MA294 Lecture

Timothy Kohl

Boston University

July 2, 2025

Groups

The integers mod m, $\mathbb{Z}_m$ under addition, and $U(m)$ the units mod m under multiplication, are prototype examples of the concept of a 'group' which is one of the most important ideas in mathematics.

Definition

Given a set G, a binary operation $*$ is a function which assigns to every ordered pair of elements $(a, b) \in G \times G$ another element of G denoted $a * b$.

i.e. If $a, b \in G$ then $a * b \in G$ which is also phrased as 'G is closed with respect to $*$'.

Now, this 'closure' property is sometimes included as part of the definition of group, but we define it separately, in order to focus on the three fundamental aspects of what it means for a set G with a binary operation $*$, sometimes written $(G, *)$, to be a group.

Definition

A set G with a binary operation $*$, denoted $(G, *)$, is a **group** if the following properties hold.

- $(a * b) * c = a * (b * c)$ for all $a, b, c, \in G$. [associativity]
- There exists an element $e \in G$, called (an) identity, such that $a * e = a$ and $e * a = a$ for all $a \in G$. [identity element]
- For every $a \in G$, there exists $b \in G$ such that $a * b = e$ and $b * a = e$. (Such an element b is called an inverse to a.) [inverses]

There are two quick facts we can establish about groups.

Proposition

In a group $(G, *)$ the identity element is unique, and every element has a unique inverse.

Proof

Suppose e, e' are both identity elements in G.

Consider $e * e'$. Since e is an identity

$$e * e' = e'$$

but since e' is *also* an identity, $e * e' = e$, and so

$$e * e' = e'$$
$$e * e' = e$$

So $e = e'$.

Proof continued

Given a in G, let b, c be inverses, and consider $b * a * c$ which can be parenthesized in two ways:

$$(b * a) * c$$

which must equal $e * c$ since b is an inverse of a, but $e * c = c$. Conversely, we can parenthesize it as

$$b * (a * c) = b * e = b$$

again because c is an inverse of a.

Lastly, we invoke associativity to realize that

$$(b * a) * c = c$$
$$b * (a * c) = b$$

so $c = b$. $\square$

We note that the group operation is not always denoted by $*$, (which looks like 'multiplication') so sometimes if the group is related to arithmetic, we use 'additive notation' and use the symbol $+$.

As such, if we use a 'multiplicative' symbol like '$*$' then the inverse of 'a' might be denoted a^{-1}, in particular because inverses have now been proven to be unique!

Similarly, if the group operation is 'additive' we might denote the inverse of 'a' by $-a$ and perhaps use the symbol '0' to denote the identity.

The notation though can vary greatly for different examples of groups.

Indeed arithmetic provides our first source of examples.

Example: $(\mathbb{Z}, +)$ is a group (the integers with addition)
Why?

Well it's certainly closed, i.e. $a, b \in \mathbb{Z}$ implies $a + b \in \mathbb{Z}$.

Also $a + (b + c) = (a + b) + c$ is a familiar fact we're all used to.

And the number 0 is such that $a + 0 = a = 0 + a$, and for every $a \in \mathbb{Z}$.

Morever, for every integer $a \in \mathbb{Z}$, the integer $-a \in \mathbb{Z}$ where now
$a + (-a) = 0 = (-a) + a$.

Before we explore more examples, let's consider some 'non-examples', namely sets with binary operations that turn out not to be groups.

Keep in mind that in order for a set with a given operation to be a group, the operation must be closed, and the associativity, identity, and inverse axioms must hold.

As such, if any property fails, we don't have a group structure.

Non-Example: $(\mathbb{Z}, \cdot)$, namely the integers with multiplication.

What fails?

Well, if $a, b \in \mathbb{Z}$ then clearly $a \cdot b \in \mathbb{Z}$ so closure holds.✓

We also know that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ so associativity holds.✓

Also, the number 1 acts as the identity since $a \cdot 1 = a = 1 \cdot a$.✓

As to inverses, we observe that, for example there is no integer a such that $2 \cdot a = 1$, and certainly 0 does not have a multiplicative inverse.

This last point echoes that discussion of units mod m as we saw earlier, which led to the development of $U(m)$.

