Week 8 Lecture 2

Groups of transformations, with a detailed activity on the transformations of the integer line.

1. Reminder: transformations form a group

Last time, we studied transformations of finite incidence geometries. We used several ideas repeatedly. For example, if a line has two points, then its image under a transformation is again a line with two points. Also, if two lines meet at a point, then their images are two lines meeting at the image of that point.

Today, we study an infinite example.

First, recall that a **group** is a set G together with an operation which takes two elements of G and gives back another element of G. The operation must satisfy the following properties:

(a) **Closure:** if $g, h \in G$, then $g * h \in G$.

(b) **Neutral element:** there is an element $e \in G$ such that $g * e = e * g = g$ for every $g \in G$.

(c) **Inverse:** for every $g \in G$, there is an element $h \in G$ such that $g * h = h * g = e$.

(d) **Associativity:** parentheses do not matter.

In our case, if $\mathcal{M}$ is a model satisfying axioms **I1** and **I2**, then $\mathrm{Aut}(\mathcal{M})$, with composition, is a group.

In practice, this means:

- if f and g are transformations, then $f \circ g$ is a transformation;
- the identity map is a transformation;
- if f is a transformation, then f^{-1} is also a transformation;
- when composing transformations, parentheses do not matter.

Author(s):

2. Other examples of groups

Example 1. The set $\mathbb{Z}$, with addition, is a group. The neutral element is 0, because $k + 0 = 0 + k = k$. The inverse of k is $-k$, because $k + (-k) = 0$. Addition is associative.

Example 2. The set $\mathbb{R}$, with addition, is also a group.

Example 3. The set $\mathbb{R} \setminus \{0\}$, with multiplication, is a group. The neutral element is 1, and the inverse of $x \neq 0$ is $1/x$.

Example 4. The set $\{1, -1\}$, with multiplication, is a group. The neutral element is 1, and each element is its own inverse.

Example 5. The set $\mathrm{GL}_2(\mathbb{R})$ of invertible 2×2 real matrices is a group under matrix multiplication. The neutral element is the identity matrix, and the inverse of a matrix A is its inverse matrix A^{-1}.

Question 1 *What other examples of groups do you know?*

3. The integer line

We now define a model $\mathcal{M}_\mathbb{Z}$. The points are

$$\mathcal{P} = \mathbb{Z}.$$

The lines are the subsets of the form

$$\{k, k+1\}, \qquad k \in \mathbb{Z}.$$

Thus $\{0, 1\}$, $\{1, 2\}$, $\{2, 3\}$, $\{-1, 0\}$, and $\{-2, -1\}$ are lines.

The goal of this activity is to determine

$$\mathrm{Aut}(\mathcal{M}_\mathbb{Z}).$$

A transformation of $\mathcal{M}_\mathbb{Z}$ is a bijection $f : \mathbb{Z} \to \mathbb{Z}$ such that, for every $k \in \mathbb{Z}$, the image

$$f(\{k, k+1\}) = \{f(k), f(k+1)\}$$

is again a line. In other words, $f(k)$ and $f(k+1)$ must be consecutive integers.

4. First examples and non-examples

Question 2 *Is the map exchanging* 0 *and* 3*, and fixing every other integer, a transformation?*

No. Let f be this map. Then

$$f(\{2,3\}) = \{f(2), f(3)\} = \{2,0\} = \{0,2\}.$$

But $\{0,2\}$ is not a line, because 0 and 2 are not consecutive. Hence f is not a transformation.

Question 3 *Is the map exchanging* 0 *and* 1*, and fixing every other integer, a transformation?*

No. Let f be this map. Then

$$f(\{1,2\}) = \{f(1), f(2)\} = \{0,2\}.$$

Again, $\{0,2\}$ is not a line. Hence f is not a transformation.

5. Translations

For every $\ell \in \mathbb{Z}$, define

$$T_\ell : \mathbb{Z} \to \mathbb{Z}, \qquad T_\ell(k) = k + \ell.$$

We claim that T_ℓ is a transformation.

First, T_ℓ is a bijection. Its inverse is $T_{-\ell}$, since $T_{-\ell}(T_\ell(k)) = k$.

Second, T_ℓ sends lines to lines. Indeed,

$$T_\ell(\{k, k+1\}) = \{T_\ell(k), T_\ell(k+1)\} = \{k+\ell, k+1+\ell\}.$$

This is the line

$$\{k+\ell, (k+\ell)+1\}.$$

Therefore T_ℓ is a transformation.

6. Reflections

Define

$$s : \mathbb{Z} \to \mathbb{Z}, \qquad s(k) = -k.$$

We claim that s is a transformation.

