AN INFINITE SIMPLE GROUP GENERATED BY 4 INVOLUTIONS

STEFAN KOHL

ABSTRACT. We present an infinite simple group which is generated by 4 involutions.

1. INTRODUCTION

Let $G := \langle g, h_1, h_2, h_3 \rangle < \mathrm{Sym}(\mathbb{Z})$, where

$$g: \ n \mapsto \begin{cases} 2n+1 & \text{if } n \in 0(2), \\ (n-1)/2 & \text{if } n \in 1(4), \\ n & \text{if } n \in 3(4), \end{cases} \qquad h_1: \ n \mapsto \begin{cases} n+1 & \text{if } n \in 0(4), \\ n-1 & \text{if } n \in 1(4), \\ n & \text{otherwise,} \end{cases}$$

$$h_2: \ n \mapsto \begin{cases} n+1 & \text{if } n \in 1(4), \\ n-1 & \text{if } n \in 2(4), \\ n & \text{otherwise,} \end{cases} \qquad h_3: \ n \mapsto \begin{cases} n+1 & \text{if } n \in 2(4), \\ n-1 & \text{if } n \in 3(4), \\ n & \text{otherwise.} \end{cases}$$

In this note, we show that G is an infinite simple group.

We need a more convenient way to write down elements of our group G:

Definition 1.1. Given disjoint residue classes $r_1(m_1)$ and $r_2(m_2)$ of $\mathbb{Z}$, we define the *class transposition* $(r_1(m_1), r_2(m_2)) \in \mathrm{Sym}(\mathbb{Z})$ 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 notation, we have $G = \langle (0(2), 1(4)), (0(4), 1(4)), (1(4), 2(4)), (2(4), 3(4)) \rangle$.

2. THE SIMPLICITY OF THE GROUP G

In order to prove the simplicity of G, we need the following lemma:

Lemma 2.1. The group G contains all class transpositions which interchange residue classes modulo powers of 2.

Proof. We observe that $h_1 = (0(4), 1(4))$, $h_2 = (1(4), 2(4))$ and $h_3 = (2(4), 3(4))$ generate a symmetric group of degree 4, which acts naturally on the residue classes (mod 4). We denote this group by H. It is $(0(2), 1(2)) = h_1 \cdot h_3 \in H$. We put

$$\begin{aligned} g_1 &:= (0(2), 1(4)) = g \in G, \\ g_2 &:= (0(2), 3(4)) = g^{h_2 \cdot h_3 \cdot h_2} \in G, \\ g_3 &:= (1(2), 0(4)) = g^{h_1 \cdot h_3} \in G, \text{ and} \\ g_4 &:= (1(2), 2(4)) = g^{h_3 \cdot h_2 \cdot h_1} \in G, \end{aligned}$$

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

and conclude that G contains the set

$$\mathcal{C}_4 = \{(0(2),1(2)),(0(2),1(4)),(0(2),3(4)),(1(2),0(4)),(1(2),2(4)),$$
$$(0(4),1(4)),(0(4),2(4)),(0(4),3(4)),(1(4),2(4)),(1(4),3(4)),(2(4),3(4))\}$$

of all 11 class transpositions which interchange residue classes modulo 2 or 4.

Let $\tau := (r_1(2^{k_1}), r_2(2^{k_2}))$ be a class transposition. We need to show that $\tau \in G$. Without loss of generality, we assume that $\tau \notin \mathcal{C}_4$. We describe an algorithm to turn τ into an element of $\mathcal{C}_4$ by successive conjugation by elements of the set $\{g_1, g_2, g_3, g_4, h_1, h_2\}$. Throughout the algorithm, we write $\tau = (r_1(2^{k_1}), r_2(2^{k_2}))$, where $k_1 \leqslant k_2$:

(1) If $k_1 = 1$, then proceed as follows:
  (a) If $r_1 = 0$ and $r_2(2^{k_2}) \subset 1(4)$, then put $\tau := \tau^{g_2}$.
  (b) If $r_1 = 0$ and $r_2(2^{k_2}) \subset 3(4)$, then put $\tau := \tau^{g_1}$.
  (c) If $r_1 = 1$ and $r_2(2^{k_2}) \subset 0(4)$, then put $\tau := \tau^{g_4}$.
  (d) If $r_1 = 1$ and $r_2(2^{k_2}) \subset 2(4)$, then put $\tau := \tau^{g_3}$.

  Now the moduli of both residue classes interchanged by τ are least 4.

(2) While $\tau \notin \mathcal{C}_4$, repeat the following:
  (a) If one of the residue classes $r_1(2^{k_1})$ and $r_2(2^{k_2})$ is a subset of 0(2) and the other is a subset of 1(2), then proceed as follows:
    (i) Let $h \in \{h_1, h_2\}$ be the class transposition whose support is a superset of exactly one of the residue classes $r_1(2^{k_1})$ and $r_2(2^{k_2})$.
    (ii) Put $\tau := \tau^h$.

    Now the support of τ is a subset of either 0(2) or 1(2).
  (b) We are now in the position that we can halve the modulus of at least one of the residue classes which are interchanged by τ (remember our choice $k_2 \geqslant k_1$):
    (i) If $r_2(2^{k_2}) \subset 1(4)$, then put $\tau := \tau^{g_1}$.
    (ii) If $r_2(2^{k_2}) \subset 3(4)$, then put $\tau := \tau^{g_2}$.
    (iii) If $r_2(2^{k_2}) \subset 0(4)$, then put $\tau := \tau^{g_3}$.
    (iv) If $r_2(2^{k_2}) \subset 2(4)$, then put $\tau := \tau^{g_4}$.

Since each iteration of the loop in Step (2) halves the modulus of at least one of the residue classes which are interchanged by τ, this algorithm terminates. Therefore our original τ is an element of G, as claimed. $\square$

Now the announced result follows from Lemma 2.1 and Corollary 3.7 in [1]:

Theorem 2.2. The group G is simple.

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.

INSTITUT FÜR GEOMETRIE UND TOPOLOGIE, PFAFFENWALDRING 57, UNIVERSITÄT STUTTGART
70550 STUTTGART, GERMANY
E-mail address: kohl@mathematik.uni-stuttgart.de