On Normal Subgroups 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 it is shown that any nontrivial normal subgroup of the group of all residue class-wise affine permutations of $\mathbb{Z}$ contains the elements $\tau : n \mapsto n + (-1)^n$ and $\nu^2 : n \mapsto n + 2$. Note that this does not hold for $\nu : n \mapsto n + 1$ (cp. Section 2.12 in [4]).

MSC 2000: Primary 20B22, Secondary 20-04

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, written $\mathrm{Mod}(f)$. 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 *integral* if all coefficients $c_{r(m)}$ equal 1.

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 $\mathrm{RCWA}(\mathbb{Z})$, and call its subgroups *residue class-wise affine* groups.

The notation 'RCWA($\mathbb{Z}$)' reflects that generalizations to suitable rings other than $\mathbb{Z}$ make perfect sense (cp. [4]).

Any finite symmetric group S_m has a monomorphic image in $\mathrm{RCWA}(\mathbb{Z})$: Let $m \geqslant 2$, and let S_m act naturally on the set $\{0, 1, \ldots, m-1\}$. Then an example of a corresponding monomorphism is

$$\varphi_m : \ \mathrm{S}_m \to \mathrm{RCWA}(\mathbb{Z}), \ \ \sigma \mapsto (\sigma^{\varphi_m} : \ n \mapsto n + (n \mod m)^\sigma - n \mod m) .$$

The conjugate of the image of φ_m under the mapping $n \mapsto n - \lfloor m/2 \rfloor$ acts m - transitively on $\{-\lfloor m/2 \rfloor, \ldots, m - \lfloor m/2 \rfloor - 1\}$. Since m can be chosen arbitrarily large, the group $\mathrm{RCWA}(\mathbb{Z})$ acts highly transitively on $\mathbb{Z}$. By Corollary 7.2A in [1], this implies that any nontrivial normal subgroup of $\mathrm{RCWA}(\mathbb{Z})$ acts highly transitively on $\mathbb{Z}$ as well. Since the action of an abelian group is at most 1-transitive, this means in particular that $\mathrm{RCWA}(\mathbb{Z})$ has a trivial centre. As any highly transitive permutation group has a subgroup which acts on a subset of cardinality $\geqslant 5$ as full symmetric group, we can also conclude that $\mathrm{RCWA}(\mathbb{Z})$ does not have nontrivial solvable normal subgroups.

There are two entirely different classes of residue class-wise affine groups and -permutations. One of these classes comprises what could be called the 'trivial cases'. The members of the other have typically a quite complicate structure and are often very difficult to investigate:

1.3 Definition We call a residue class-wise affine group G *tame* if the set of moduli of its elements is bounded, and *wild* otherwise. We call a residue class-wise affine permutation *tame* if it generates a tame cyclic group, and *wild* otherwise.

Obviously, finite residue class-wise affine groups and integral residue class-wise affine permutations are tame. It can be shown by elementary arguments that tameness is a class invariant, i.e. that it is invariant under conjugation (see Lemma 1.8.3 in [4]). For this, one looks at the equation $(\alpha^\beta)^k = (\alpha^k)^\beta$ for $\alpha, \beta \in \mathrm{RCWA}(\mathbb{Z})$ and $k \in \mathbb{Z}$ and convinces oneself that conjugation by β increases the modulus of an element at most by a constant factor which solely depends on β. Further it can be shown that a group $G < \mathrm{RCWA}(\mathbb{Z})$ is tame if and only if it *respects* some partition of $\mathbb{Z}$ into finitely many residue classes (see Theorem 2.5.8 in [4]):

1.4 Definition Let $\mathcal{P}$ be a partition of $\mathbb{Z}$ into finitely many residue classes. We say that a group $G < \mathrm{RCWA}(\mathbb{Z})$ *respects* $\mathcal{P}$ 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 denote the permutation group induced by G on $\mathcal{P}$ by $G_{\mathcal{P}}$. We say that a permutation $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ *respects* $\mathcal{P}$ if the cyclic group $\langle\sigma\rangle$ does so. We denote the permutation induced by σ on $\mathcal{P}$ by $\sigma_{\mathcal{P}}$. In case $G_{\mathcal{P}} = 1$ resp. $\sigma_{\mathcal{P}} = 1$ we say that G resp. σ *fixes* $\mathcal{P}$.

