Groups Generated by Class Transpositions – Results and Open Problems

Stefan Kohl

Talk. UV Algebra Winter Conference 2009

Class Transpositions

By $r(m)$ we denote the residue class $r + m\mathbb{Z}$.

Let $r_1(m_1)$ and $r_2(m_2)$ be disjoint residue classes of $\mathbb{Z}$. Recall that this means that $\gcd(m_1, m_2) \nmid (r_1 - r_2)$.

We always assume that $0 \leqslant r_1 < m_1$ and that $0 \leqslant r_2 < m_2$.

Let the *class transposition* $\tau_{r_1(m_1),r_2(m_2)}$ be the permutation which interchanges $r_1 + tm_1$ and $r_2 + tm_2$ for every $t \in \mathbb{Z}$, and which fixes everything else.

For convenience, we set

$$\tau := \tau_{0(2),1(2)} : \ n \mapsto n + (-1)^n.$$

Products of Two Class Transpositions

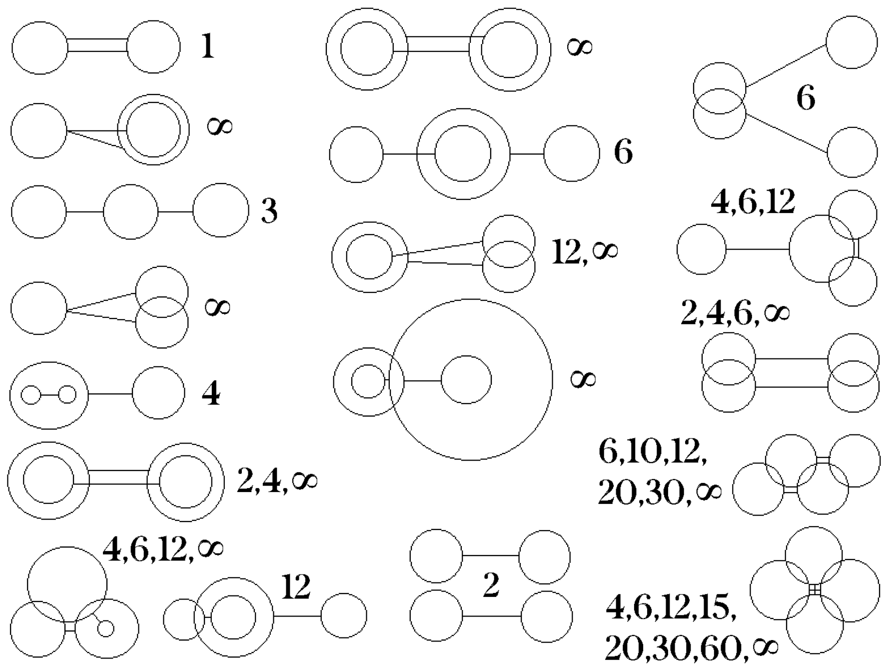
Some examples:

σ	$\mathrm{ord}(\sigma)$
$\tau_{0(4),2(4)} \cdot \tau_{1(4),3(4)}$	2
$\tau_{0(3),1(3)} \cdot \tau_{0(3),2(3)}$	3
$\tau_{0(2),1(2)} \cdot \tau_{0(4),2(4)}$	4
$\tau_{1(2),0(4)} \cdot \tau_{1(4),2(4)}$	6
$\tau_{0(2),1(4)} \cdot \tau_{2(3),1(6)}$	10
$\tau_{1(2),0(4)} \cdot \tau_{1(3),2(6)}$	12
$\tau_{0(2),1(4)} \cdot \tau_{0(3),2(3)}$	15
$\tau_{0(3),1(6)} \cdot \tau_{1(4),3(4)}$	20
$\tau_{0(2),1(4)} \cdot \tau_{0(5),2(5)}$	30
$\tau_{1(3),0(6)} \cdot \tau_{1(5),2(5)}$	60
$\tau_{0(4),1(6)} \cdot \tau_{1(4),2(6)}$	∞, finite cycles
$\tau_{0(2),1(4)} \cdot \tau_{1(2),2(4)}$	∞, infinite cycles

Order and cycle structure of the product of two class transpositions depend crucially on how the 4 involved residue classes intersect each other.

