The Goal: The purpose of these notes is to explain the outer automorphism of the symmetric group S_6 and its connection to the Steiner $(5,6,12)$ design and the Mathieu group M_{12}. In view of giving short proofs, we often appeal to a mixture of logic and direct computer-assisted enumerations.

Preliminaries: It is an exercise to show that the symmetric group S_n admits an outer automorphism if and only if $n=6$. The basic idea is that any automorphism of S_n must map the set of transpositions bijectively to the set of conjugacy classes of a single permutation. A counting argument shows that the only possibility, for $n \neq 6$, is that the automorphism maps the set of transpositions to the set of transpositions. From here it is not to hard to see that the automorphism must be an inner automorphism – i.e., conjugation by some element of S_n. For $n=6$ there are 15 transpositions and also 15 *triple transpositions*, permutations of the form $(ab)(cd)(ef)$ with all letters distinct. This leaves open the *possibility* of an outer automorphism.

The Steiner Design: Let $P_1(\boldsymbol{Z}/11)$ denote the projective line over $\boldsymbol{Z}/11$. The group $\Gamma = SL_2(\boldsymbol{Z}/11)$ consists of those transformations

$$x \to (ax+b)/(cx+d)$$

with $ad-bc \equiv 1 \bmod 11$. There are $660 = (12 \times 11 \times 10)/2$ elements in this group. Let

$$B_\infty = \{1,3,4,5,9,\infty\} \subset P_1(\boldsymbol{Z}/11)$$

be the 6-element subset consisting of the squares mod 11 and the element ∞. Let $\Gamma_\infty \subset \Gamma$ be the stabilizer of B_∞. Let $\mathcal{B}$ be the orbit of B_∞ under the action of Γ.

Lemma 0.1 *Γ_∞ has order 5 and stabilizes ∞. At the same time $\mathcal{B}$ has 132 members.*

Proof: Let N be the order of Γ_∞ and let M be the size of $\mathcal{B}$. We have $MN = 660$. The element

$$\beta(x) = \frac{5x+0}{0x+9} = 3x$$

belongs to Γ_∞ and generates an order 5 subgroup. A direct enumeration shows that this is all of Γ_∞. Hence $N=5$ and $M=132$. ♠

The 132 elements of $\mathcal{B}$ are called *blocks*. Together they comprise the Steiner $(5, 6, 12)$ design.

Lemma 0.2 *Every 5 element subset of $P_1(\boldsymbol{Z}/11)$ is contained in a unique block.*

Proof: A direct enumeration shows that no distinct block has 5 members in common with B_∞. By symmetry, no two blocks have 5 elements in common. Hence, each 5-element subsets lies in at most one block. There are 792 5-element subsets. At the same time, the number of 5-element subsets contained in blocks is $6 \times 132 = 792$. This accounts for all of them. ♠

Lemma 0.3 *The complement of a block in $P_1(\boldsymbol{Z}/11)$ is also a block.*

Proof: Let $I(x) = -1/x$. This element belongs to Γ. We compute that $I(B_\infty)$ is the subset $B_0 = \{0, 2, 6, 7, 8, 10\}$. This is the complement of B_∞ and hence also a block. The general case now follows from symmetry. ♠

The Mathieu Group By construction, the elements of Γ are automorphisms of $\mathcal{B}$. Amazingly, $\mathcal{B}$ has additional automorphisms.

Lemma 0.4 *The permutation*

$$\pi = (1, \infty)(0, 7)(2, 8)(6, 10)$$

preserves $\mathcal{B}$.

Proof: This is a direct computer-assisted enumeration. ♠

Note that π preserves both B_0 and B_∞ and acts as a transposition on B_∞ and as a triple cycle on B_0.

Let M_{12} denote the group generated by Γ and π. This group is known as a *Mathieu group*. We can work out the exact order of M_{12}. Given that π acts on B_∞ as a transposition swapping 1 and ∞, and Γ_∞ is generated by a 5-cycle which fixes ∞, we see that the stabilizer of B_∞ in M_{12} is S_6. This is much bigger than Γ_∞. The orbit of B_∞ under M_{12} is $\mathcal{B}$. Therefore M_{12} has order

$$6! \times 132 = 95040 = 12 \times 11 \times 10 \times 9 \times 8.$$

This is $720/5 = 144$ times as large as the order of Γ.

Lemma 0.5 *Given any two ordered* 5*-tuples, there is a unique element of* M_{12} *mapping the one to the other. That is,* M_{12} *acts sharply transitively on the set of ordered* 5*-tuples in* $P_1(\boldsymbol{Z}/11)$.

Proof: Suppose that X and Y are two 5-element subsets of $P_1(\boldsymbol{Z}/11)$. There are unique blocks B_X and B_Y which contains X and Y respectively. There is an element $\gamma \in M_{12}$ such that $\gamma(B_X) = B_Y$. Since the stabilizer of each block in $\mathcal{B}$ is S_6, we can choose γ so that $\gamma(X) = Y$. In other words, M_{12} acts transitively on the 5-element subsets of $P_1(\boldsymbol{Z}/11)$. But there are precisely 95040 such subsets. Therefore, M_{12} acts sharply transitively on these subsets. ♠

Lemma 0.6 *Every element of* M_{12} *is the product of at least* 4 *transpositions.*

Proof: Consider an element of M_{12} which, hypothetically, is the product of at most 3 transpositions. Such an element would only move at most 6 members of $P_1(\boldsymbol{Z}/11)$ and hence would fix some ordered 5-tuple. This contradicts sharp transitivity. ♠

The Outer Automophism: Let S_6 be the stabilizer of B_∞ in M_{12}. Note that S_6 is simultaneously the stabilizer of B_0. Therefore, conjugation by I is an automorphism of S_6. By construction π acts as a transposition on B_∞ but $I\pi I^{-1}$ acts as a triple transposition on B_∞. Hence, conjugation by I is an outer automorphism of S_6. The previous lemma shows that this calculation is not just a crazy accident.

A Cell Complex: Let me elaborate a bit on Lemma 0.2. Two Steiner blocks can intersect in 4 elements. One can make a cell complex K in which the vertices are Steiner blocks and the k-simplices are $(k+1)$-tuples of blocks which mutually intersect in sets of size 4. The group M_{12} automatically acts on this complex K. I computed that K respectively has

$$66 \times (2, 45, 300, 675, 432, 12)$$

k-simplices for $k = 0, 1, 2, 3, 4, 5$, and no 6-simplices. This space has Euler characteristic 132. Each 5-simplex is such that the blocks corresponding to the vertices have 5 elements in common with a unique 6-element subset which is not a block. (Call these *unblocks*.) Therefore, there is a canonical bijection between the set of 5-simplices and the set of unblocks.