l = 3k + 1$ is given by

$$\mathcal{C}_k := \begin{cases} 1(4) \cup 0(12) \cup \{-2\} & \text{if } k = 0, \text{ resp.} \\ \cup \left(\left(2(4) \setminus \bigcup_{j=1}^{k-1} \mathcal{C}_j \right) \setminus \bigcup_{j=0}^{k} \left(2(4)^{\kappa^j} \cap 2(4)^{\kappa^{-(k-j)}} \right) \right)^{\langle \kappa \rangle} & \text{if } k > 0. \end{cases}$$

Further one can see that the sets $\mathcal{C}_k$, $k \in \mathbb{N}_0$ form a partition of $\mathbb{Z} \setminus \{-4, -1\}$ into disjoint nonempty subsets. For this purpose it is in principle sufficient to convince oneself that for no $n \in 2(4)$ the loop around 2(4) is passed infinitely often, that for any $k \in \mathbb{N}$ there is an $n \in 2(4)$ such that the cycle which n belongs to passes the vertex 2(4) exactly k times (choose e.g. $n := 2^{k+1} - 2$), and that passing the loop for one time is compensated by one 'detour' $8(12) \to 11(12) \to 8(12)$. (Cp. the relations of the affine partial mappings given above.) Using RCWA we get

$$\begin{aligned} \mathcal{C}_1 &= 2(24) \cup 3(24) \cup 18(24) \cup 19(24) \cup 4(36) \cup 28(36) \cup 8(72) \cup 56(72), \\ \mathcal{C}_2 &= 6(48) \cup 7(48) \cup 38(48) \cup 39(48) \cup 10(72) \cup 11(72) \cup 58(72) \cup 59(72) \\ &\quad \cup 16(108) \cup 88(108) \cup 20(144) \cup 116(144) \cup 32(216) \cup 176(216), \quad \text{and} \\ \mathcal{C}_3 &= 14(96) \cup 15(96) \cup 78(96) \cup 79(96) \cup 22(144) \cup 23(144) \cup 118(144) \cup 119(144) \\ &\quad \cup 34(216) \cup 35(216) \cup 178(216) \cup 179(216) \cup 44(288) \cup 236(288) \\ &\quad \cup 52(324) \cup 268(324) \cup 68(432) \cup 356(432) \cup 104(648) \cup 536(648). \end{aligned}$$

Further simplifications of the construction of κ do not seem to be possible. It is relatively easy to see that no vertex can simply be left away. It is further necessary that the modulus of the mapping has at least two distinct prime divisors. The two prime divisors are needed to construct a vertex which intersects nontrivially with its image, but is neither subset nor superset of it. Such a vertex is crucial for the construction. The choice of 6 or 10 as modulus of the mapping would not leave enough room for the rest of the construction. It is obvious that these considerations are purely heuristic. They are given exclusively for illustrational purposes.

In the following we give some cycle length statistics for the permutation κ. For this we consider all cycles which intersect nontrivially with the interval $[1, 12^4]$:

Cycle length	Number of cycles	Cycle length	Number of cycles
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 Concatenation of Finite Cycles

We modify the mapping κ a bit: We expand the cyclus $8(12) \to 11(12) \to 8(12)$ of its transition graph given in Figure B.4.1 by inserting a 'trifurcation'. For example, this may yield the mapping

$$\tilde{\kappa} \in \mathrm{RCWA}(\mathbb{Z}): \quad n \longmapsto \begin{cases} \frac{3n+2}{2} & \text{if } n \in 2(4), \\ \frac{n+1}{3} & \text{if } n \in 8(12), \\ 2n & \text{if } n \in 4(12), \\ \frac{n+4}{3} & \text{if } n \in 11(12), \\ 3n+33 & \text{if } n \in 1(12) \cup 9(12), \\ 3n-39 & \text{if } n \in 5(12), \\ 2n-4 & \text{if } n \in 0(12), \\ n-1 & \text{if } n \in 3(12) \cup 7(12). \end{cases}$$

The transition graph $\Gamma_{\tilde{\kappa},12}$ of $\tilde{\kappa}$ for modulus 12 looks as follows:

