SIMPLE GROUPS GENERATED BY INVOLUTIONS INTERCHANGING RESIDUE CLASSES MODULO LATTICES IN $\mathbb{Z}^d$

STEFAN KOHL

ABSTRACT. We present a series of countable simple groups, whose generators are involutions which interchange disjoint residue classes modulo lattices in $\mathbb{Z}^d$ ($d \in \mathbb{N}$). This work is motivated by the famous $3n+1$ conjecture.

1. INTRODUCTION

This paper continues the work which has been carried out in [1]. The subject of that article is the discussion of the following simple group, which is generated by involutions interchanging disjoint residue classes of the integers:

Definition 1.1. Let $\mathrm{CT}(\mathbb{Z})$ be the group generated by the set of all *class transpositions*: Given disjoint residue classes $r_1(m_1)$ and $r_2(m_2)$ of $\mathbb{Z}$, we define the *class transposition* $\tau_{r_1(m_1),r_2(m_2)} \in \mathrm{Sym}(\mathbb{Z})$ as the permutation which interchanges $r_1 + km_1$ and $r_2 + km_2$ for each integer k and which fixes all other points. Here we assume that $0 \leqslant r_1 < m_1$ and that $0 \leqslant r_2 < m_2$.

In this article, we generalize this construction to groups acting on $\mathbb{Z}^d$ ($d \in \mathbb{N}$):

Definition 1.2. Let $d \in \mathbb{N}$, and let $L_1, L_2 \in \mathbb{Z}^{d\times d}$ be matrices of full rank which are in Hermite normal form. Further let $r_1+\mathbb{Z}^dL_1$ and $r_2+\mathbb{Z}^dL_2$ be disjoint residue classes, and assume that the representatives r_1 and r_2 are reduced modulo $\mathbb{Z}^dL_1$ and $\mathbb{Z}^dL_2$, respectively. Then we define the *class transposition* $\tau_{r_1+\mathbb{Z}^dL_1,r_2+\mathbb{Z}^dL_2} \in \mathrm{Sym}(\mathbb{Z}^d)$ as the involution which interchanges $r_1 + kL_1$ and $r_2 + kL_2$ for all $k \in \mathbb{Z}^d$.

Definition 1.3. We denote the group which is generated by the set of all class transpositions of $\mathbb{Z}^d$ by $\mathrm{CT}(\mathbb{Z}^d)$.

Obviously, the group $\mathrm{CT}(\mathbb{Z}^{d_1})$ embeds into $\mathrm{CT}(\mathbb{Z}^{d_2})$ if $d_1 \leqslant d_2$. Therefore the class of subgroups of $\mathrm{CT}(\mathbb{Z}^d)$ is in particular at least not smaller than the class of subgroups of $\mathrm{CT}(\mathbb{Z})$, which is exhibited to a certain extent in [1].

The purpose of this article is to prove the following:

Theorem 1.4. *Let $d \in \mathbb{N}$. Then the group $\mathrm{CT}(\mathbb{Z}^d)$ is simple.*

In [1], the author has shown that this holds in case $d = 1$. The purpose of this article is to treat the case $d > 1$.

Originally, the work which led to the discovery of the simple group $\mathrm{CT}(\mathbb{Z})$ has been motivated by the famous $3n+1$ conjecture. This conjecture asserts that iterated application of the so-called Collatz mapping

$$T : \ \mathbb{Z} \longrightarrow \mathbb{Z}, \quad n \longmapsto \begin{cases} n/2 & \text{if } n \text{ is even,} \\ (3n+1)/2 & \text{if } n \text{ is odd} \end{cases}$$

2000 *Mathematics Subject Classification.* Primary 20E32, secondary 20B40, 20B22, 20-04.

to a positive integer yields 1 after a finite number of steps. This conjecture has been made by Lothar Collatz in the 1930s, and is still open today. Lagarias [3] has compiled a comprehensive annotated bibliography on this conjecture, which currently lists more than 200 references. A survey article and a monograph on Collatz' conjecture are [2] and [4], respectively.

The elements of the group $\mathrm{CT}(\mathbb{Z})$ are bijective mappings which are 'similar to T' in the sense that they are affine on residue classes as well. If one investigates the group $\mathrm{CT}(\mathbb{Z})$ by means of theory or by means of computation, it turns out that its subgroups and its elements can often be handled much easier than T. So it seems that part of the problem is that Collatz' mapping T is not injective.

