A Normal Subgroup of the Group of 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). In this article, a normal subgroup of the group of all 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 $c_{r(m)} > 0$.

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 $\mathrm{RCWA}(\mathbb{Z})$.

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

In this article we determine a normal subgroup of $\mathrm{RCWA}(\mathbb{Z})$.

We construct it as the kernel of an epimorphism from $\mathrm{RCWA}(\mathbb{Z})$ to $\mathbb{Z}^\times$. Having in mind the common term for the epimorphism $\mathrm{S}_n \to \mathbb{Z}^\times$, we call our epimorphism the *sign* mapping.

Transpositions in the symmetric group S_n cannot be written as products of two transpositions. There is no immediate analogue of this in $\mathrm{RCWA}(\mathbb{Z})$. For this reason the sign considered here cannot simply be derived from the one of finite-degree permutations. It will rather turn out to be a lift of an epimorphism $\widetilde{\mathrm{sgn}} : \langle n \mapsto n+1, n \mapsto -n \rangle \to \mathbb{Z}^\times$ to the whole of $\mathrm{RCWA}(\mathbb{Z})$.

2.1 Definition 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

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

where $\exp : z \mapsto e^{2\pi i z}$. Given this, we define the *sign* of a permutation $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ with modulus m by

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

2.2 Remark Let $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ and let m be the modulus of σ. 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 we have

$$\mathrm{sgn}(\sigma) \ = \ (-1)^{\dfrac{1}{m}\left(\displaystyle\sum_{r(m) \in \mathbb{Z}/m\mathbb{Z}} \frac{b_{r(m)}}{a_{r(m)}} + \sum_{r(m): \ a_{r(m)} < 0} (m - 2r)\right)}.$$

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

2.3 Definition We denote a residue class $r(m)$ with distinguished representative r and signed modulus m by $[r/m]$. The image $[r/m]^\alpha$ of such a residue class under an affine mapping $\alpha : n \mapsto (an+b)/c$ is defined by the residue class $r(m)^\alpha$ with distinguished representative r^α and modulus am/c. Let $k \in \mathbb{N}$. We call the decomposition

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

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

Let $\mathcal{P}$ be a partition of $\mathbb{Z}$ into finitely many residue classes with distinguished representatives and signed moduli. 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 $[r/m]$:

2.4 Definition Let $[r/m]$ be a residue class with signed modulus and distinguished representative. Then we set

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

For residue classes $r(m)$ not having a distinguished representative or a signed modulus we always assume $m > 0$ and $r \in \{0, \dots, m-1\}$, and set $\varrho\,(r(m)) := \varrho\,([r/m])$. Given a partition $\mathcal{P}$ of $\mathbb{Z}$ into finitely many residue classes with signed moduli and distinguished representatives, we set

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

and $\varrho\,(\mathbb{Z}) := (-1)^\epsilon \cdot \varrho\,(\mathcal{P})$, where $\epsilon \in \{0,1\}$ is chosen such that $\varrho\,(\mathbb{Z}) = \exp\,(t)$ for some $t \in [0, \frac{1}{2}[$.

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

2.5 Lemma *Let $\mathcal{P}$ be a partition of $\mathbb{Z}$ into finitely many residue classes with signed moduli and 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 signs of the moduli 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 $\mathcal{P}$, i.e. is well-defined.

Proof:

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

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

In case $m<0$ 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 any $k \in \mathbb{Z}$, the following holds:

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

   In case $m < 0$ 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 sign of the modulus 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. □

2.6 Remark We can explicitly determine $\varrho(\mathbb{Z})$: It is $\varrho(\mathbb{Z}) = \exp(1/4) = i$. However we will not need this value in the sequel.

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

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

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

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

$$\varrho(\mathcal{P}^\sigma) = \varrho(\mathcal{P})\cdot\mathrm{sgn}(\sigma),$$

thus

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

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

Proof: We assume that the mapping α is given by $n \mapsto (an+b)/c$ for certain coefficients $a,b,c \in \mathbb{Z}$. First assume $a > 0$. Then it holds that

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

Now assume $a < 0$. Then we have

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

thus our first assertion.

In order to get the corresponding assertion for a residue class-wise affine mapping σ and a partition $\mathcal{P}$ we simply refine $\mathcal{P}$ to a base for σ by representative stabilizing and orientation-preserving decomposition of residue classes in $\mathcal{P}$. Then we can apply the assertion proven above to the restrictions of σ to the residue classes in the refined partition. This way to proceed is correct due to Lemma 2.5. $\square$

Now we have all the necessary prerequisites needed for proving the main result of this article:

2.9 Theorem *The mapping*

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

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 $\mathrm{sgn}(\sigma_1\sigma_2) = \mathrm{sgn}(\sigma_1) \cdot \mathrm{sgn}(\sigma_2)$ and that there is a bijective residue class-wise mapping of $\mathbb{Z}$ with sign -1.

1. We would like to show that the sign of σ is a unit of $\mathbb{Z}$. By Lemma 2.8, for suitable $\epsilon \in \{0,1\}$ we have $\varrho\,(\mathbb{Z}) = \varrho\,(\mathbb{Z}^\sigma) = (-1)^\epsilon \cdot \varrho\,(\mathbb{Z}) \cdot \mathrm{sgn}(\sigma)$. Dividing the leftmost and the rightmost term by $\varrho\,(\mathbb{Z})$ completes the proof.