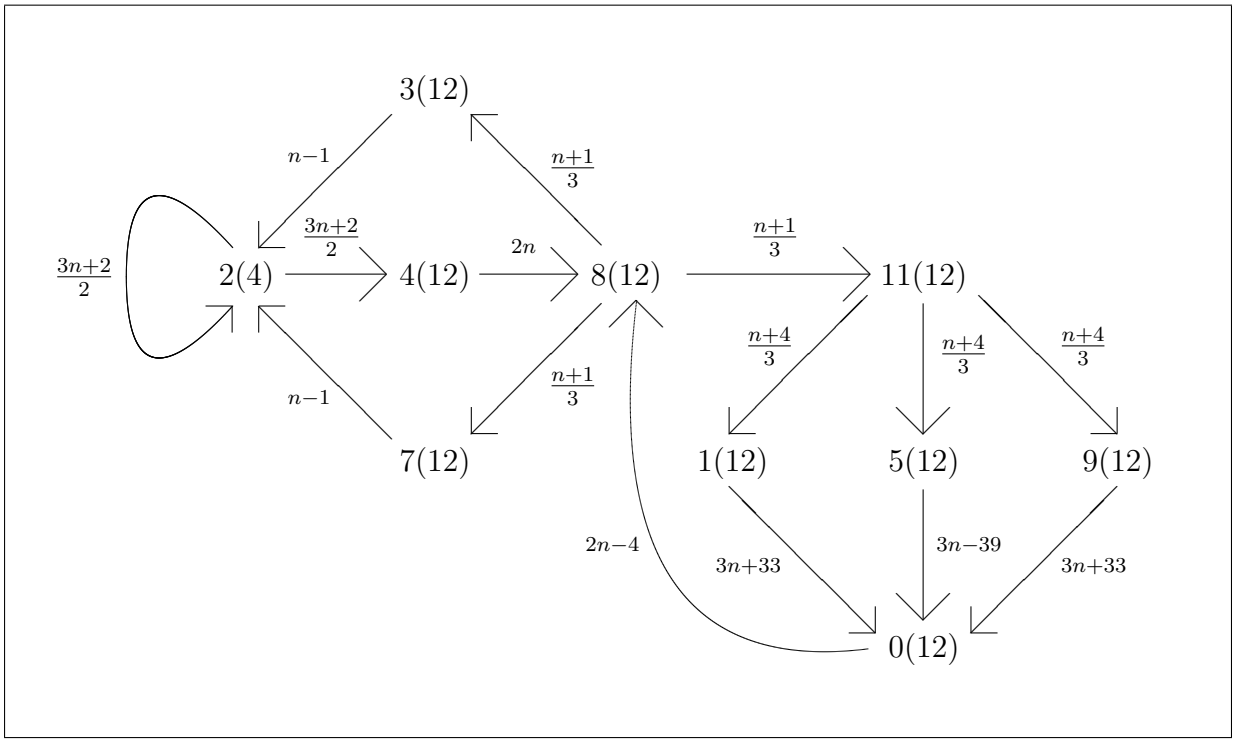


Figure B.5.1: Transition graph of $\tilde{\kappa}$.

Again for reasons of clarity we have bundled suitable vertices together. It is immediate to see that -2 is the only fixed point of $\tilde{\kappa}$, and using RCWA it is easy to check that the set of numbers belonging to 4-cycles is given by

$$2(24) \cup 3(24) \cup 18(24) \cup 19(24) \cup 4(36) \cup 28(36) \cup 8(72) \cup 56(72) \cup \{25, 71, 108, 212\}$$
$$\subsetneq 2(4) \cup 3(12) \cup 4(12) \cup 7(12) \cup 8(12) \cup \{25, 71, 108, 212\}.$$

