A Normal Subgroup of the Group of Class-Wise Order-Preserving Residue Class-Wise Affine Permutations of the Integers

Stefan Kohl

Institut für Geometrie und Topologie
Universität Stuttgart
70550 Stuttgart / Germany

E-mail: kohl@mathematik.uni-stuttgart.de

Abstract

A permutation of $\mathbb{Z}$ is called *residue class-wise affine* if there is a positive integer m such that it is affine on residue classes (mod m). It is further called *class-wise order-preserving* if it is order-preserving on residue classes (mod m). In this article, a normal subgroup of the group of all class-wise order-preserving residue class-wise affine permutations of $\mathbb{Z}$ is determined.

MSC 2000: Primary 20B22, Secondary 20B27, 20B40

1 Introduction

1.1 Definition We call a mapping $f : \mathbb{Z} \to \mathbb{Z}$ *residue class-wise affine* if there is a positive integer m such that the restrictions of f to the residue classes $r(m) \in \mathbb{Z}/m\mathbb{Z}$ are all affine. This means that for any residue class $r(m)$ there are coefficients $a_{r(m)}$, $b_{r(m)}$, $c_{r(m)} \in \mathbb{Z}$ such that the restriction of the mapping f to the set $r(m) = \{r + km | k \in \mathbb{Z}\}$ is given by

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

We call the smallest possible m the *modulus* of f. To ensure uniqueness of the coefficients, we assume that $\gcd(a_{r(m)}, b_{r(m)}, c_{r(m)}) = 1$ and that $c_{r(m)} > 0$. We call f *class-wise order-preserving* if all coefficients $a_{r(m)}$ are positive.

It is easy to see that the residue class-wise affine permutations form a countable subgroup of $\mathrm{Sym}(\mathbb{Z})$.

1.2 Definition We denote the group of all residue class-wise affine permutations of $\mathbb{Z}$ by $\mathrm{RCWA}(\mathbb{Z})$. Further we denote the subgroup consisting of all class-wise order-preserving elements of $\mathrm{RCWA}(\mathbb{Z})$ by $\mathrm{RCWA}^+(\mathbb{Z})$.

The notation '$\mathrm{RCWA}(\mathbb{Z})$' reflects that generalizations to suitable rings other than $\mathbb{Z}$ make perfect sense (cp. [3]).

2 A Normal Subgroup of $\mathrm{RCWA}^+(\mathbb{Z})$

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

2.1 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 a residue class-wise affine mapping $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ with modulus m by the sum of the determinants of its restrictions to residue classes (mod m), i.e. we set

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

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 residue class-wise affine mapping usually does not yield an integer – injectivity, surjectivity and class-wise order-preservingness are all crucial.

2.2 Remark Let $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$ and $m := \mathrm{Mod}(\sigma)$. As in the definition of a residue class-wise affine 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:

2.3 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 by the residue class $r(m)^\alpha$ with distinguished representative r^α. Let $k \in \mathbb{N}$. We call the 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:

2.4 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:

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

Proof: We have to show that $\delta(\mathcal{P})$ mod 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

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

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. $\square$

2.6 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 this value is not needed in the sequel.

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

2.8 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

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

Inserting this into the expression in the last line of Definition 2.4 yields

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

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 $(\mathbb{Z}, +)$:

2.9 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 $\det(\sigma_1\sigma_2) = \det(\sigma_1) + \det(\sigma_2)$ and that there is a class-wise order-preserving bijective residue class-wise affine mapping of $\mathbb{Z}$ with determinant 1.

1. We would like to show that $\det(\sigma) \in \mathbb{Z}$. By Lemma 2.8 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 $\det(\sigma_1\sigma_2) = \det(\sigma_1) + \det(\sigma_2)$. Let $m := \mathrm{Mod}(\sigma_1) \cdot \mathrm{Mod}(\sigma_2)$. By construction, the partition $\mathcal{P} := \{[0/m], [1/m], \dots, [(m-1)/m]\}$ 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 2.8 we have

   $$\begin{aligned} \delta(\mathcal{P}) + \det(\sigma_1\sigma_2) \ &= \ \delta(\mathcal{P}^{\sigma_1\sigma_2}) \ = \ \delta(\mathcal{P}^{\sigma_1}) + \det(\sigma_2) \\ &= \ \delta(\mathcal{P}) + \det(\sigma_1) + \det(\sigma_2). \end{aligned}$$

   Subtracting $\delta(\mathcal{P})$ from the leftmost and the rightmost term reveals the claimed additivity of the determinant.

