TWO INVARIANTS OF RESIDUE-CLASS-WISE AFFINE PERMUTATIONS OF THE INTEGERS

STEFAN KOHL

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).

We determine two in some sense canonical epimorphisms $\pi^+ : \mathrm{RCWA}^+(\mathbb{Z}) \to (\mathbb{Z}, +)$ and $\pi^- : \mathrm{RCWA}(\mathbb{Z}) \to \mathbb{Z}^\times$, where $\mathrm{RCWA}(\mathbb{Z})$ denotes the group consisting of all residue-class-wise affine permutations of $\mathbb{Z}$, and $\mathrm{RCWA}^+(\mathbb{Z})$ denotes its subgroup formed by the class-wise order-preserving elements.

1. INTRODUCTION

The subject of this note are bijective mappings of the following type:

Definition 1.1. 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, i.e. given by

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

for certain coefficients $a_{r(m)}$, $b_{r(m)}$, $c_{r(m)} \in \mathbb{Z}$ depending on $r(m)$. We call the smallest possible m the *modulus* of f, written $\mathrm{Mod}(f)$.

For reasons of uniqueness, 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 $a_{r(m)}$ are positive.

The *permutations* of this kind obviously form a countable subgroup of $\mathrm{Sym}(\mathbb{Z})$.

Definition 1.2. We denote the group of all residue-class-wise affine permutations of $\mathbb{Z}$ by $\mathrm{RCWA}(\mathbb{Z})$, and call its subgroups *residue-class-wise affine* groups.

Further we denote the subgroup of $\mathrm{RCWA}(\mathbb{Z})$ which consists of all class-wise order-preserving elements by $\mathrm{RCWA}^+(\mathbb{Z})$.

In this note, we prove the following:

Theorem 1.3. There are epimorphisms

$$\pi^+ : \ \mathrm{RCWA}^+(\mathbb{Z}) \to (\mathbb{Z}, +), \quad \sigma \ \mapsto \ \frac{1}{m} \sum_{r(m) \in \mathbb{Z}/m\mathbb{Z}} \frac{b_{r(m)}}{|a_{r(m)}|}$$

and

$$\pi^- : \ \mathrm{RCWA}(\mathbb{Z}) \to \mathbb{Z}^\times, \quad \sigma \ \mapsto \ (-1)^{\pi^+(\sigma) + \sum_{r(m):\ a_{r(m)} < 0} \frac{m - 2r}{m}},$$

where we use the notation for the coefficients introduced in Definition 1.1.

2000 *Mathematics Subject Classification.* Primary 20B22, Secondary 20B27, 20B40.

The relevance of these results is basically the following:

In [1] it is shown that the subgroups of the kernels of π^+ resp. π^- which are generated by the torsion elements are simple. Further it is conjectured that these subgroups are improper, i.e. that the kernels are in fact equal to these simple groups.

For a general introduction to residue-class-wise affine groups, we refer to [2]. These groups are accessible to computational methods. In this context we refer to the package RCWA [3] for the computer algebra system GAP [4].

2. The Epimorphism π^+

In this section we construct our epimorphism π^+ from $\mathrm{RCWA}^+(\mathbb{Z})$ to $(\mathbb{Z}, +)$.

Definition 2.1. Let $r(m)$ be a residue class and let $\alpha : n \mapsto (an + b)/c$ be an order-preserving affine mapping with source $r(m)$. Then we put $\pi^+(\alpha) := b/(am)$.

Further given $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$, we put $\pi^+(\sigma) := \sum_{r(m)\in\mathbb{Z}/m\mathbb{Z}} \pi^+(\sigma|_{r(m)})$, where m denotes the modulus of σ.

It is easy to see that π^+ is the mapping given in Theorem 1.3.

Evaluating the expression given there for an arbitrary residue-class-wise affine mapping usually does not yield an integer, unless the mapping is bijective and class-wise order-preserving.

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

Definition 2.2. We denote a residue class $r(m)$ with distinguished representative r and signed modulus m by $[r/m]$. We define the image $[r/m]^\alpha$ of such a residue class under an affine mapping α 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

$$[r/m] \ = \ [r/(km)] \cup [(r+m)/(km)] \cup \cdots \cup [(r+(k-1)m)/(km)]$$

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 successive decomposition of residue classes in $\mathcal{P}$ in the above way.

We assign rational numbers to such residue classes:

Definition 2.3. Given a residue class $[r/m]$, let $\delta([r/m]) := r/m - 1/2$. Given a partition $\mathcal{P}$ of $\mathbb{Z}$ into finitely many residue classes with distinguished representatives, let $\delta(\mathcal{P}) := \sum_{[r/m]\in\mathcal{P}} \delta([r/m])$. Furthermore we define the value $\delta(\mathbb{Z})$ by $\delta(\mathcal{P}) - \lfloor \delta(\mathcal{P}) \rfloor$.