Apart from this, $\tilde{\kappa}$ has a cycle of a given finite length $l > 4$ if and only if $l \equiv 4\ (5)$ and $l \geqslant 74$. However not all cycles of $\tilde{\kappa}$ are finite – more precisely, there is exactly one infinite cycle. This cycle passes the residue classes (mod 12) acyclically, and the asymptotic density of the set of its elements is strictly positive. Computational investigations suggest a density of $\frac{3}{8}$. The set of integers belonging to finite cycles seems to have density $1-\frac{3}{8} = \frac{5}{8}$. Provided that these assertions hold, we get a partition of $\mathbb{Z}$ into the set of fixed points (of density 0), the set of integers belonging to 4-cycles (of density $\frac{1}{4}$), the set of integers belonging to cycles of length $l \equiv 4\ (5)$ with $l \geqslant 74$ (of density $\frac{3}{8}$) and the set of integers forming the infinite cycle (of density $\frac{3}{8}$ as well).
We would like to take a closer look at this. Similar as above, we define the affine mappings $\alpha_{r(m)} := \tilde{\kappa}|_{r(m)}$ for

$$r(m) \in \{2(4), 0(12), 1(12), 3(12), 4(12), 5(12), 7(12), 8(12), 9(12), 11(12)\}.$$

In order to enable the reader to recognize the corresponding paths in the transition graph, we do not identify equal mappings $\alpha_{r(m)}$ with one another. We get the following equalities:

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. $\forall k \in \mathbb{N}_0\ \alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}\alpha_{2(4)}{}^{k+4}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}\alpha_{2(4)}{}^{2}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}\alpha_{2(4)}{}^{3}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{5(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}\alpha_{2(4)}{}^{2}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{5(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}\alpha_{2(4)}{}^{3}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}(\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)})^{k+2}\alpha_{5(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}\alpha_{2(4)}{}^{2}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{5(12)} = 1$.

3. $\forall k \in \mathbb{N}_0\ \alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}\alpha_{2(4)}{}^{2}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}\alpha_{2(4)}{}^{k+4}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}\alpha_{2(4)}{}^{2}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{9(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{3(12)}\alpha_{2(4)}{}^{3}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{5(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}\alpha_{2(4)}{}^{2}\alpha_{4(12)}\alpha_{8(12)}\alpha_{11(12)}\alpha_{5(12)}\alpha_{0(12)}\alpha_{8(12)}\alpha_{7(12)}\alpha_{2(4)}{}^{3}\alpha_{4(12)}(\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)}\alpha_{0(12)})^{k}\alpha_{8(12)}\alpha_{11(12)}\alpha_{1(12)} = (n \mapsto n + 324)$.

Here the equalities (1) correspond to the cycles of length 4, the equalities (2) correspond to the cycles of length $l \equiv 4\ (5)$ with $l \geqslant 74$ and the equalities (3) correspond to the infinite cycle. In the last-mentioned case the path underlying the given equation is passed consecutively for different k. If we start the first 'round' at $n = 0$, then computational investigations suggest that the value of k in the rth round equals the valuation of the 2-adic number $r + \sum_{i=0}^{\infty} 4^i$. Thus in a certain sense we can say that the infinite cycle is an acyclic concatenation of finite cycles of lengths $l_r \equiv 4\ (5)$, where the 'starting points' $n \in 0(324)$ are shifted by 324 each time.

B.6 An 'Erratic' Cycle Almost Covering Z

It is possible to extend the constructions given in the previous section even further. Looking at the mapping κ, we have noticed that the loop around the vertex 2(4) and the pair of edges connecting the vertices 8(12) and 11(12) act in a certain sense as 'counterparts'. With reasonable experience in such constructions it is possible to combine three such pairs to a permutation ω which except of the fixed points 4, 6 and 8 and the transpositions $(-17\ \ -45)$, (13 36) and (17 48) consists of only one single cycle. This cycle passes the residue classes (mod $\mathrm{Mod}(\omega) = 36$) acyclically, and comprises all integers $n \in \mathbb{Z} \setminus \{-45, -17, 4, 6, 8, 13, 17, 36, 48\}$. The transition graph of ω for modulus 36 is depicted in Figure B.6.1. For reasons of clarity, we have again bundled suitable vertices together.