3. 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 $\nu \in \mathrm{RCWA}^+(\mathbb{Z}) : \ n \mapsto n+1$ lies in the preimage of 1. □

We would like to illustrate the additivity of the determinant by an example:

2.10 Example Let $\sigma_1, \sigma_2 \in \mathrm{RCWA}^+(\mathbb{Z})$ be given by

$$n \ \mapsto \ \begin{cases} \frac{3n}{5} & \text{if } n \in 0(5), \\ \frac{9n+1}{5} & \text{if } n \in 1(5), \\ \frac{3n+14}{5} & \text{if } n \in 2(5), \\ \frac{9n-2}{5} & \text{if } n \in 3(5), \\ \frac{9n+4}{5} & \text{if } n \in 4(5) \end{cases} \quad \text{resp.} \quad n \ \mapsto \ \begin{cases} \frac{n}{2} & \text{if } n \in 0(12), \\ n+1 & \text{if } n \in 1(6), \\ \frac{3n-8}{2} & \text{if } n \in 2(4), \\ n & \text{if } n \in 3(6), \\ n-3 & \text{if } n \in 4(12), \\ n-1 & \text{if } n \in 5(6) \cup 8(12). \end{cases}$$

Then it is

$$\sigma_1 \cdot \sigma_2 \in \mathrm{RCWA}^+(\mathbb{Z}): \quad n \ \longmapsto \ \begin{cases} \frac{3n}{10} & \text{if } n \in 0(20), \\ \frac{27n-37}{10} & \text{if } n \in 1(20), \\ \frac{3n-1}{5} & \text{if } n \in 2(20), \\ \frac{9n-7}{5} & \text{if } n \in 3(10) \cup 18(20), \\ \frac{9n-1}{5} & \text{if } n \in 9(10) \cup 4(20), \\ \frac{3n}{5} & \text{if } n \in 5(10), \\ \frac{9n-4}{5} & \text{if } n \in 6(10) \cup 11(20), \\ \frac{3n+19}{5} & \text{if } n \in 7(10), \\ \frac{27n-46}{10} & \text{if } n \in 8(20), \\ \frac{9n-40}{10} & \text{if } n \in 10(20), \\ \frac{9n+2}{10} & \text{if } n \in 12(20), \\ \frac{27n-28}{10} & \text{if } n \in 14(20). \end{cases}$$

We have

$$\begin{aligned} \det(\sigma_1) &= \frac{1}{9 \cdot 5} + \frac{14}{3 \cdot 5} - \frac{2}{9 \cdot 5} + \frac{4}{9 \cdot 5} \ = \ 1, \\ \det(\sigma_2) &= \frac{1}{1 \cdot 6} - \frac{8}{3 \cdot 4} - \frac{3}{1 \cdot 12} - \frac{1}{1 \cdot 6} - \frac{1}{1 \cdot 12} \ = \ -1 \end{aligned}$$

and

$$\begin{aligned} \det(\sigma_1 \cdot \sigma_2) &= -\frac{37}{27 \cdot 20} - \frac{1}{3 \cdot 20} - \frac{7}{9 \cdot 10} - \frac{7}{9 \cdot 20} - \frac{1}{9 \cdot 10} - \frac{1}{9 \cdot 20} \\ &\quad - \frac{4}{9 \cdot 10} - \frac{4}{9 \cdot 20} + \frac{19}{3 \cdot 10} - \frac{46}{27 \cdot 20} - \frac{40}{9 \cdot 20} + \frac{2}{9 \cdot 20} \\ &\quad - \frac{28}{27 \cdot 20} \\ &= 0 \ = \ 1 + -1 \ = \ \det(\sigma_1) + \det(\sigma_2). \end{aligned}$$

3 Background

Detailed background on the subject is given in [3].

Investigating residue class-wise affine groups by means of computation is feasible – see the package RCWA [2] for the computer algebra system GAP [1]. Both [3] and the manual of [2] discuss numerous examples of residue class-wise affine mappings and -groups.

4 Acknowledgements

The author would like to thank Wolfgang Rump for the idea of introducing the invariant δ for the proof of Theorem 2.9.

References

[1] The GAP Group. *GAP – Groups, Algorithms, and Programming; Version 4.4.6*, 2005. (`http://www.gap-system.org`).

[2] Stefan Kohl. *RCWA - Residue Class-Wise Affine Groups*, 2005. GAP package (`http://www.gap-system.org/Packages/rcwa.html`).

[3] Stefan Kohl. *Restklassenweise affine Gruppen*. Dissertation, Universität Stuttgart, 2005.