MA294 Lecture

Timothy Kohl

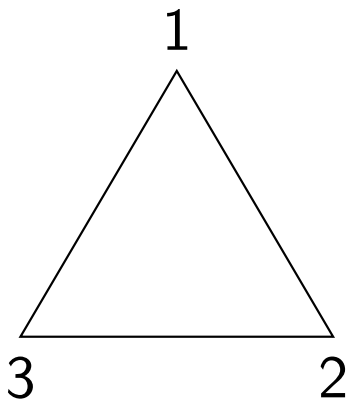
Boston University

February 1, 2024

Dihedral Groups

Our next example, is the first in a family of groups, which are called the *Dihedral* groups, which are denoted D_n for $n = 3, 4, \ldots$ and are the 'plane symmetries of the regular n-gon', i.e. a polygon with n-sides all the same length.

The first of these is D_3, the group of plane symmetries of the equilateral triangle.

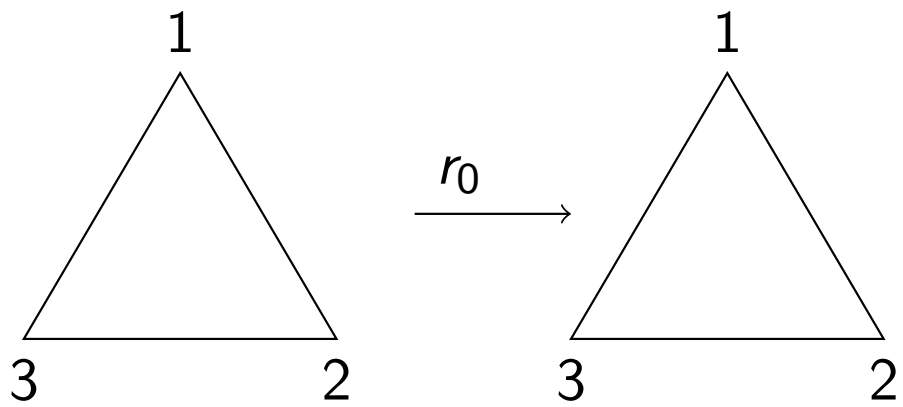


where by plane symmetries we mean rotations and 'flips' of the triangle which leave the triangle as it was, except perhaps for moving its vertices.

The symmetries of a regular n-gon consists of **r**otations, and **f**lips, and there are n of each type for a total of $2n$ overall.
For the case $n = 3$ we have $D_3 = \{r_0, r_{120}, r_{240}, f_1, f_2, f_3\}$ where the subscript on r is the angle (in degrees) one rotates (clockwise).

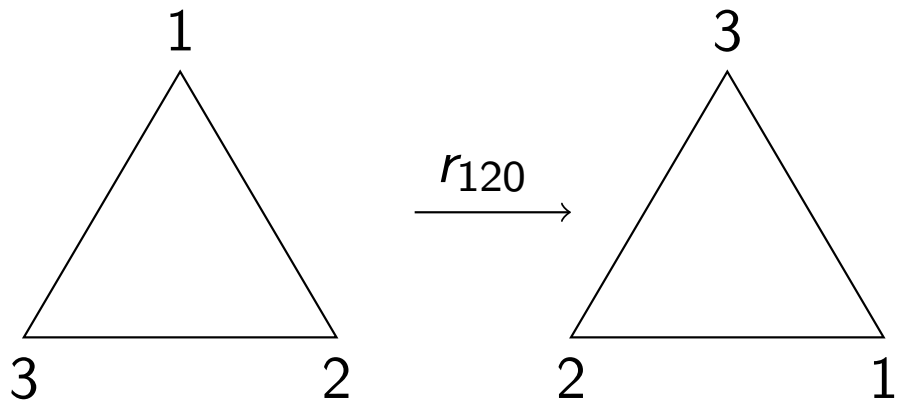
We'll get to the flips in a moment.