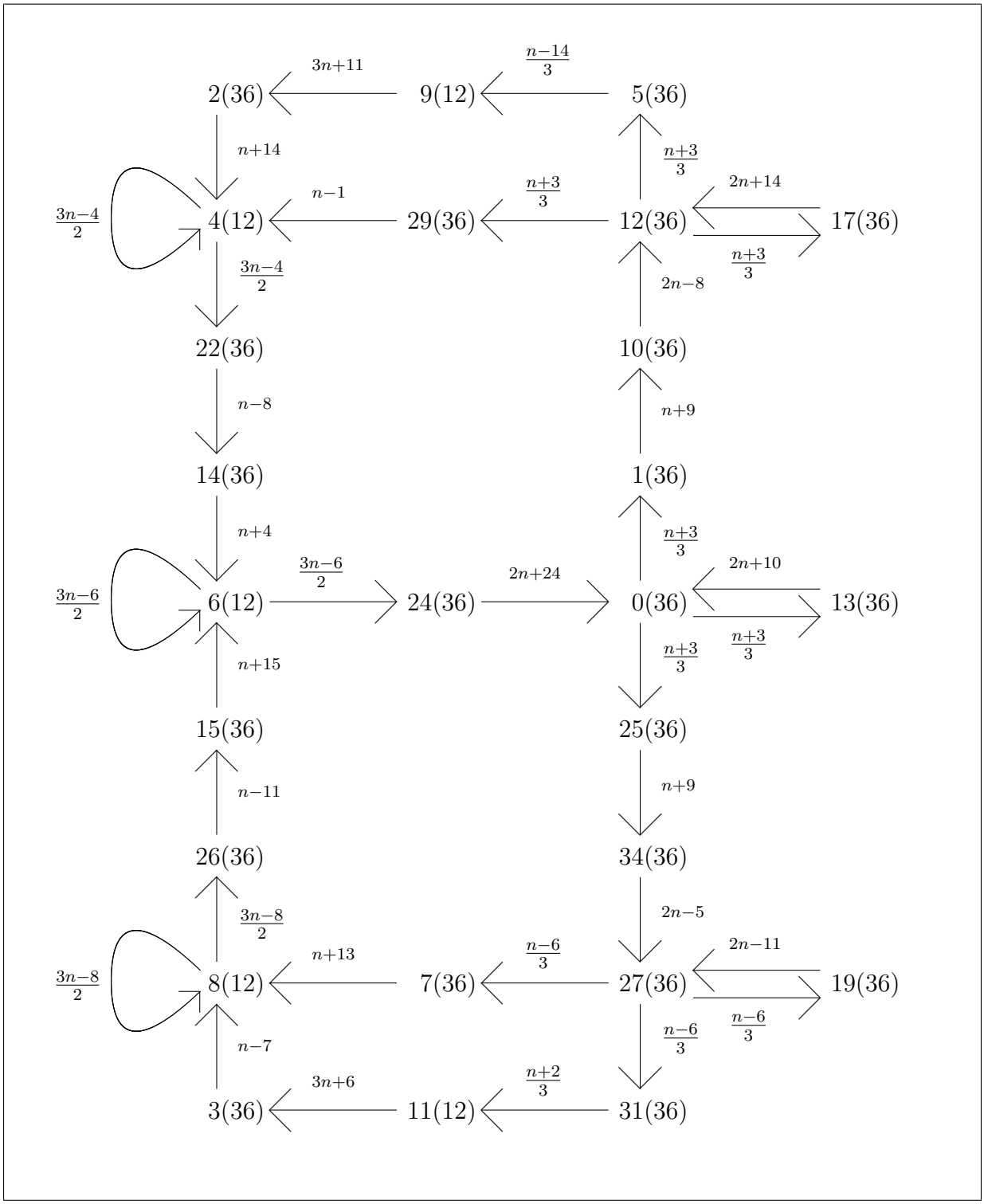


Figure B.6.1: Transition graph of ω.