Intersection Types

It happens that there are 18 different such "intersection types". On the picture below, residue classes are denoted by circles, and class transpositions are denoted by lines connecting two circles.



Already for class transpositions which interchange residue classes with moduli $\leqslant 6$, there are 88 different subcases where the products have different cycle structure.

Groups Generated by 3 Class Transpositions

Open problem: What are the possible structures of groups generated by 3 class transpositions? – In particular, can 3 class transpositions generate an infinite simple group?

Four Class Transpositions can!

Put $G := \langle \kappa, \lambda, \mu, \nu \rangle$, where $\kappa = \tau_{0(2),1(2)}$, $\lambda = \tau_{1(2),2(4)}$, $\mu = \tau_{0(2),1(4)}$, $\nu = \tau_{1(4),2(4)}$.

John McDermott (Galway) has pointed out to me the following:

The group G is isomorphic to the Higman-Thompson group (cf. Higman 1974), the first finitely presented infinite simple group which has been discovered.

How to Prove this?

To check that the group G is isomorphic to the Higman-Thompson group, it suffices to verify that its generators satisfy the defining relations given by Higman:

- $\kappa^2 = \lambda^2 = \mu^2 = \nu^2 = 1$,
- $\lambda\kappa\mu\kappa\lambda\nu\kappa\nu\mu\kappa\lambda\kappa\mu = \kappa\nu\lambda\kappa\mu\nu\kappa\lambda\nu\mu\nu\lambda\nu\mu = 1$,
- $(\lambda\kappa\mu\kappa\lambda\nu)^3 = (\mu\kappa\lambda\kappa\mu\nu)^3 = 1$,
- $(\lambda\nu\mu)^2\kappa(\mu\nu\lambda)^2\kappa = 1$,
- $(\lambda\nu\mu\nu)^5 = 1$,
- $(\lambda\kappa\nu\kappa\lambda\nu)^3\kappa\nu\kappa(\mu\kappa\nu\kappa\mu\nu)^3\kappa\nu\kappa\nu = 1$,
- $((\lambda\kappa\mu\nu)^2(\mu\kappa\lambda\nu)^2)^3 = 1$,
- $(\lambda\nu\lambda\kappa\mu\kappa\mu\nu\lambda\nu\mu\kappa\mu\kappa)^4 = 1$,
- $(\mu\nu\mu\kappa\lambda\kappa\lambda\nu\mu\nu\lambda\kappa\lambda\kappa)^4 = 1$, and
- $(\lambda\mu\kappa\lambda\kappa\mu\lambda\kappa\nu\kappa)^2 = (\mu\lambda\kappa\mu\kappa\lambda\mu\kappa\nu\kappa)^2 = 1$.

The Group $\mathrm{CT}(\mathbb{Z})$

Let $\mathrm{CT}(\mathbb{Z})$ be the group which is generated by *all* class transpositions of $\mathbb{Z}$.

Some results:

The group $\mathrm{CT}(\mathbb{Z})$ is simple.

The group $\mathrm{CT}(\mathbb{Z})$ itself is countable, but it has an uncountable series of simple subgroups $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z})$, which is parametrized by the sets $\mathbb{P}$ of odd primes.

Further, the group $\mathrm{CT}(\mathbb{Z})$

- is not finitely generated,
- acts highly transitively on $\mathbb{N}_0$, and
- its torsion elements are divisible.

Open Problems on $\mathrm{CT}(\mathbb{Z})$

Open Problems on $\mathrm{CT}(\mathbb{Z})$:

- Does the group $\mathrm{CT}(\mathbb{Z})$ have nontrivial outer automorphisms?

  – Intuition suggests: "likely not", which would be a nice result. Otherwise it would be interesting to know how outer automorphisms look like.

- Call a permutation of $\mathbb{Z}$ *residue-class-wise affine* if there is an $m \in \mathbb{N}$ such that its restrictions to the residue classes (mod m) are all affine. – Is $\mathrm{CT}(\mathbb{Z})$ the group of *all* residue-class-wise affine permutations which fix $\mathbb{N}_0$ setwise?

  – Most likely yes. A way to prove this would be to turn the heuristic factorization method presently implemented in RCWA into a proper algorithm.

Some Groups Which Embed into CT($\mathbb{Z}$)

- Every finite group embeds into CT($\mathbb{Z}$).

