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 generated by involutions interchanging disjoint residue classes modulo lattices in $\mathbb{Z}^d$ ($d \in \mathbb{N}$).

1. INTRODUCTION

In this paper we generalize the construction of the simple group $\mathrm{CT}(\mathbb{Z}) < \mathrm{Sym}(\mathbb{Z})$ investigated in [1] to groups $\mathrm{CT}(\mathbb{Z}^d)$ acting on $\mathbb{Z}^d$ ($d \in \mathbb{N}$).

Definition 1.1. 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 $k \in \mathbb{Z}^d$ and which fixes everything else.

Definition 1.2. Let $\mathrm{CT}(\mathbb{Z}^d)$ denote the group which is generated by the set of all class transpositions of $\mathbb{Z}^d$.

The purpose of this article is to prove the following generalization of Theorem 3.4 in [1]:

Theorem 1.3. *The groups* $\mathrm{CT}(\mathbb{Z}^d)$ *are simple.*

2. BASIC TERMS

In order to prove the simplicity of $\mathrm{CT}(\mathbb{Z}^d)$, we need to introduce some terms:

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 $L = \mathbb{Z}^dM$ 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 $\mathrm{Mod}(f)$. Further 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, and 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.

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

For the sake of simplicity, we identify a lattice L with the Hermite normal form of the matrix by whose rows it is spanned, and denote the i-th row of the spanning matrix by $L_{(i)}$.

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 $\mathrm{CT}(\mathbb{Z}^d)$

In order to show that the groups $\mathrm{CT}(\mathbb{Z}^d)$ are simple, 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

$$\tau_{r_1+\tilde{L}, r_2+\tilde{L}} = \iota_2^{\tau_{r+\tilde{L}, r_1+\hat{L}} \cdot \tau_{r+L_{(d)}+\tilde{L}, r_2+\hat{L}}} \cdot \iota_2^{\tau_{r+\tilde{L}, r_1+2L_{(d)}+\hat{L}} \cdot \tau_{r+L_{(d)}+\tilde{L}, r_2+2L_{(d)}+\hat{L}}} \in N,$$

which completes the proof of the theorem. □

There is a straightforward generalization of Definition 3.6 and Corollary 3.7 in [1]:

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.*

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. Open Questions

Question 4.1. *How can it be decided whether a given element* $\sigma \in \mathrm{RCWA}(\mathbb{Z}^d)$ *lies in the group* $\mathrm{CT}(\mathbb{Z}^d)$*?*

Question 4.2. *Obviously the group* $\mathrm{CT}(\mathbb{Z}^{d_1})$ *embeds into* $\mathrm{CT}(\mathbb{Z}^{d_2})$ *if* $d_1 \leqslant d_2$*. But are there positive integers* $d_1 < d_2$ *such that* $\mathrm{CT}(\mathbb{Z}^{d_2})$ *embeds into* $\mathrm{CT}(\mathbb{Z}^{d_1})$*?*

Question 4.3. *Are there distinct sets* $\mathbb{P}_1$ *and* $\mathbb{P}_2$ *of odd primes and positive integers* d_1 *and* d_2 *such that the groups* $\mathrm{CT}_{\mathbb{P}_1}(\mathbb{Z}^{d_1})$ *and* $\mathrm{CT}_{\mathbb{P}_2}(\mathbb{Z}^{d_2})$ *are isomorphic?*

References

1. Stefan Kohl, *A simple group generated by involutions interchanging residue classes of the integers*, Math. Z. **264** (2010), no. 4, 927–938, DOI: 10.1007/s00209-009-0497-8.

Departamenti i Matematikës, Universiteti "Ismail Qemali" Vlorë, Lagja: Pavarësia, Vlorë / Albania

E-mail address: stefan@mcs.st-and.ac.uk