Note that the support of a cycle of a tame mapping can be the whole of $\mathbb{Z}$ (example: $\nu : n \mapsto n+1$), but that by Conclusion 2.5.17 it can never be the complement of a nonempty finite set. An example of a part of the infinite cycle of the permutation ω is (... -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 ...). It seems that the quotient $\max\{0^{\omega^n} | 0 \leqslant n \leqslant n_{\max}\}/n_{\max}$ is not bounded. E.g. for $n_{\max} = 10^1, 10^2, \ldots, 10^6$ its integral part takes the values 2, 10, 32, 81, 430 resp. 4649. Sometimes integers with small absolute value appear in the cycle 'relatively far away from 0' – e.g. it is $0^{\omega^{133}} = 9$ and $0^{\omega^{11925}} = 249$. The permutation ω can be factored into elements of the set of generators given in Section 2.9: It is

$$\begin{aligned}\omega \;=\; & \nu_{3(36)}^{-1} \cdot \nu_{5(36)}^{-1} \cdot \nu_{24(36)} \cdot \nu_{33(36)} \cdot \nu_{35(36)} \\ & \cdot \big((1,5,2,11,7,6,29,26,35,27,16,31,30,28,3,13,17,14,23,15,19,18,25) \\ & \quad (4,33,34,8,21,22,32)(9,10,20)(12,24,36)\big)^{\varphi_{36}} \\ & \cdot \tau_{1(12),0(36)} \cdot \tau_{5(12),12(36)} \cdot \tau_{9(12),27(36)} \cdot \tau_{1(4),4(12)} \cdot \tau_{7(12),2(36)} \cdot \tau_{11(12),3(36)} \\ & \cdot \tau_{4(18),0(36)} \cdot \tau_{6(18),12(36)} \cdot \tau_{8(18),27(36)},\end{aligned}$$

where φ_m denotes the integral rcwa representation of the symmetric group S_m given in Theorem 2.1.2. It is much easier to determine this factorization than to obtain the factorization of the mapping α in Example 2.9.9. The reason for this is simply that ω is balanced, but α is not. From the above factorization we immediately read off that

$$\det(\omega) \;=\; -1 + -1 + 1 + 1 + 1 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 \;=\; 1.$$

B.7 An Example for the 'Connected Component Criterion'

In this section we would like to give a larger example for the application of the 'wildness criterion' in Theorem A.11. Let σ_1 be defined as in Section B.3. It is possible to choose $\tilde{\theta} \in \mathrm{RCWA}(\mathbb{Z})$ such that $\sigma_1^{\tilde{\theta}}$ and $\tilde{\sigma} := \sigma_1 \cdot \sigma_1^{\tilde{\theta}}$ are given by

$$n \;\mapsto\; \begin{cases} \frac{3n}{2} & \text{if } n \in 2(\ 4), \\ 2n+1 & \text{if } n \in 3(\ 6), \\ \frac{n-1}{3} & \text{if } n \in 7(12), \\ n & \text{otherwise} \end{cases} \quad \text{resp.} \quad n \;\mapsto\; \begin{cases} n & \text{if } n \in\ 0(\ 4), \\ \frac{3n+3}{2} & \text{if } n \in\ 1(\ 4), \\ 2n+3 & \text{if } n \in\ 2(12), \\ n-2 & \text{if } n \in\ 3(12) \cup 7(12), \\ \frac{n}{3} & \text{if } n \in\ 6(12), \\ n+1 & \text{if } n \in 10(12), \\ 2n-3 & \text{if } n \in 11(12). \end{cases}$$

The transition graph $\Gamma_{\tilde{\sigma},12}$ depicted in Figure B.7.1 is weakly connected, but not strongly connected.