- Every free group of finite rank embeds into CT($\mathbb{Z}$).

- Every free product of finitely many finite groups embeds into CT($\mathbb{Z}$).

- The class of subgroups of CT($\mathbb{Z}$) is closed under taking
  - direct products,
  - wreath products with finite groups, and
  - restricted wreath products with $(\mathbb{Z}, +)$.

Examples of Subgroups of $\mathrm{CT}(\mathbb{Z})$

We have for example

- $\mathrm{F}_2 \cong \langle (\tau \cdot \tau_{0(2),1(4)})^2, (\tau \cdot \tau_{0(2),3(4)})^2 \rangle$ (the free group of rank 2),

- $\mathrm{PSL}(2,\mathbb{Z}) \cong \langle \tau, \tau_{0(4),2(4)} \cdot \tau_{1(2),0(4)} \rangle$ (the modular group),

- $\mathrm{C}_2 \wr \mathbb{Z} \cong \langle \tau \cdot \tau_{0(2),1(4)}, \tau_{3(8),7(8)} \rangle$ (the lamplighter group), and

- $\mathbb{Z} \wr \mathbb{Z} \cong \langle \tau \cdot \tau_{0(2),1(4)}, \tau_{3(8),7(8)} \cdot \tau_{3(8),7(16)} \rangle$, and

- $G := \langle \tau_{0(4),3(4)}, \tau_{0(6),3(6)}, \tau_{1(4),0(6)} \rangle$ is an infinite group, which has only finite orbits on $\mathbb{Z}$.

More on Subgroups of $\mathrm{CT}(\mathbb{Z})$

The group $\mathrm{CT}(\mathbb{Z})$ has

- finitely generated subgroups which do not have finite presentations, and

- finitely generated subgroups with unsolvable membership problem.

Since words in the generators of subgroups of $\mathrm{CT}(\mathbb{Z})$ can always be evaluated and compared, groups with unsolvable word problem do *not* embed into $\mathrm{CT}(\mathbb{Z})$.

Open problem: Does the group $\mathrm{CT}(\mathbb{Z})$ have subgroups of intermediate growth?

– The “standard” examples of groups of intermediate growth like the Grigorchuk group likely do not embed; the question itself seems ‘wide open’.

The Series of Subgroups $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z})$

Let $\mathbb{P}$ be a set of odd primes.

The group $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z})$ is the subgroup of $\mathrm{CT}(\mathbb{Z})$ which is generated by all class transpositions $\tau_{r_1(m_1),r_2(m_2)}$ for which all odd prime factors of m_1 and m_2 lie in $\mathbb{P}$.

The groups $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z})$ are simple as well. They are finitely generated if and only if $|\mathbb{P}| < \infty$.

Open problem: Are the uncountably many groups $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z})$ pairwise nonisomorphic?
If not: Under which conditions on the sets $\mathbb{P}_1$ and $\mathbb{P}_2$ of odd primes is $\mathrm{CT}_{\mathbb{P}_1}(\mathbb{Z}) \cong \mathrm{CT}_{\mathbb{P}_2}(\mathbb{Z})$?

The group $\mathrm{CT}_{\emptyset}(\mathbb{Z})$ is the finitely presented simple group generated by 4 class transpositions mentioned earlier.

Open problem: Is $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z})$ always finitely presented if $\mathbb{P}$ is finite?

The Class Transposition Graph

Let Γ be the graph whose vertices are the class transpositions and in which two vertices are connected by an edge if their product has finite order.

Open questions:

- All graphs with at most 4 vertices embed into Γ. – Does every finite graph embed?

- Is Γ just a realization of the Universal Graph? *(Likely not.)*

Computational Aspects

So far, research in computational group theory focussed mainly on finite permutation groups, matrix groups, finitely presented groups, polycyclically presented groups and automatic groups.

The subgroups of $\mathrm{CT}(\mathbb{Z})$ form another large class of groups which are accessible to computational methods. Algorithms to compute with such groups are described in

Algorithms for a Class of Infinite Permutation Groups. *J. Symb. Comput.* 43(2008), no. 8, 545-581.

They are implemented in the package RCWA for the computer algebra system GAP.

Many of the results presented in this talk have first been discovered during extensive experiments with the RCWA package.

A Little Example

In 1932, Lothar Collatz investigated the permutation

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

of the integers. The cycle structure of α is unknown so far.