First, s is a bijection, and $s^{-1} = s$. Second,

$$s(\{k, k+1\}) = \{s(k), s(k+1)\} = \{-k, -k-1\} = \{-k-1, -k\}.$$

This is a line, because $-k-1$ and $-k$ are consecutive. Thus s is a transformation.

More generally, for any $a \in \mathbb{Z}$, the map

$$k \longmapsto a - k$$

is a transformation. It is the composition $T_a \circ s$.

7. Normalizing an arbitrary transformation

Let $f \in \mathrm{Aut}(\mathcal{M}_{\mathbb{Z}})$. Suppose

$$f(0) = m.$$

We want to reduce to the case where 0 is fixed.

Since T_{-m} is a transformation, the composition

$$g := T_{-m} \circ f$$

is also a transformation. Moreover,

$$g(0) = T_{-m}(f(0)) = T_{-m}(m) = 0.$$

Now we ask: where can $g(1)$ go?

Since $\{0, 1\}$ is a line, its image under g must be a line:

$$g(\{0, 1\}) = \{g(0), g(1)\} = \{0, g(1)\}.$$

The only lines containing 0 are $\{-1, 0\}$ and $\{0, 1\}$. Therefore

$$g(1) = 1 \qquad \text{or} \qquad g(1) = -1.$$

Thus every transformation can be normalized so that 0 is fixed, and then there are two cases:

$$g(0) = 0, \quad g(1) = 1,$$

or

$$g(0) = 0, \quad g(1) = -1.$$

8. Case 1: $g(0) = 0$ and $g(1) = 1$

We now prove that if $g \in \mathrm{Aut}(\mathcal{M}_{\mathbb{Z}})$, $g(0) = 0$, and $g(1) = 1$, then

$$g = \mathrm{id}\,.$$

Step 1: showing that $g(2) = 2$

Since $\{1, 2\}$ is a line, its image is a line:

$$g(\{1, 2\}) = \{g(1), g(2)\} = \{1, g(2)\}.$$

Thus $g(2)$ must be adjacent to 1. Therefore

$$g(2) = 0 \qquad \text{or} \qquad g(2) = 2.$$

But $g(0) = 0$, and g is injective. Since $2 \neq 0$, we cannot have $g(2) = 0$. Therefore

$$g(2) = 2.$$

Step 2: showing that $g(3) = 3$

Since $\{2, 3\}$ is a line, its image is a line:

$$g(\{2, 3\}) = \{g(2), g(3)\} = \{2, g(3)\}.$$

Thus $g(3)$ must be adjacent to 2. Therefore

$$g(3) = 1 \qquad \text{or} \qquad g(3) = 3.$$

But $g(1) = 1$, and g is injective. Since $3 \neq 1$, we cannot have $g(3) = 1$. Therefore

$$g(3) = 3.$$

9. Reminder: what is induction?

We now want to show that $g(k) = k$ for all nonnegative integers k.

When a pattern repeats, a common proof strategy is **induction**. The idea is the following. Suppose we want to prove a statement $P(n)$ for every integer $n \geq 0$. It is enough to prove:

(a) **Base case:** $P(0)$ is true.

(b) **Induction step:** assuming $P(k)$ is true, prove $P(k + 1)$.

We will use a slightly stronger version, called **strong induction**. To prove $P(n)$ for all $n \geq 0$, we prove:

(a) **Base case:** $P(0)$ is true.

(b) **Strong induction step:** assuming $P(0), P(1), \ldots, P(k)$ are true, prove $P(k + 1)$.

10. Step 3: showing that $g(k) = k$ for all $k \geq 0$

We prove by strong induction that

$$g(k) = k$$

for all $k \geq 0$.

The base case is $k = 0$, and it is true because $g(0) = 0$.

Now assume that $g(0) = 0, g(1) = 1, \ldots, g(k) = k$, where $k \geq 1$. We want to prove that $g(k + 1) = k + 1$.

Since $\{k, k+1\}$ is a line, its image is a line:

$$g(\{k, k+1\}) = \{g(k), g(k+1)\} = \{k, g(k+1)\}.$$

Therefore $g(k+1)$ must be adjacent to k. Hence

$$g(k+1) = k-1 \qquad \text{or} \qquad g(k+1) = k+1.$$

But $g(k-1) = k-1$ by the induction hypothesis, and g is injective. Since $k+1 \neq k-1$, we cannot have $g(k+1) = k-1$. Therefore

$$g(k+1) = k+1.$$

By strong induction,

$$g(k) = k$$

for every $k \geq 0$.