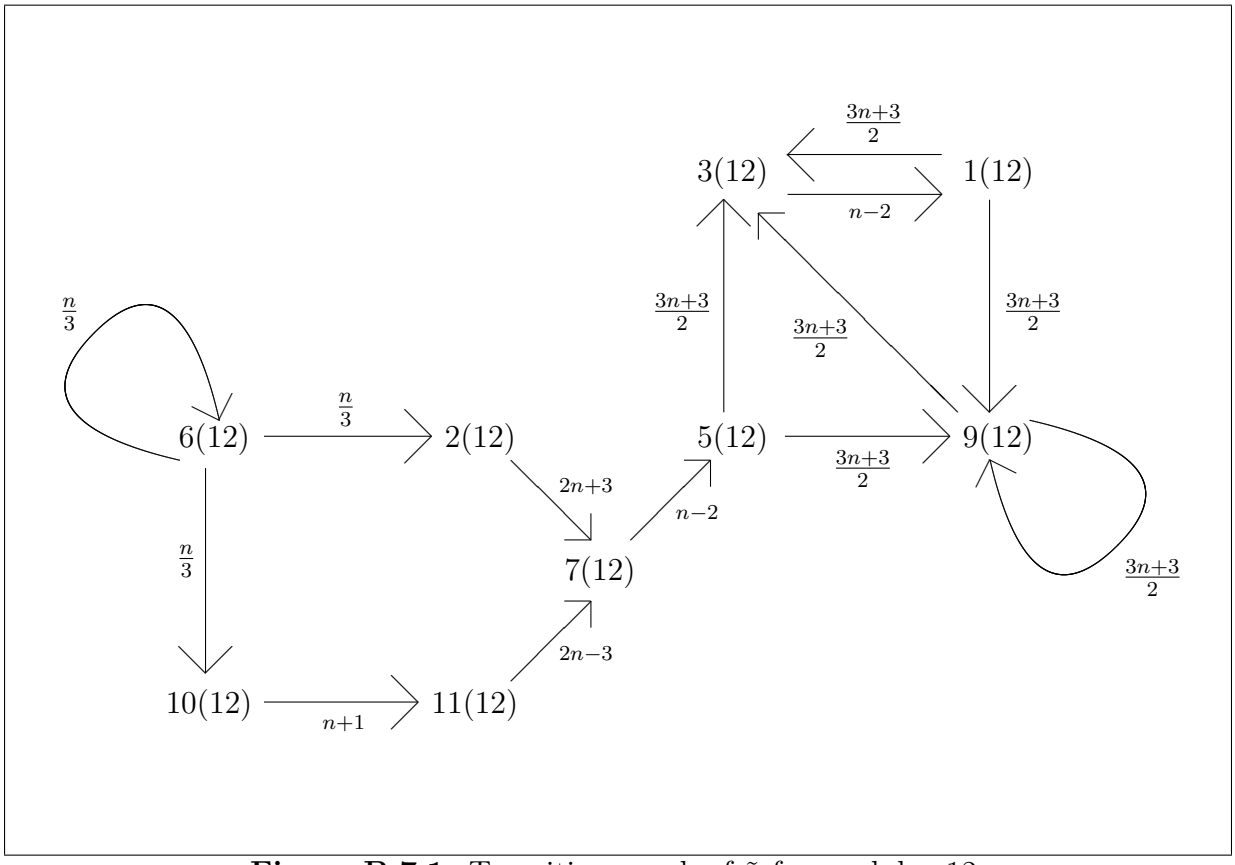


Figure B.7.1: Transition graph of $\tilde{\sigma}$ for modulus 12.

Thus by Theorem A.11, the mapping $\tilde{\sigma}$ is wild. The vertex 6(12) has outgoing edges only. A strongly connected component of $\Gamma_{\tilde{\sigma},12}$ which has only ingoing edges is formed by the vertices 1(12), 3(12) and 9(12). It is obvious that any trajectory enters this connected component after a finite number of steps. It is also easy to see that except of (1 3), the permutation $\tilde{\sigma}$ does not have nontrivial finite cycles. A 'typical' cycle of $\tilde{\sigma}$ is (... 1458 486 162 54 18 6 2 7 5 9 15 13 21 33 51 49 75 73 111 109 165 249 375 ...).

Computational investigations of lots of further examples can be found in the manual of the GAP package RCWA [Koh05].

Notation

Sets and Mappings

M; $\lvert M\rvert$; $\emptyset$	Set; cardinality of M; empty set.
$M \cup N$	Union of M and N.
$M \cap N$	Intersection of M and N.
$M \setminus N$	Set-theoretic difference of M and N.
$\cup M$; $\cap M$	Union / intersection of the elements of M, where M is a set of sets.
id	Identity mapping.
x^f; M^f	Image of the element x / the set M under the mapping f.
$x^{f^{-1}}$; $M^{f^{-1}}$	Preimage of the element x / the set M under the mapping f.
$f \cdot g$, fg	Compositum of the mappings f and g; the mapping f is applied first.
$f\lvert_M$	Restriction of the mapping f to the set M.
$\operatorname{im} f$	Image of the mapping f.
$\ker \varphi$	Kernel of the homomorphism φ.