However, a key observation is now that the mapping T can be extended in natural ways to permutations of $\mathbb{Z}^2$. An example of such an extension is

$$\sigma_T \in \mathrm{Sym}(\mathbb{Z}^2): \quad (m,n) \longmapsto \begin{cases} (2m+1,(3n+1)/2) & \text{if } n \text{ is odd,} \\ (2m, n/2) & \text{if } n \equiv 4 \bmod 6, \\ (m, n/2) & \text{otherwise.} \end{cases}$$

This motivates a move from $\mathbb{Z}$ to $\mathbb{Z}^2$, and generalizing further, to $\mathbb{Z}^d$ for $d \in \mathbb{N}$.

2. Basic Terms

In this section we introduce some basic terms which will be needed to prove the simplicity of $\mathrm{CT}(\mathbb{Z}^d)$.

Definition 2.1. Let $d \in \mathbb{N}$. We call a mapping $f : \mathbb{Z}^d \to \mathbb{Z}^d$ *residue-class-wise affine* if there is a lattice $L = \mathbb{Z}^d M$ where $M \in \mathbb{Z}^{d\times d}$ is a matrix of full rank, such that the restrictions of f to the residue classes $r + L \in \mathbb{Z}^d/L$ are all affine. This means that for any residue class $r + L \in \mathbb{Z}^d/L$, there is a matrix $A_{r+L} \in \mathbb{Z}^{d\times d}$, a vector $b_{r+L} \in \mathbb{Z}^d$ and a positive integer c_{r+L} such that the restriction of f to $r + L$ is given by

$$f|_{r+L} : r + L \longrightarrow \mathbb{Z}^d, \quad v \longmapsto \frac{v \cdot A_{r+L} + b_{r+L}}{c_{r+L}}.$$

For reasons of uniqueness, we assume that L is chosen maximal with respect to inclusion, and that no prime factor of c_{r+L} divides all coefficients of A_{r+L} and b_{r+L}.

We call the lattice L the *modulus* of f, written $\mathrm{Mod}(f)$.

We define the *prime set* of f as the set of all primes which divide the determinant of at least one of the coefficients A_{r+L} or which divide the determinant of M.

We call the mapping f *class-wise translating* if all coefficients A_{r+L} are identity matrices and all coefficients c_{r+L} are equal to 1.

For the sake of simplicity, we identify a lattice with the Hermite normal form of the matrix by whose rows it is spanned.

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

Definition 2.2. We denote the group which is formed by all residue-class-wise affine permutations of $\mathbb{Z}^d$ by $\mathrm{RCWA}(\mathbb{Z}^d)$, and call its subgroups *residue-class-wise affine* groups.

A more or less immediate observation is the following:

Theorem 2.3. *The groups* $\mathrm{CT}(\mathbb{Z}^d)$ *and* $\mathrm{RCWA}(\mathbb{Z}^d)$ *are not finitely generated.*

Proof. It is easy to see that the prime set of a product of residue-class-wise affine permutations is a subset of the union of the prime sets of the factors, and that inversion leaves the prime set invariant. Therefore as there are infinitely many primes and as for any prime p there is a class transposition $\tau_{(1,0,\ldots,0)+\mathbb{Z}^d\cdot\mathrm{diag}(2,1,\ldots,1),(0,0,\ldots,0)+\mathbb{Z}^d\cdot\mathrm{diag}(2p,1,\ldots,1)}$ whose prime set is $\{p\}$, the assertion follows. □

3. The Simplicity of $\mathrm{CT}(\mathbb{Z}^d)$

The aim of this section is to show that the groups $\mathrm{CT}(\mathbb{Z}^d)$ are simple. For this we need some lemmata:

Lemma 3.1. *Given any two class transpositions $\tau_{r_1+L_1,r_2+L_2}$ and $\tau_{r_3+L_3,r_4+L_4}$ whose support is not all of $\mathbb{Z}^d$, there is always a product π of 6 class transpositions such that $\tau_{r_1+L_1,r_2+L_2}^{\pi} = \tau_{r_3+L_3,r_4+L_4}$.*

Proof. Let $r_5 + L_5, r_6 + L_6 \subset \mathbb{Z}^d \setminus (r_1 + L_1 \cup r_2 + L_2)$ be disjoint residue classes such that $\cup_{i=3}^6 r_i + L_i \neq \mathbb{Z}^d$, and let $r_7 + L_7, r_8 + L_8 \subset \mathbb{Z}^d \setminus \cup_{i=3}^6 r_i + L_i$ be disjoint residue classes. Then the following hold:

(1) ${\tau_{r_1+L_1,r_2+L_2}}^{\tau_{r_1+L_1,r_5+L_5}} \cdot \tau_{r_2+L_2,r_6+L_6} = \tau_{r_5+L_5,r_6+L_6}$.
(2) ${\tau_{r_5+L_5,r_6+L_6}}^{\tau_{r_5+L_5,r_7+L_7}} \cdot \tau_{r_6+L_6,r_8+L_8} = \tau_{r_7+L_7,r_8+L_8}$.
(3) ${\tau_{r_7+L_7,r_8+L_8}}^{\tau_{r_3+L_3,r_7+L_7}} \cdot \tau_{r_4+L_4,r_8+L_8} = \tau_{r_3+L_3,r_4+L_4}$.