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

Lemma 2.4. *The value $\delta(\mathbb{Z})$ is independent of the choice of the partition $\mathcal{P}$.*

Proof. We need to show that $\delta(\mathcal{P})$ mod 1 is invariant under representative-stabilizing refinements of $\mathcal{P}$ and under changes of the representatives of the residue classes in $\mathcal{P}$. Given a residue class $[r/m]$ and $k \in \mathbb{N}$, we have

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

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

$$\delta([r/m]) \ = \ r/m - 1/2 \ = \ (r+km)/m - 1/2 - k \ = \ \delta([(r+km)/m]) - k.$$

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

Remark 2.5. 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.

Definition 2.6. 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.

Lemma 2.7. *Let $\alpha: \ n \mapsto (an+b)/c$ be an order-preserving affine mapping whose source is a residue class $[r/m]$. Then, $\delta([r/m]^\alpha) = \delta([r/m]) + \pi^+(\alpha)$. Let $\sigma \in \mathrm{RCWA}^+(\mathbb{Z})$, and let $\mathcal{P}$ be a base for σ. Then, $\delta(\mathcal{P}^\sigma) = \delta(\mathcal{P}) + \pi^+(\sigma)$.*

Proof. We have $\delta([r/m]^\alpha) \ = \ \delta([((ar+b)/c)/(am/c)]) \ = \ r/m - 1/2 + b/(am) \ = \delta([r/m]) + \pi^+(\alpha)$. The second assertion is now immediate. □

Now we have all necessary prerequisites needed for proving our first result:

Theorem 2.8. *The mapping $\pi^+ : \mathrm{RCWA}^+(\mathbb{Z}) \to (\mathbb{Z}, +)$ is an epimorphism.*

Proof. Let $\sigma_1, \sigma_2, \sigma \in \mathrm{RCWA}^+(\mathbb{Z})$. We have to show that $\pi^+(\sigma)$ is an integer, that $\pi^+(\sigma_1\sigma_2) = \pi^+(\sigma_1) + \pi^+(\sigma_2)$ and that 1 lies in the image of π^+.

(1) We show that $\pi^+(\sigma) \in \mathbb{Z}$.
By Lemma 2.7 we have $\delta(\mathbb{Z}) = \delta(\mathbb{Z}) + \pi^+(\sigma) - \lfloor \delta(\mathbb{Z}) + \pi^+(\sigma) \rfloor$. Thus $\pi^+(\sigma) = \lfloor \delta(\mathbb{Z}) + \pi^+(\sigma) \rfloor \in \mathbb{Z}$.

(2) We show that $\pi^+(\sigma_1\sigma_2) = \pi^+(\sigma_1) + \pi^+(\sigma_2)$.
Let $m := \mathrm{Mod}(\sigma_1) \cdot \mathrm{Mod}(\sigma_2)$, and $\mathcal{P} := \{[0/m], [1/m], \dots, [(m-1)/m]\}$. By construction, $\mathcal{P}$ 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 2.7 we have

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

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

(3) We have already shown that π^+ is an homomorphism from $\mathrm{RCWA}^+(\mathbb{Z})$ to $(\mathbb{Z}, +)$. It is indeed an epimorphism, since $n \mapsto n+1$ lies in the preimage of 1. □

3. The Epimorphism π^-

In this section we construct our epimorphism π^- from $\mathrm{RCWA}(\mathbb{Z})$ to $\mathbb{Z}^\times$.

Definition 3.1. Let $r(m) \subseteq \mathbb{Z}$ be a residue class, and let $\alpha : n \mapsto (an+b)/c$ be an affine mapping with source $r(m)$. Further let $\exp : z \mapsto e^{2\pi i z}$. We put

$$\pi^-(\alpha) \ := \ \begin{cases} \exp(+b/(2am)) & \text{if } \ a > 0, \\ \exp(-b/(2am) - r/m + 1/2) & \text{if } \ a < 0. \end{cases}$$

Further, given $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ we put $\pi^-(\sigma) := \prod_{r(m) \in \mathbb{Z}/m\mathbb{Z}} \pi^-(\sigma|_{r(m)})$, where m denotes the modulus of σ.

It is easy to see that π^- is the mapping given in Theorem 1.3.