Rings and Fields

$\mathbb{N}$	Set of positive integers.
$\mathbb{N}_0$	Set of nonnegative integers.
$\mathbb{Z}$	Ring of integers.
$\mathbb{Z}_{(p)}, \mathbb{Z}_{(\pi)}$	(Semi-)localisation of $\mathbb{Z}$ at p resp. π.
$\mathbb{Q}$	Rational field.
$\mathbb{F}_q$	Field with q elements.
$\mathbb{F}_q[x]$	Polynomial ring in one variable over $\mathbb{F}_q$.
R	Euclidean ring all of those residue class rings are finite.
K	Quotient field of the ring R.
$\operatorname{char}(R)$, $\operatorname{char}(K)$	Characteristic of the ring R / field K.
$R^\times$	Group of units of the ring R.
$\operatorname{Aff}(R)$	Monoid of affine mappings of the ring R.
$\operatorname{AFF}(R)$	Group of bijective affine mappings of the ring R.

$\mathrm{AFF}(K)$	Affine group of the field K.
$r(m)$	Residue class r (mod m).
$\mathfrak{R}(m)$	Set of representatives for the residue classes (mod m); we always assume that $(r \bmod m) \in \mathfrak{R}(m)$.
$\mathbb{P}(R)$	Set of prime elements of the ring R.
p, q	Prime(-power), if not specified otherwise.
$a\|b$	'a divides b'.
$p^k\|\|n$	$p^k \mid n$, but $p^{k+1} \nmid n$.
gcd	Greatest common divisor.
lcm	Least common multiple.
$\det(A)$	Determinant of the matrix A.
$\exp(z)$	Function exp: $\mathbb{C} \to \mathbb{C}$, $z \mapsto e^{2\pi i z}$.

Groups, General Notation

G	Group, unless specified otherwise.
$\langle g_1, \ldots, g_n \rangle$	Group resp. monoid generated by $g_1, \ldots, g_n$.
$\|G\|$	Order of the group G.
$\mathrm{ord}(g)$	Order of the group element g.
$\exp(G)$	Exponent of the group G (= lcm of the orders of the elements).
$[g, h]$	Commutator of g and h; $[g, h] = g^{-1}h^{-1}gh$.
$\mathrm{Z}(G)$	Centre of G.
$\mathrm{C}_G(H)$	Centralizer of H in G.
$\mathrm{N}_G(H)$	Normalizer of H in G.
$\mathrm{Aut}(G)$	Automorphism group of G.
$H \trianglelefteq G$	'H is normal subgroup of G'.
$\|G : H\|$	Index of H in G.
$G \times H$	Direct product of the groups G and H.
$G \rtimes H$	Semidirect product of the groups G and H (G is normal).
$G \wr P$	Wreath product of the group G with the permutation group P.
G_x	Stabilizer of the point x under the action of G.
$G_{(M)}$	Pointwise stabilizer of M under the action of G.
$G_{\{M\}}$	Setwise stabilizer of M under the action of G.
x^G, M^G	Orbit of the point x / the set of points M under the action of G.
$\mathrm{supp}(g)$	Support of the permutation g.
$\mathrm{supp}(G)$	Support of the permutation group G.

Series of Groups

C_n	Cyclic group of order n.
D_n	Dihedral group of degree n (of order $2n$).
$\mathrm{S}_n/\mathrm{Sym}(M)$	Symmetric group of degree n / on the set M.
A_n	Alternating group of degree n.