The assertion follows. □

Lemma 3.2. *Let $\sigma, \upsilon \in \mathrm{RCWA}(\mathbb{Z}^d)$, and put $L := \mathrm{Mod}(\sigma)$. If the mapping υ is class-wise translating and fixes all residue classes (mod L) setwise, then the commutator $[\sigma, \upsilon]$ is class-wise translating as well.*

Proof. Since υ fixes all residue classes (mod L), an affine partial mapping α of $[\sigma, \upsilon]$ is given by $\alpha_{\upsilon^{-1}}^{\alpha_\sigma} \cdot \alpha_\upsilon$ for certain affine partial mappings α_σ, α_υ and $\alpha_{\upsilon^{-1}}$ of σ, υ and υ^{-1}, respectively. The assertion follows, since the translations form a normal subgroup of the affine group of $\mathbb{Q}^d$. □

Lemma 3.3. *Let G be a subgroup of $\mathrm{RCWA}(\mathbb{Z}^d)$ which contains $\mathrm{CT}(\mathbb{Z}^d)$. Then any nontrivial normal subgroup $N \trianglelefteq G$ has a class-wise translating element $\iota \neq 1$.*

Proof. Let $\sigma \in N \setminus \{1\}$, and put $L := \mathrm{Mod}(\sigma)$. Without loss of generality, we can assume that σ is not class-wise translating. We pick a residue class $r + L$ such that $\sigma|_{r+L}$ is not a translation. By Lemma 3.2, the mappings $\iota_{i,j,k} := [\sigma, \tau_{r+iL_j+2kL, r+(i+k)L_j+2kL}] \in N$ $(k \in \mathbb{N},\ i \in \{0, \ldots, k-1\},\ j \in \{1, \ldots, d\})$ are class-wise translating. If we choose k sufficiently large, then σ does not map all residue classes $r + iL_j + kL$ to themselves. Therefore not all $\iota_{i,j,k}$ are equal to 1. □

Now we can prove our theorem:

Theorem 3.4. *The groups $\mathrm{CT}(\mathbb{Z}^d)$ are simple.*

Proof. Let $d \in \mathbb{N}$, and let N be a nontrivial normal subgroup of $\mathrm{CT}(\mathbb{Z}^d)$. We have to show that N contains all class transpositions.

By Lemma 3.1, all class transpositions whose support is not all of $\mathbb{Z}^d$ are conjugate in $\mathrm{CT}(\mathbb{Z}^d)$. Further, any class transposition can be written as a product of two class transpositions with disjoint supports: putting $D := \mathrm{diag}(1, \ldots, 1, 2)$, we have $\tau_{r_1+L_1,r_2+L_2} = \tau_{r_1+DL_1,r_2+DL_2} \cdot \tau_{r_1+L_{1,d}+DL_1,r_2+L_{2,d}+DL_2}$. Therefore it is already sufficient to show that N contains one class transposition whose support is a proper subset of $\mathbb{Z}^d$.

By Lemma 3.3, the normal subgroup N has a class-wise translating element $\iota_1 \neq 1$. Let L be a sublattice of the modulus of ι_1 such that $|\mathbb{Z}/L| \geqslant 3$, and choose a residue class $r+L$ which is moved by ι_1. Then put $\tilde{L} := DL$ and $\iota_2 := \tau_{r+\tilde{L},r+L_d+\tilde{L}} \cdot \tau_{(r+\tilde{L})^{\iota_1},(r+L_d+\tilde{L})^{\iota_1}} = [\tau_{r+\tilde{L},r+L_d+\tilde{L}}, \iota_1] \in N$.