We want to determine whether $\alpha \in \mathrm{CT}(\mathbb{Z})$.

For this, we attempt to factor α into class transpositions. Due to the particular form of α, that is not particularly easy and we need a notable number of factors.

"Prime Switch" σ_p

The factorization method makes use of certain special products of class transpositions:

For an odd prime p, let

$$\sigma_p := \tau_{0(8),1(2p)} \cdot \tau_{4(8),2p-1(2p)} \cdot \tau_{0(4),1(2p)} \cdot \tau_{2(4),2p-1(2p)} \cdot \tau_{2(2p),1(4p)} \cdot \tau_{4(2p),2p+1(4p)} \in \mathrm{CT}(\mathbb{Z}).$$

We have

$$\sigma_p: \ n \mapsto \begin{cases} (pn+2p-2)/2 & \text{if} \ \ n \in 2(4), \\ n/2 & \text{if} \ \ n \in 0(4) \setminus (4(4p) \cup 8(4p)), \\ n+2p-7 & \text{if} \ \ n \in 8(4p), \\ n-2p+5 & \text{if} \ \ n \in 2p-1(2p), \\ n+1 & \text{if} \ \ n \in 1(2p), \\ n-3 & \text{if} \ \ n \in 4(4p), \\ n & \text{if} \ \ n \in 1(2) \setminus (1(2p) \cup 2p-1(2p)). \end{cases}$$

$$\alpha \in \mathrm{CT}(\mathbb{Z})$$

Now we have

$$\begin{aligned}
\alpha \;=\;& \tau_{2(3),3(6)} \cdot \tau_{1(3),0(6)} \cdot \tau_{0(3),1(3)} \cdot \tau \cdot \tau_{0(36),1(36)} \\
&\cdot \tau_{0(36),35(36)} \cdot \tau_{0(36),31(36)} \cdot \tau_{0(36),23(36)} \cdot \tau_{0(36),18(36)} \\
&\cdot \tau_{0(36),19(36)} \cdot \tau_{0(36),17(36)} \cdot \tau_{0(36),13(36)} \cdot \tau_{0(36),5(36)} \\
&\cdot \tau_{2(36),10(36)} \cdot \tau_{2(36),11(36)} \cdot \tau_{2(36),15(36)} \cdot \tau_{2(36),20(36)} \\
&\cdot \tau_{2(36),28(36)} \cdot \tau_{2(36),26(36)} \cdot \tau_{2(36),25(36)} \cdot \tau_{2(36),21(36)} \\
&\cdot \tau_{2(36),4(36)} \cdot \tau_{3(36),8(36)} \cdot \tau_{3(36),7(36)} \cdot \tau_{9(36),16(36)} \\
&\cdot \tau_{9(36),14(36)} \cdot \tau_{9(36),12(36)} \cdot \tau_{22(36),34(36)} \\
&\cdot \tau_{27(36),32(36)} \cdot \tau_{27(36),30(36)} \cdot \tau_{29(36),33(36)} \\
&\cdot \tau_{10(18),35(36)} \cdot \tau_{5(18),35(36)} \cdot \tau_{10(18),17(36)} \\
&\cdot \tau_{5(18),17(36)} \cdot \tau_{8(12),14(24)} \cdot \tau_{6(9),17(18)} \cdot \tau_{3(9),17(18)} \\
&\cdot \tau_{0(9),17(18)} \cdot \tau_{6(9),16(18)} \cdot \tau_{3(9),16(18)} \cdot \tau_{0(9),16(18)} \\
&\cdot \tau_{6(9),11(18)} \cdot \tau_{3(9),11(18)} \cdot \tau_{0(9),11(18)} \cdot \tau_{6(9),4(18)} \\
&\cdot \tau_{3(9),4(18)} \cdot \tau_{0(9),4(18)} \cdot \tau_{0(6),14(24)} \cdot \tau_{0(6),2(24)} \\
&\cdot \tau_{8(12),17(18)} \cdot \tau_{7(12),17(18)} \cdot \tau_{8(12),11(18)} \\
&\cdot \tau_{7(12),11(18)} \cdot \sigma_3^{-1} \cdot \tau_{7(12),17(18)} \cdot \tau_{2(6),17(18)} \\
&\cdot \tau_{0(3),17(18)} \cdot \sigma_3^{-3} \in \mathrm{CT}(\mathbb{Z}).
\end{aligned}$$

Simple Supergroups of CT($\mathbb{Z}$)

Let $r(m) \subseteq \mathbb{Z}$ be a residue class.