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

Definition 3.2. Given a residue class $[r/m]$ with signed modulus and distinguished representative, we set $\varrho\,([r/m]) := \exp\,(\mathrm{sgn}(m) \cdot (r/m - 1/2)/2)$. Given a partition $\mathcal{P}$ of $\mathbb{Z}$ into a finite number of residue classes with signed moduli and distinguished representatives, we set $\varrho\,(\mathcal{P}) := \prod_{[r/m] \in \mathcal{P}} \varrho\,([r/m])$ 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:

Lemma 3.3. *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:

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

In case $m < 0$ just the signs of all exponents are changed, thus $\varrho\,(\mathcal{P})$ 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:

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

In case $m < 0$ just the signs of all exponents are changed, 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 the value of $\varrho\,(\mathcal{P})$ by a factor of

$$\frac{\varrho\,([r/\text{-}m])}{\varrho\,([r/m])} \;=\; \frac{\exp\,(-(r/\text{-}m - 1/2)/2)}{\exp\,((r/m - 1/2)/2)} \;=\; \exp\,(1/2) \;=\; -1,$$

as claimed. $\square$

Remark 3.4. 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.

Lemma 3.5. *Let α be an affine mapping with source $r(m)$. Then we have $\varrho([r/m]^\alpha) = \varrho([r/m]) \cdot \pi^-(\alpha)$.*

Let $\sigma \in \mathrm{RCWA}(\mathbb{Z})$, and let $\mathcal{P}$ be a partition of $\mathbb{Z}$ into finitely many residue classes with distinguished representatives and signed moduli. Then we have $\varrho(\mathcal{P}^\sigma) = \varrho(\mathcal{P}) \cdot \pi^-(\sigma)$. Therefore for suitable $\epsilon \in \{0,1\}$ it is $\varrho(\mathbb{Z}^\sigma) = (-1)^\epsilon \cdot \varrho(\mathbb{Z}) \cdot \pi^-(\sigma)$.

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 we have

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

Now assume $a < 0$. Then we have

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

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 successive representative-stabilizing and orientation-preserving decomposition of residue classes in $\mathcal{P}$. Then we can apply the assertion proved above to the restrictions of σ to the residue classes in the refined partition. This way to proceed is correct due to Lemma 3.3. □

Now we can prove our second result:

Theorem 3.6. *The mapping π^- is an epimorphism from $\mathrm{RCWA}(\mathbb{Z})$ to $\mathbb{Z}^\times$.*

Proof. Let $\sigma_1, \sigma_2, \sigma \in \mathrm{RCWA}(\mathbb{Z})$. We have to show that $\pi^-(\sigma)$ is a unit of $\mathbb{Z}$, that $\pi^-(\sigma_1\sigma_2) = \pi^-(\sigma_1) \cdot \pi^-(\sigma_2)$ and that -1 lies in the image of π^-.

(1) We show that the sign of σ is a unit of $\mathbb{Z}$. By Lemma 3.5, for suitable $\epsilon \in \{0,1\}$ we have $\varrho(\mathbb{Z}) = \varrho(\mathbb{Z}^\sigma) = (-1)^\epsilon \cdot \varrho(\mathbb{Z}) \cdot \pi^-(\sigma)$. Dividing the leftmost and the rightmost term by $\varrho(\mathbb{Z})$ completes the proof.

(2) We show that $\pi^-(\sigma_1\sigma_2) = \pi^-(\sigma_1) \cdot \pi^-(\sigma_2)$. Let $\mathcal{P}$ be a partition of $\mathbb{Z}$ into finitely many residue classes with signed moduli and distinguished representatives. By Lemma 3.5 we have

$$\begin{aligned}
\varrho(\mathcal{P}) \cdot \pi^-(\sigma_1\sigma_2) &= \varrho(\mathcal{P}^{\sigma_1\sigma_2}) = \varrho(\mathcal{P}^{\sigma_1}) \cdot \pi^-(\sigma_2) \\
&= \varrho(\mathcal{P}) \cdot \pi^-(\sigma_1) \cdot \pi^-(\sigma_2).
\end{aligned}$$

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

(3) The images of $n \mapsto n+1$ and $n \mapsto -n$ under π^- are -1. □

4. ACKNOWLEDGEMENTS

I thank Wolfgang Rump for the idea of introducing the invariant δ in the proof of Theorem 2.8.

REFERENCES

1. Stefan Kohl, *A simple group generated by involutions interchanging residue classes of the integers*, Preprint, http://www.cip.mathematik.uni-stuttgart.de/ kohlsn/preprints/simplegp.pdf.
2. ______, *Restklassenweise affine Gruppen*, Dissertation, Universität Stuttgart, 2005, http://deposit.d-nb.de/cgi-bin/dokserv?idn=977164071.
3. ______, *RCWA - Residue-Class-Wise Affine Groups; Version 2.5.4*, 2007, GAP package, published at http://www.gap-system.org/Packages/rcwa.html.
4. The GAP Group, *GAP – Groups, Algorithms, and Programming; Version 4.4.10*, 2007, http://www.gap-system.org.

INSTITUT FÜR GEOMETRIE UND TOPOLOGIE, PFAFFENWALDRING 57, UNIVERSITÄT STUTTGART 70550 STUTTGART, GERMANY

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