The first is r_0 which is a clockwise rotation of 0 degrees, i.e.

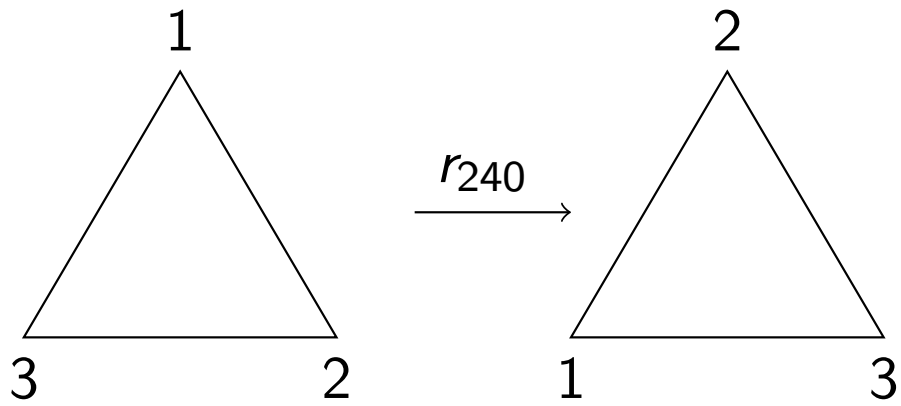


which doesn't do anything to the triangle, but that's fine, and we'll see how this operation will be the identity element of the group D_3.

The other two rotations act as follows:

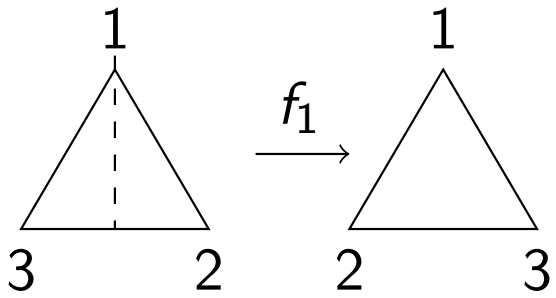


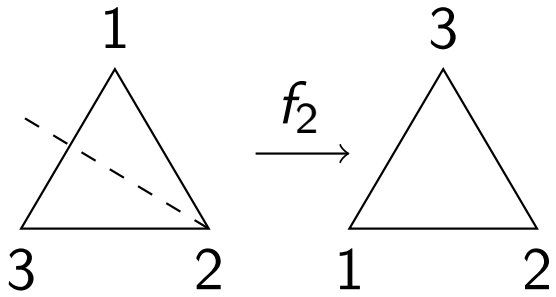
which, as you can see, cyclically moves the vertices in a clockwise fashion, and similarly

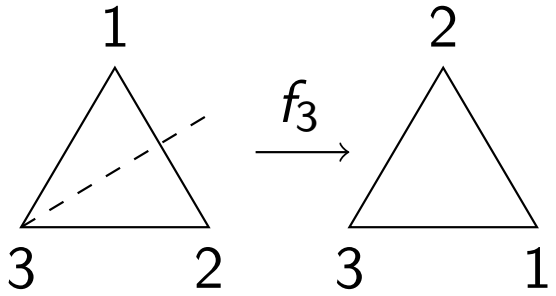


which rotates a further (1/3) turn which can, again, be seen by looking at the vertices.

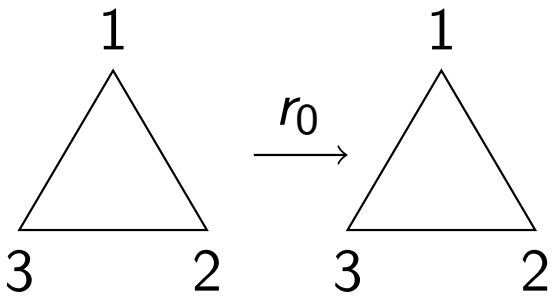
The three flips f_1, f_2, f_3 are obtained by drawing a line through a vertex to the opposite side and then flipping it over the line, thereby exchanging the other two vertices.