By the choice of L, we can now choose two distinct residue classes $r_1 + \tilde{L}$ and $r_2 + \tilde{L}$ in the complement of the support of ι_2. Putting $\hat{L} := D^2 L$, we have now

$$\begin{aligned}\tau_{r_1+\tilde{L},r_2+\tilde{L}} \;=\; & \iota_2^{\tau_{r+\tilde{L},r_1+\hat{L}} \cdot \tau_{r+L_d+\tilde{L},r_2+\hat{L}}} \\ & \cdot \iota_2^{\tau_{r+\tilde{L},r_1+2L_d+\hat{L}} \cdot \tau_{r+L_d+\tilde{L},r_2+2L_d+\hat{L}}} \;\in\; N,\end{aligned}$$

which completes the proof of the theorem. □

Definition 3.5. Given a set $\mathbb{P}$ of odd primes, let $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z}^d) \leqslant \mathrm{CT}(\mathbb{Z}^d)$ denote the subgroup which is generated by all class transpositions whose prime sets are subsets of $\mathbb{P} \cup \{2\}$.

Corollary 3.6. *The groups $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z}^d)$ are simple. Therefore the group $\mathrm{CT}(\mathbb{Z}^d)$ has an uncountable series of simple subgroups, which is parametrized by the sets of odd primes.*

Proof. All of our arguments in this section apply to the groups $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z}^d)$ as well: In the proof of Lemma 3.1, we can choose the four residue classes $r_5 + L_5, \ldots, r_8 + L_8$ in such a way that all prime factors of the determinants of their moduli already divide the determinant of one of $L_1, \ldots, L_4$. The proofs of Lemma 3.2, Lemma 3.3 and Theorem 3.4 likewise do not require the presence of class transpositions whose moduli have determinants with certain odd factors. □

4. The Permutation σ_T

In this section, we will have a closer look at the permutation

$$\sigma_T \in \mathrm{RCWA}(\mathbb{Z}^2): \quad (m,n) \longmapsto \begin{cases} (2m+1, (3n+1)/2) & \text{if } n \text{ is odd,} \\ (2m, n/2) & \text{if } n \equiv 4 \bmod 6, \\ (m, n/2) & \text{otherwise} \end{cases}$$

introduced above.

The $3n+1$ conjecture asserts that any cycle of this permutation which contains a point (m,n) with $n > 0$ intersects nontrivially with the line $n = 1$, or equivalently that the first coordinates of the points of any cycle take only finitely many distinct even values.

First we observe that any cycle of the permutation σ_T lies entirely in one of the quadrants $Q_1 := \{(m,n) \in \mathbb{Z}^2 : m,n \geqslant 0\}$, $Q_2 := \{(m,n) \in \mathbb{Z}^2 : m \geqslant 0, n < 0\}$, $Q_3 := \{(m,n) \in \mathbb{Z}^2 : m,n < 0\}$ or $Q_4 := \{(m,n) \in \mathbb{Z}^2 : m < 0, n \geqslant 0\}$. Obviously we can restrict our attention to cycles lying in Q_1.

The permutation σ_T can be factored into 2 permutations whose cycle structure can be described easily: We have $\sigma_T = \alpha\beta$, where

$$\alpha \in \mathrm{RCWA}(\mathbb{Z}^2): \; (m,n) \mapsto \begin{cases} (2m, n/2) & \text{if } n \text{ is even,} \\ (2m+1, (n-1)/2) & \text{if } n \text{ is odd,} \end{cases}$$

and

$$\beta \in \mathrm{RCWA}(\mathbb{Z}^2): \; (m,n) \mapsto \begin{cases} (m/2, n) & \text{if } m \text{ is even and } n \not\equiv 2 \bmod 3, \\ (m, n) & \text{if } m \text{ is even and } n \equiv 2 \bmod 3, \\ (m, 3n+2) & \text{if } m \text{ is odd.} \end{cases}$$

Both α and β have infinite order. The cycles of α have roughly hyperbolic shape and run, so to speak, from $(0, \pm\infty)$ to $(\pm\infty, 0)$. A given cycle contains only finitely many points both of whose coordinates are nonzero. The fixed points of α are (0,0) and (-1,-1).

REFERENCES

1. Stefan Kohl, *A simple group generated by involutions interchanging residue classes of the integers*, 2007, preprint, available at http://www.cip.mathematik.uni-stuttgart.de/~kohlsn/preprints/simplegp.pdf.
2. Jeffrey C. Lagarias, *The 3x+1 problem and its generalizations*, Amer. Math. Monthly **92** (1985), 3–23. MR 777565 (86i:11043)
3. ———, *The 3x+1 problem: An annotated bibliography*, 2007, http://arxiv.org/abs/math.NT/0309224 (part I), http://arxiv.org/abs/math.NT/0608208 (part II).
4. Günther J. Wirsching, *The dynamical system generated by the 3n+1 function*, Lecture Notes in Mathematics, no. 1681, Springer-Verlag, 1998.

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

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