2. 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 residue classes with signed moduli and distinguished representatives. By Lemma 2.8 we have

$$\begin{aligned} \varrho\,(\mathcal{P}) \cdot \mathrm{sgn}(\sigma_1\sigma_2) \ &= \ \varrho\,(\mathcal{P}^{\sigma_1\sigma_2}) \ = \ \varrho\,(\mathcal{P}^{\sigma_1}) \cdot \mathrm{sgn}(\sigma_2) \\ &= \ \varrho\,(\mathcal{P}) \cdot \mathrm{sgn}(\sigma_1) \cdot \mathrm{sgn}(\sigma_2). \end{aligned}$$

   Dividing the leftmost and the rightmost term by $\varrho\,(\mathcal{P})$ finishes the proof of our assertion.

3. The signs of $\nu : n \mapsto n+1$ and $\varsigma : n \mapsto -n$ are -1. □

We would like to illustrate the multiplicativity of the sign by an example:

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

$$n \mapsto \begin{cases} 5n+1 & \text{if } n \in 0(2), \\ \frac{n-1}{5} & \text{if } n \in 1(10), \\ n+10 & \text{if } n \in 5(10), \\ n & \text{otherwise} \end{cases} \quad \text{resp.} \quad n \mapsto \begin{cases} -n & \text{if } n \in 0(12), \\ n & \text{if } n \in 1(4), \\ \frac{3n+2}{2} & \text{if } n \in 2(4), \\ n-1 & \text{if } n \in 3(12) \cup 7(12), \\ -2n+16 & \text{if } n \in 4(12), \\ \frac{-n+17}{3} & \text{if } n \in 8(12), \\ 2n-2 & \text{if } n \in 11(12). \end{cases}$$

Then it is

$$\sigma_1 \cdot \sigma_2 \in \mathrm{RCWA}(\mathbb{Z}) : \quad n \ \mapsto \begin{cases} 5n+1 & \text{if } n \in 0(4), \\ \frac{-n+1}{5} & \text{if } n \in 1(60), \\ 10n & \text{if } n \in 2(12), \\ n-1 & \text{if } n \in 3(60) \cup \ 7(60) \cup 19(60) \\ & \qquad \cup 27(60) \cup 39(60) \cup 43(60), \\ n+9 & \text{if } n \in 5(60) \cup 45(60), \\ 5n & \text{if } n \in 6(12) \cup 10(12), \\ n & \text{if } n \in 9(20) \cup 13(20) \cup 17(20), \\ \frac{3n+7}{10} & \text{if } n \in 11(20), \\ n+10 & \text{if } n \in 15(20), \\ \frac{-2n+82}{5} & \text{if } n \in 21(60), \\ 2n-2 & \text{if } n \in 23(60) \cup 47(60) \cup 59(60), \\ 2n+18 & \text{if } n \in 25(60), \\ \frac{-n+86}{15} & \text{if } n \in 41(60). \end{cases}$$

We have

$$\begin{aligned} \mathrm{sgn}(\sigma_1) \ &= \ \exp\left(\frac{1}{20}\right) \cdot \exp\left(-\frac{1}{20}\right) \cdot \exp\left(\frac{1}{2}\right) \ = \ \exp\left(\frac{1}{2}\right) \ = \ -1, \\ \mathrm{sgn}(\sigma_2) \ &= \ \exp\left(0+0+\frac{1}{2}\right) \cdot \exp\left(\frac{1}{12}\right) \cdot \exp\left(-\frac{1}{24}\right)^2 \\ & \quad \cdot \exp\left(\frac{1}{3}-\frac{1}{3}+\frac{1}{2}\right) \cdot \exp\left(\frac{17}{24}-\frac{2}{3}+\frac{1}{2}\right) \cdot \exp\left(-\frac{1}{24}\right) \\ &= \ \exp\left(\frac{1}{2}\right) \ = \ -1 \end{aligned}$$

and

$$\begin{aligned} \mathrm{sgn}(\sigma_1 \cdot \sigma_2) \ &= \ \exp\left(\frac{1}{40}\right) \cdot \exp\left(\frac{1}{120}-\frac{1}{60}+\frac{1}{2}\right) \cdot \exp\left(-\frac{1}{120}\right)^6 \\ & \quad \cdot \exp\left(\frac{3}{40}\right)^2 \cdot \exp\left(\frac{7}{120}\right) \cdot \exp\left(\frac{1}{4}\right) \cdot \exp\left(\frac{41}{120}-\frac{7}{20}+\frac{1}{2}\right) \\ & \quad \cdot \exp\left(-\frac{1}{120}\right)^3 \cdot \exp\left(\frac{3}{40}\right) \cdot \exp\left(\frac{43}{60}-\frac{41}{60}+\frac{1}{2}\right) \\ &= \ \exp(2) \ = \ 1 \ = \ -1 \cdot -1 \ = \ \mathrm{sgn}(\sigma_1) \cdot \mathrm{sgn}(\sigma_2). \end{aligned}$$

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.

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.