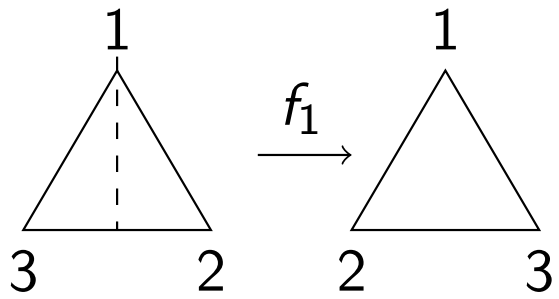


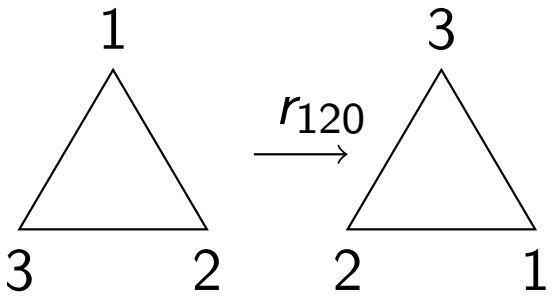


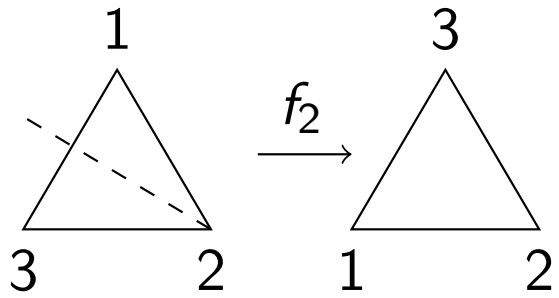


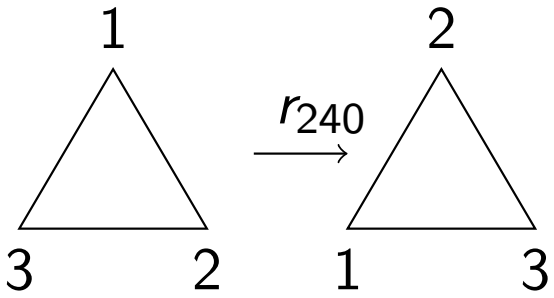
$D_3 = \{r_0, r_{120}, r_{240}, f_1, f_2, f_3\}$

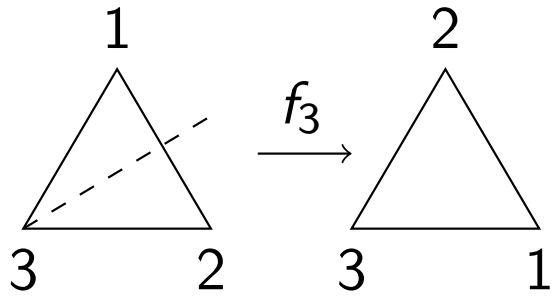












To set the stage for the group 'multiplication' we shall define for D_3 we should point out that the elements of D_3 (or any D_n for that matter) are functions whose input is the triangle, and whose output is yet another triangle (basically the same one) but has been 'repositioned'.