Indeed, $\mathbb{Z}_m$ is not a group under multiplication since not every element has an inverse under multiplication, especially 0.

More on this later.

Here is another non-example based on the integers, namely $(\mathbb{Z}, -)$.

This is not a group even though it is closed.

What fails is associativity, and the existence of an identity, and therefore inverses.

i.e. Generally $(a - b) - c \neq a - (b - c)$ and while $a - 0 = a$, $0 - a = -a$.

Note also, that if one property fails, one doesn't need to check whether any others *do* hold since the group definition requires all 3 (or 4 if you include closure) properties to hold.

Other examples of groups.

$(\mathbb{Q}, +)$ - The rational numbers $\frac{a}{b}$ with addition.

closure and associativity are clear, and 0 is the identity as it is for $\mathbb{Z}$, and for $\frac{a}{b} \in \mathbb{Q}$, one has $-\frac{a}{b} \in \mathbb{Q}$ too.

If $\mathbb{Q}^*$ is the set of non-zero rationals, and $\cdot$ is multiplication, then $(\mathbb{Q}^*, \cdot)$ is a group,again, closure and associativity are clear,and certainly $\frac{a}{b} \cdot 1 = \frac{a}{b}$.

The omission of 0 gives rise to the existence of inverses for every element,since if $\frac{a}{b} \in \mathbb{Q}^*$ then $\frac{b}{a} \in \mathbb{Q}^*$ and obviously $\frac{a}{b} \cdot \frac{b}{a} = 1$.

Recall that $U(m)$ is constructed from $\mathbb{Z}_m$ by omitting those elements of $\mathbb{Z}_m$ that don't have inverses.

Is there a subset of $\mathbb{Z}$ which is a group under multiplication?

Yes, but it's kind of small, namely $\{\pm 1\}$ since any integer $a < -1$ or $a > 1$ will not have an inverse, but $(-1)(-1) = 1$ and also $(-1) \cdot 1 = (-1$ and $1 \cdot (-1) = -1$ and of course, $1 \cdot 1 = 1$.

Two really simple (dare I say trivial) examples of groups.

$(\{0\}, +)$ - literally the number zero by itself under addition

$(\{1\}, \cdot)$ - literally the number 1 under multiplication.

The verification of these is not too difficult.

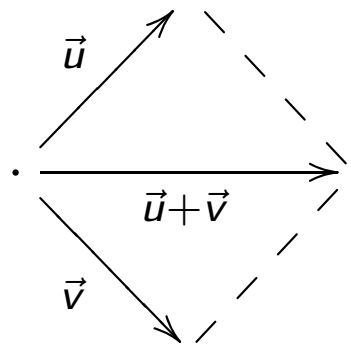
And, of course, as explored earlier, $(\mathbb{Z}_m, +)$ and $(U(m), \cdot)$ are both groups, where in $\mathbb{Z}_m$ it's addition mod m and in $U(m)$ it's multiplication mod m.

We noted in the development of $\mathbb{Z}_m$ and $U(m)$ that they do indeed form groups under the different operations.

We should also note that we consider the addition and multiplication operations on $\mathbb{Z}_m$, in particular how they interact via the distibutive law $a \cdot (b + c) = a \cdot b + a \cdot c$.

Sets which are closed with respect to *two* operations like this are called rings, which is a different class of mathematical objects we'll explore later in the course.

Another example of a group is the set of vectors in the plane, where the addition is by the so-called 'parallelogram rule' to add two vectors $\vec{u}$ and $\vec{v}$ to get $\vec{u} + \vec{v}$.



And one can see that this operation is closed and associative.

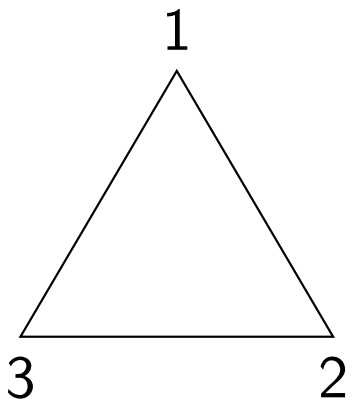
Moreover, there exists $\vec{0}$ which has zero length and has the property that $\vec{0} + \vec{u} = \vec{u}$.