In the sequel we need the following three infinite series of tame elements of particularly simple structure:

1.5 Definition Let $\nu \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto n+1$, $\varsigma \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto -n$ and $\tau \in \mathrm{RCWA}(\mathbb{Z}) : n \mapsto n + (-1)^n$. Further let $r(m)$ be a residue class, and let $r_1(m_1)$ and $r_2(m_2)$ be disjoint residue classes.

- We define the *class shift* $\nu_{r(m)} \in \mathrm{RCWA}(\mathbb{Z})$ by

$$\nu_{r(m)} : \quad n \ \mapsto \begin{cases} n+m & \text{if } \ n \in r(m), \\ n & \text{otherwise.} \end{cases}$$

- We define the *class reflection* $\varsigma_{r(m)} \in \mathrm{RCWA}(\mathbb{Z})$ by

$$\varsigma_{r(m)} : \quad n \ \mapsto \begin{cases} -n+2r & \text{if } \ n \in r(m), \\ n & \text{otherwise,} \end{cases}$$

  where we assume $0 \leqslant r < m$.

- We define the *class transposition* $\tau_{r_1(m_1),r_2(m_2)} \in \mathrm{RCWA}(\mathbb{Z})$ by

$$\tau_{r_1(m_1),r_2(m_2)} : \quad n \ \mapsto \begin{cases} \dfrac{m_2 n + (m_1 r_2 - m_2 r_1)}{m_1} & \text{if } \ n \in r_1(m_1), \\ \dfrac{m_1 n + (m_2 r_1 - m_1 r_2)}{m_2} & \text{if } \ n \in r_2(m_2), \\ n & \text{otherwise,} \end{cases}$$

  where we assume $0 \leqslant r_1 < m_1$ and $0 \leqslant r_2 < m_2$.

Looking at respected partitions, it is easy to see that all tame elements of $\mathrm{RCWA}(\mathbb{Z})$ can be written as products of class shifts, class reflections and class transpositions. It is an open problem whether the tame elements generate the group $\mathrm{RCWA}(\mathbb{Z})$ or a proper normal subgroup thereof (cp. Conjecture 2.9.8 in [4] and the corresponding factorization routine in [3]).

1.6 Lemma *Class shifts $\nu_{r(m)} \neq \nu$ are conjugate in* RCWA($\mathbb{Z}$). *The same holds for class reflections $\varsigma_{r(m)} \neq \varsigma$ resp. class transpositions $\tau_{r_1(m_1),r_2(m_2)} \neq \tau$.*

Products of the same numbers of class shifts, inverses of class shifts, class reflections and class transpositions, each are conjugate as well, provided that the supports of the factors of any of them are pairwisely disjoint and do not entirely cover $\mathbb{Z}$ up to a finite complement.

Proof: The assertions hold since given two ordered partitions $\mathcal{P}_1$ and $\mathcal{P}_2$ of $\mathbb{Z}$ into the same number of residue classes with distinguished representatives, there is always a $\sigma \in$ RCWA($\mathbb{Z}$) which is affine on the elements of $\mathcal{P}_1$ such that $\mathcal{P}_1^\sigma = \mathcal{P}_2$. □

2 Elements Lying in Any Normal Subgroup of RCWA($\mathbb{Z}$)

The aim of this article is to show that any nontrivial normal subgroup of RCWA($\mathbb{Z}$) contains the elements $\tau : n \mapsto n + (-1)^n$ and $\nu^2 : n \mapsto n + 2$.

We need some lemmata:

2.1 Lemma *Let $\sigma \in$ RCWA($\mathbb{Z}$) and $m :=$ Mod(σ). Let $\upsilon \in$ RCWA($\mathbb{Z}$) further be an integral mapping which respects and fixes the partition $\mathbb{Z}/m\mathbb{Z}$ of $\mathbb{Z}$. Then the commutator $\gamma := [\sigma, \upsilon]$ is integral.*

Proof: Let α be an affine partial mapping of γ. By definition, α is the product of affine partial mappings