i.e. Literally

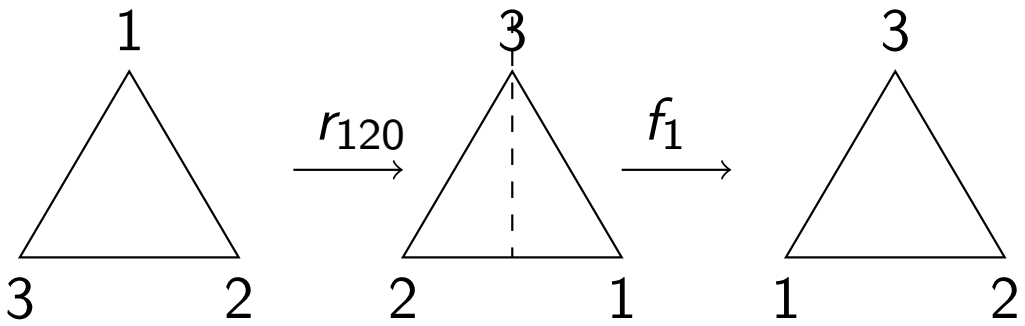
$$r_{120}\left(\begin{array}{ccc} & 1 & \\ 3 & \triangle & 2 \end{array}\right) = \begin{array}{ccc} & 3 & \\ 2 & \triangle & 1 \end{array}$$

and, being functions, we can make sense of an expressions like

$$(f_1 \circ r_{120})\left(\begin{array}{ccc} & 1 & \\ 3 & \triangle & 2 \end{array}\right) = f_1\left(r_{120}\left(\begin{array}{ccc} & 1 & \\ 3 & \triangle & 2 \end{array}\right)\right)$$

We have the *set* of six operations $D_3 = \{r_0, r_{120}, r_{240}, f_1, f_2, f_3\}$,so let's consider the 'multiplication' on this set that turns it into a group?

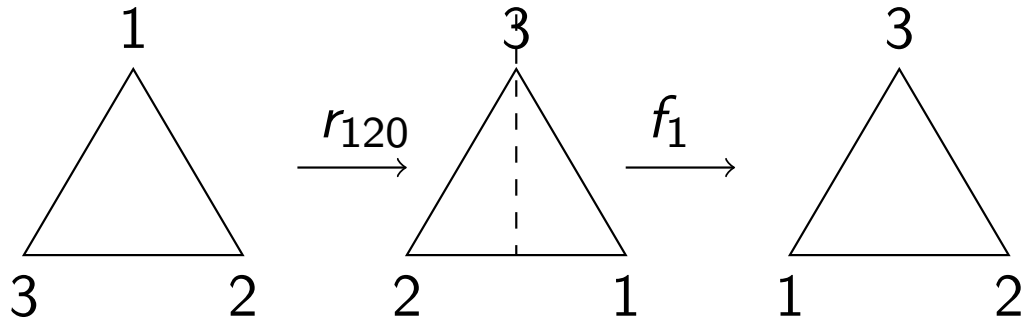
For example, $f_1 \circ r_{120}$ means first apply r_{120}, and then apply f_1,



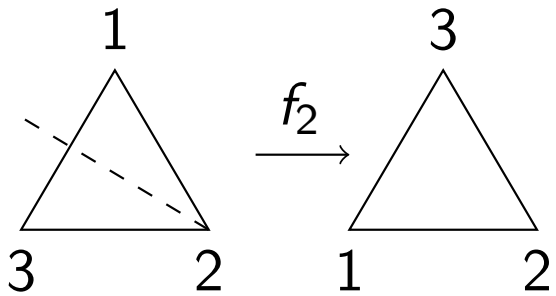
and keep in mind that in the f_1 operation we applied, the flip was about the line through where the 1 vertex is at the *beginning*.

The key observation we wish to make is that $f_1 \circ r_{120}$ is equivalent to one of the six operations in D_3, but which one?