$\mathrm{GL}(n,q)$	General linear group of degree n over $\mathbb{F}_q$.
$\mathrm{SL}(n,q)$	Special linear group of degree n over $\mathbb{F}_q$.
$\mathrm{PSL}(n,q)$	Projective special linear group of degree n over $\mathbb{F}_q$.
$\Gamma\mathrm{L}(n,q)$	General semilinear group of degree n over $\mathbb{F}_q$.
$\mathrm{P}\Gamma\mathrm{L}(n,q)$	Projective semilinear group of degree n over $\mathbb{F}_q$.

$\mathrm{Rcwa}(R)$	Monoid of all residue class-wise affine (*rcwa*-) mappings of the ring R (→ Definition 1.3.3).
$\mathrm{RCWA}(R)$	Group of all bijective rcwa mappings of the ring R (→ Definition 1.3.3).
$\mathrm{RCWA}^+(R)$	Group of all class-wise order-preserving bijective rcwa mappings of the (ordered) ring R (→ Definition 1.7.1).
$\mathrm{Mod}(f)$	Modulus of the rcwa mapping f (→ Definition 1.1.2).
$\mathrm{Mod}(G)$	Modulus of the rcwa monoid / of the rcwa group G (→ Definition 1.4.2).
$\mathrm{Mult}(f)$	Multiplier of the rcwa mapping f (→ Definition 1.1.2).
$\mathrm{Mult}(G)$	Multiplier of the rcwa monoid / of the rcwa group G (→ Definition 1.4.2).
$\mathrm{Div}(f)$	Divisor of the rcwa mapping f (→ Definition 1.1.2).
$\mathrm{Div}(G)$	Divisor of the rcwa Monoid / of the rcwa group G (→ Definition 1.4.2).
$\mathcal{P}(f)$	Prime set of the rcwa mapping f (→ Definition 1.1.2).
$\mathcal{P}(G)$	Prime set of the rcwa monoid / of the rcwa group G (→ Definition 1.4.2).
$a_{r(m)}, b_{r(m)}, c_{r(m)}$	Coefficients of an rcwa mapping on the residue class $r(m)$ (→ Definition 1.1.2).
$\Gamma_{f,m}$	Transition graph of the rcwa mapping f for modulus m (→ Definition 1.6.1).
$\mu(M)$	Natural density of $M \subseteq R$ (→ Definition A.1).
$\mu_{\mathrm{img}}(f)$	Image density of the rcwa mapping f (→ Definition A.4).
π_f	Restriction monomorphism associated to the rcwa mapping f (→ Definition 2.3.1).

$\mathcal{P}$	Partition of the ring R into finitely many residue classes, unless specified otherwise.
$\sigma_{\mathcal{P}}$	Permutation induced by the tame rcwa mapping σ on the respected partition $\mathcal{P}$ (→ Definition 2.5.2).
$G_{\mathcal{P}}$	Permutation group induced by the tame rcwa group G on the respected partition $\mathcal{P}$ (→ Definition 2.5.2).
$\mathrm{Sym}(\mathcal{P})$	Tame rcwa group which respects the partition $\mathcal{P}$ and acts on it as full symmetric group (→ Definition 2.5.2).
$\det(\sigma)$	Determinant of the rcwa mapping $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ (→ Definition 2.11.1).
$[r/m]$	Residue class $r(m)$ with fixed representative r (→ Definition 2.11.3), in Section 2.12 additionally with signed modulus (→ Definition 2.12.3).
$\delta\left([r/m]\right)$	Mapping $\delta:\ [r/m] \mapsto r/m - 1/2$ (→ Definition 2.11.4).
$\mathrm{sgn}(f)$	Sign of the rcwa mapping f (→ Definition 2.12.1).
$\varrho\left(r(m)\right)$	Mapping $\varrho:\ [r/m] \mapsto e^{\pm\,\delta([r/m])/2}$ (→ Definition 2.12.4).
$\nu_{r(m)}$, $\varsigma_{r(m)}$, $\tau_{r_1(m_1),r_2(m_2)}$	Class shift, class reflection, class transposition (→ Definition 2.9.1).
ν, ς, τ	Mapping $\nu : n \mapsto n+1$, $\varsigma : n \mapsto -n$ resp. $\tau : n \mapsto n + (-1)^n$ (→ Definition 2.9.1).

Bibliography

[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.