- $\alpha_{\sigma^{-1}} : n \mapsto (c_1 n - b_1)/a_1$ of σ^{-1},
- $\alpha_{\upsilon^{-1}} : n \mapsto u_1 n + r_1(1 - u_1) + k_1 m$ of υ^{-1},
- $\alpha_\sigma : \quad n \mapsto (a_2 n + b_2)/c_2$ of σ and
- $\alpha_\upsilon : \quad n \mapsto u_2 n + r_2(1 - u_2) + k_2 m$ of υ

for certain coefficients $a_1, a_2, b_1, b_2, c_1, c_2, r_1, r_2, k_1, k_2 \in \mathbb{Z}$ and $u_1, u_2 \in \mathbb{Z}^\times$. Since the mapping υ respects and fixes the partition $\mathbb{Z}/m\mathbb{Z}$, we have $a_1 = a_2$, $b_1 = b_2$ and $c_1 = c_2$. Let

$$\varphi : \ \mathrm{Aff}(\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Q}), \quad (n \mapsto an + b) \ \mapsto \ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},$$

where Aff($\mathbb{Q}$) denotes the affine group over the rational field.

Since the determinant of a product of matrices is the product of the determinants of the factors, we have

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

This implies that $\alpha \in \mathrm{Aff}(\mathbb{Z}) = \langle n \mapsto n+1, n \mapsto -n \rangle$. We conclude that γ is integral, as claimed. □

2.2 Lemma *Any nontrivial normal subgroup of* RCWA($\mathbb{Z}$) *has an integral element* $\sigma \neq 1$.

Proof: Let $\tilde{\sigma} \in N \setminus \{1\}$ and $m := \mathrm{Mod}(\tilde{\sigma})$. Without loss of generality we can assume that there is a residue class $r(m)$ such that $r(m)^{\tilde{\sigma}} \neq r(m)$ – otherwise $\tilde{\sigma}$ already would be integral. Put $\sigma := [\tilde{\sigma}, \nu_{r(m)}] = \tilde{\sigma}^{-1}\tilde{\sigma}^{\nu_{r(m)}}$. By definition of a normal subgroup, we have $\sigma \in N$. Further since $r(m)^{\tilde{\sigma}} \neq r(m)$ it is $\sigma \neq 1$, and by Lemma 2.1, σ is integral. □

Now we can prove our theorem:

2.3 Theorem *Any nontrivial normal subgroup of* RCWA($\mathbb{Z}$) *contains the elements* $\tau : n \mapsto n + (-1)^n$ *and* $\nu^2 : n \mapsto n+2$.

Proof: By Lemma 2.2, any nontrivial normal subgroup N of RCWA($\mathbb{Z}$) has an integral element $\sigma \neq 1$. Let $m \geqslant 3$ be a multiple of the modulus of σ. We choose a residue class $r(m) \in \mathbb{Z}/m\mathbb{Z}$ such that $\sigma|_{r(m)} \neq 1$, and put $\tilde{\sigma} := [\sigma, \nu_{r(m)}] = \sigma^{-1}\sigma^{\nu_{r(m)}} \in N$. We have to distinguish three different cases:

1. It is $r(m)^\sigma \neq r(m)$. Then

$$\tilde{\sigma} \;=\; \begin{cases} \nu_{r(m)}\nu_{r(m)^\sigma}^{-1} & \text{if } \sigma|_{r(m)} \text{ is order-preserving,} \\ \nu_{r(m)}\nu_{r(m)^\sigma} & \text{if } \sigma|_{r(m)} \text{ is order-reversing.} \end{cases}$$

   By Lemma 1.6, in the former case $\tilde{\sigma}$ is conjugate to $\nu_{1(3)}\nu_{2(3)}^{-1}$ and in the latter it is conjugate to $\nu_{1(3)}\nu_{2(3)}$. Since $(\nu_{1(3)}\nu_{2(3)})^{\varsigma_{2(3)}} = \nu_{1(3)}\nu_{2(3)}^{-1}$, we know that always both of these elements lie in N.

2. It is $r(m)^\sigma = r(m)$ and $\mathrm{ord}(\sigma|_{r(m)}) = 2$. Then we have $\tilde{\sigma} = \nu_{r(m)}^2$. By Lemma 1.6, in this case $\tilde{\sigma}$ is conjugate to $\nu_{1(2)}^2$.

3. It is $r(m)^\sigma = r(m)$ and $\mathrm{ord}(\sigma|_{r(m)}) = \infty$. Then σ and $\nu_{r(m)}$ commute. But for some $k \in \mathbb{Z} \setminus \{0\}$ we have $[\sigma, \varsigma_{r(m)}] = \nu_{r(m)}^{2k}$. Again by Lemma 1.6, the permutation $\nu_{r(m)}^{2k}$ is conjugate to $\nu_{1(2)}^{2k}$.