We define the *class shift* $\nu_{r(m)}$ by

$$\nu_{r(m)} \in \mathrm{Sym}(\mathbb{Z}) : \; n \mapsto \begin{cases} n+m & \text{if } n \in r(m), \\ n & \text{otherwise.} \end{cases}$$

We define the *class reflection* $\varsigma_{r(m)}$ by

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

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

The groups

$$K^+ := \langle \mathrm{CT}(\mathbb{Z}), \nu_{1(3)} \cdot \nu_{2(3)}^{-1} \rangle$$

and

$$K^- := \langle \mathrm{CT}(\mathbb{Z}), \nu_{1(3)} \cdot \nu_{2(3)}, \varsigma_{0(2)} \cdot \nu_{0(2)} \rangle$$

are simple as well.

The $3n + 1$ Conjecture

In the 1930s, Lothar Collatz made the following conjecture:

3n+1 Conjecture. Iterated application of the mapping

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

to any positive integer yields 1 after a finite number of steps.

This conjecture – nowadays famous – is still open today, although there are more than 200 related mathematical publications. - Cf. Jeffrey C. Lagarias' annotated bibliography (http://arxiv.org/abs/math.NT/0309224, http://arxiv.org/abs/math.NT/0608208).

A Bijective Extension of T to $\mathbb{Z}^2$

The mapping T is not injective.

Dealing with permutations and permutation groups is usually easier.

However, the mapping T can be extended in natural ways to permutations of $\mathbb{Z}^2$. –

For example:

$\sigma_T \in \mathrm{Sym}(\mathbb{Z}^2)$:

$$(m, n) \mapsto \begin{cases} (2m+1, (3n+1)/2) & \text{if } n \in 1(2), \\ (2m, n/2) & \text{if } n \in 4(6), \\ (m, n/2) & \text{otherwise.} \end{cases}$$

This turns the $3n+1$ conjecture into the question whether the line $n = 4$ is a set of representatives for the cycles of σ_T on the half-plane $n > 0$.

A Factorization of σ_T

Furthermore, the mapping σ_T can be written as the product of two permutations whose cycle structure can be described very easily:

We have $\sigma_T = \alpha\beta$, where

$$\alpha : (m,n) \mapsto \begin{cases} (2m, n/2) & \text{if } 2|n, \\ (2m+1, (n-1)/2) & \text{if } 2 \nmid n, \end{cases}$$

and

$$\beta : (m,n) \mapsto \begin{cases} (m/2, n) & \text{if } 2|m \ \wedge \ n \notin 2(3), \\ (m, n) & \text{if } 2|m \ \wedge \ n \in 2(3), \\ (m, 3n+2) & \text{if } 2 \nmid m. \end{cases}$$

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

The Groups $\mathsf{CT}(\mathbb{Z}^d)$

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 $r_1 + \mathbb{Z}^d L_1$ and $r_2 + \mathbb{Z}^d L_2$ be disjoint residue classes, and assume that r_1 and r_2 are reduced modulo $\mathbb{Z}^d L_1$ and $\mathbb{Z}^d L_2$, respectively.

Let the *class transposition*

$$\tau_{r_1+\mathbb{Z}^d L_1, r_2+\mathbb{Z}^d L_2} \in \mathsf{Sym}(\mathbb{Z}^d)$$

be the involution which interchanges $r_1 + kL_1$ and $r_2 + kL_2$ for every $k \in \mathbb{Z}^d$, and which fixes everything else.

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

The groups $\mathsf{CT}(\mathbb{Z}^d)$, $d \in \mathbb{N}$ are simple as well.

The development version of RCWA contains already basic methods to compute in $\mathsf{CT}(\mathbb{Z}^2)$.

Recent Paper

Many of the results presented in this talk can be found in my article

A Simple Group Generated by Involutions Interchanging Residue Classes of the Integers. *Mathematische Zeitschrift*, DOI: 10.1007/s00209-009-0497-8.

My GAP package RCWA is available at

http://www.gap-system.org/Packages/rcwa.html