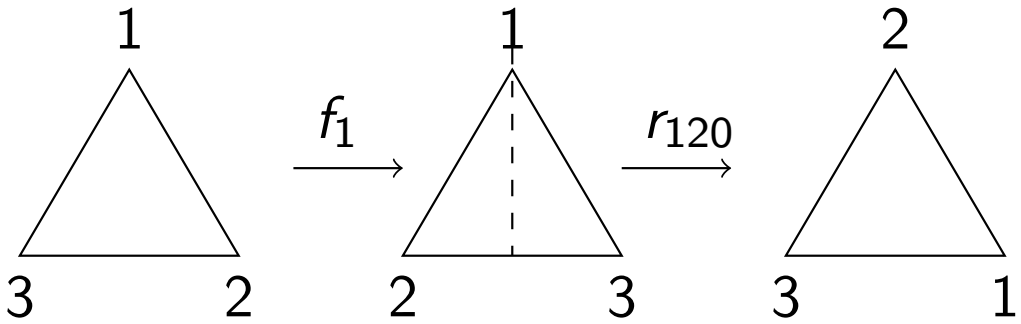
Observe that $f_1 \circ r_{120}$



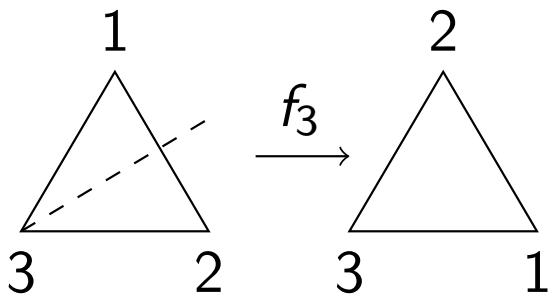
equals f_2, namely



In comparison, consider $r_{120} \circ f_1$:



which equals f_3, namely



So in particular, we find that

$$r_{120} \circ f_1 \neq f_1 \circ r_{120}$$

so the group operation in D_3 is not commutative, which is different than all the other examples of groups we've seen so far.

Indeed, in a group $(G, *)$ it need not always be the case that $a * b = b * a$ for every $a, b \in G$.

Recall that the arithmetic of $\mathbb{Z}_4$ is fully revealed by considering the table

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

which is filled in by computing all the possible $i + j$ for $i, j \in \mathbb{Z}_4$, where i is in the left column, and j is in the top row, and the cells are filled in with $i + j \in \mathbb{Z}_4$.

We call such a structure, for a group (like $(\mathbb{Z}_4, +)$ for example) a 'group table' or 'Cayley table'.

Let's consider the group table for D_3.

$\circ$	r_0	r_{120}	r_{240}	f_1	f_2	f_3
r_0	r_0	r_{120}	r_{240}	f_1	f_2	f_3
r_{120}	r_{120}	r_{240}	r_0	f_3	f_1	f_2
r_{240}	r_{240}	r_0	r_{120}	f_2	f_3	f_1
f_1	f_1	f_2	f_3	r_0	r_{120}	r_{240}
f_2	f_2	f_3	f_1	r_{240}	r_0	r_{120}
f_3	f_3	f_1	f_2	r_{120}	f_{240}	r_0

where we note how the composition gives rise to the elements in the cells, e.g.

- $r_{120} \circ f_1 = f_3$
- $f_1 \circ r_{120} = f_2$

Given the group table for D_3 we can make some observations:

$\circ$	r_0	r_{120}	r_{240}	f_1	f_2	f_3
r_0	r_0	r_{120}	r_{240}	f_1	f_2	f_3
r_{120}	r_{120}	r_{240}	r_0	f_3	f_1	f_2
r_{240}	r_{240}	r_0	r_{120}	f_2	f_3	f_1
f_1	f_1	f_2	f_3	r_0	r_{120}	r_{240}
f_2	f_2	f_3	f_1	r_{240}	r_0	r_{120}
f_3	f_3	f_1	f_2	r_{120}	f_{240}	r_0

- r_0 is the identity of D_3 (Look at the gray cells in the table.)
- $r_{120}^{-1} = r_{240}$ and $r_{240}^{-1} = r_{120}$
- $r_{120} \circ r_{120} = r_{240}$ which makes sense, but also $r_{240} \circ r_{240} = r_{120}$ (Why?)
- $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, and $f_3^{-1} = f_3$ (Yes, this can happen.)

The one axiom for being a group we haven't discussed for the case of D_3 is associativity.