We conclude that the normal subgroup N contains at least one of the elements $\nu_{1(3)}\nu_{2(3)}^{\pm 1}$, $\nu_{1(2)}^2$ resp. $\nu_{1(2)}^{2k}$ for some $k \in \mathbb{Z} \setminus \{0\}$.

Let $k \in \mathbb{Z} \setminus \{0\}$ and let p be a prime which does not divide $2k$. Then $[[\nu_{1(2)}^{2k}, \nu_{1(p)}], \nu_{1(2p)}] = \nu_{1(2p)}\nu_{p+1(2p)}^{-1} =: \hat{\sigma}$. If $\nu_{1(2)}^{2k} \in N$, then so is $\hat{\sigma}$. By Lemma 1.6, $\hat{\sigma}$ is conjugate to $\nu_{1(3)}\nu_{2(3)}^{-1}$, which in turn is conjugate to $\nu_{1(3)}\nu_{2(3)}$. Let

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

(cp. [5], page 4). Then it is $\nu_{1(2)}^2 = \left(\nu_{1(3)}\nu_{2(3)}\right)^{\alpha^{-1}} \in N$. Thus as all class shifts $\neq \nu$ are conjugate, the normal subgroup N contains any square of such a class shift. Let

$$\gamma_1 \in \mathrm{RCWA}(\mathbb{Z}): \quad n \;\mapsto\; \begin{cases} \frac{n}{2} & \text{if } n \in 0(4), \\ \frac{-3n+9}{2} & \text{if } n \in 1(4), \\ \frac{3n+4}{2} & \text{if } n \in 2(4), \\ \frac{3n-7}{2} & \text{if } n \in 3(4). \end{cases}$$

Then we have

$$\underbrace{\tau_{0(6),1(6)} \cdot \tau_{0(6),3(6)}}_{=:\,\theta} \;=\; \left(\nu_{1(2)}^2\right)^{\gamma_1} \cdot [\nu_{1(2)}^2, \nu_{0(3)}] \;\in\; N.$$

Further let $\gamma_2 := \nu_{4(6)} \cdot \nu_{0(6)}^{-1} \cdot \nu_{2(6)}^{-1} \cdot \tau_{0(6),1(6)} \cdot \tau_{0(6),4(6)} \cdot \tau_{3(6),5(6)}$. Then it is

$$\tau_{1(3),2(3)} \;=\; \left(\theta \cdot \theta^{\tau_{2(6),3(6)}}\right)^{\gamma_2} \;\in\; N.$$

Thus as all class transpositions $\neq \tau$ are conjugate, the normal subgroup N contains any of them. Let $\upsilon := \nu_{1(2)}^2 \in N$, $\gamma_3 := \tau_{1(3),2(3)} \cdot \tau_{0(6),3(6)} \cdot \tau_{2(3),0(6)} \cdot \alpha^{-1}$ and $\gamma_4 := \tau_{1(3),3(6)} \cdot \alpha^{-1}$. Then we have

$$\nu^2 \;=\; \upsilon^{\alpha^{\nu^3}} \cdot\; \upsilon^{\alpha^{\nu}} \cdot\; \upsilon^{\alpha^{\nu^{-1}}} \cdot\; \left(\upsilon \cdot \upsilon^{\tau}\right)^{-1} \;\in\; N$$

and

$$\tau \;=\; \tau_{1(3),2(3)}^{\gamma_3} \cdot \tau_{1(3),2(3)}^{\gamma_4} \;\in\; N,$$

as claimed. □

3 Background and Remarks

Detailed background on the subject is given in [4].

Performing the computations in this article by hand would have been tedious and error-prone. For this reason, wherever possible they have been done using the package RCWA [3] for the computer algebra system GAP [2].

References

[1] John D. Dixon and Brian Mortimer. *Permutation Groups*. Number 163 in Graduate Texts in Mathematics. Springer-Verlag, 1996.

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

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

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

[5] Günther J. Wirsching. The dynamical system on the natural numbers generated by the 3n+1 function. Habilitationsschrift, Katholische Universität Eichstätt, 1996.