That is, how to we know that, for example

$$f_1 \circ (r_{120} \circ r_{120}) = (f_1 \circ r_{120}) \circ r_{120}$$

or for any other composition in D_3?

The reason that this is true is that the group operation is function composition.

Recall from basic algebra/calculus that if, for example $f(x) = e^x$, $g(x) = cos(x)$ and $h(x) = x + 1$ what it means to compose $(f \circ g)(x)$ which is $f(g(x)) = e^{g(x)} = e^{cos(x)}$.

And for three functions we have
$(f \circ g \circ h)(x) = f(g(h(x))) = e^{g(h(x))} = e^{cos(h(x))} = e^{cos(x+1)}$.

The point is, $(f \circ g) \circ h = f \circ (g \circ h)$ since, applied to a given x, one applies h first, then g, and then f, i.e. we can drop the parentheses and simply write it as $(f \circ g \circ h)(x)$, which is exactly what associativity is all about.

As noted earlier, function composition is not commutative and for groups we don't necessarily expect the group operation to be commutative.

Definition

A group $(G, *)$ is commutative or abelian (after N.H. Abel) if for all $a, b \in G$ one has $a * b = b * a$.

Note: If for even one pair of elements a,b one has $a * b \neq b * a$ then G is non-abelian.

Also, being non-abelian does **not** say that $a * b \neq b * a$ for *all* a, b, only that it happens for at least one a, b.

We've seen already some examples of abelian groups, e.g. $(\mathbb{Z}, +)$, $(\mathbb{Z}_m, +)$, and $(U(m), \cdot)$.

And we've already established that D_3 is non-abelian.

There is another important example of a non-abelian group, which comes from the study of matrices in linear algebra.

Recall that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ are 2×2 matrices, that we can multiply them as follows

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix}$$

and one may show (after a bit of calculation) that for matrices M, N, P, that $(MN)P = M(NP)$, namely that matrix multiplication is associative.

Also recall that if $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and furthermore, if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $\delta = det(M) = ad - bc$ (the determinant).

So if $\delta \neq 0$ then we can define $N = \frac{1}{\delta}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d/\delta & -b/\delta \\ -c/\delta & a/\delta \end{pmatrix}$.

This matrix has the property that $MN = I$ and $NM = I$, namely $N = M^{-1}$ the inverse of M.

This combination leads to the following group definition.

Definition

The 2^{nd} general linear group (over the reals $\mathbb{R}$)

$$\begin{aligned} GL_2(\mathbb{R}) &= \{2 \times 2 \text{ invertible matrices with entries in } \mathbb{R}\} \\ &= \{2 \times 2 \text{ real matrices } A \text{ where } det(A) \neq 0\} \end{aligned}$$

And, as we've just demonstrated, this *is* a group, and moreover an *infinite* group since it contains infinitely many members.

Note also, we could replace $\mathbb{R}$ with the integers $\mathbb{Z}$ and get another version of this,

$$GL_2(\mathbb{Z}) = \{2 \times 2 \text{ invertible matrices with entries in } \mathbb{Z}\}$$

the only difference would be that the invertibility of a given integer matrix is a bit more subtle than it is for real matrices.

Specifically recall that if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $\delta = det(M) = ad - bc$ (the determinant) where (if M had real entries)

$$M^{-1} = \frac{1}{\delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d/\delta & -b/\delta \\ -c/\delta & a/\delta \end{pmatrix}$$

But for

$$M^{-1} = \frac{1}{\delta}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d/\delta & -b/\delta \\ -c/\delta & a/\delta \end{pmatrix}$$

the issue is that $\frac{1}{\delta}$ is real provided $\delta \neq 0$, but if M is an integer matrix, then $\delta \in \mathbb{Z}$ only if $\delta = \pm 1$.

The upshot of this is that for an integer matrix M to be invertible, one must have that $det(M) = \pm 1$, not just that it be non-zero!