Also, for every vector $\vec{u}$, the vector pointing in the *opposite direction* may be denoted $-\vec{u}$ and the sum of them is the zero vector $\vec{0}$.

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.

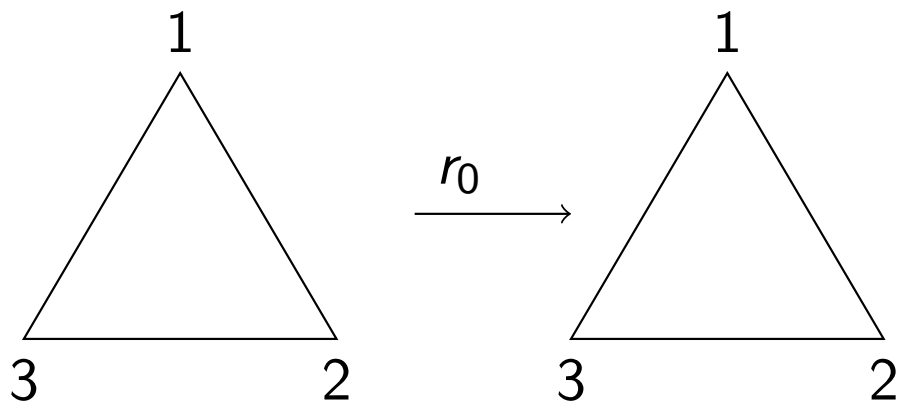


where by plane symmetries we mean rotations and 'flips' of the triangle which leave the triangle as it was, except perhaps for moving its vertices.

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).

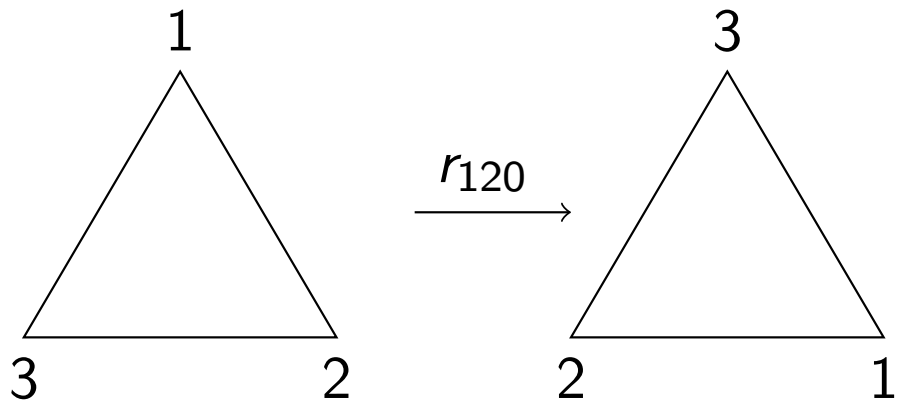
We'll get to the flips in a moment.

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

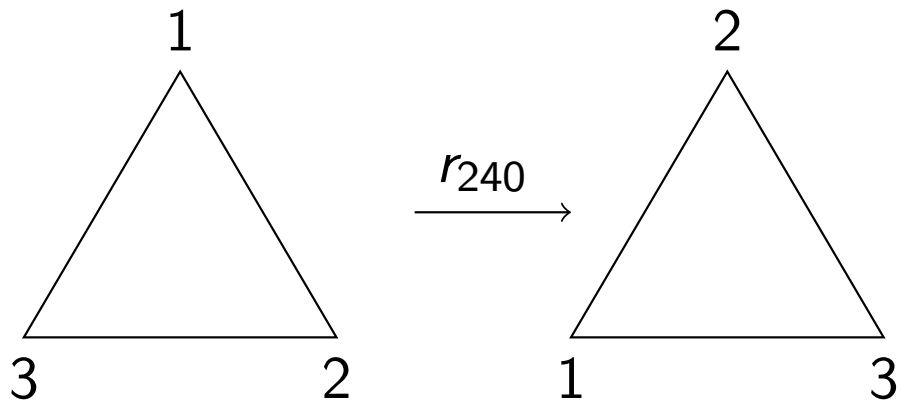


which doesn't do anything to the triangle, but that's fine, and we'll see how this operation will be the identity element of the group D_3.

The other two rotations act as follows:

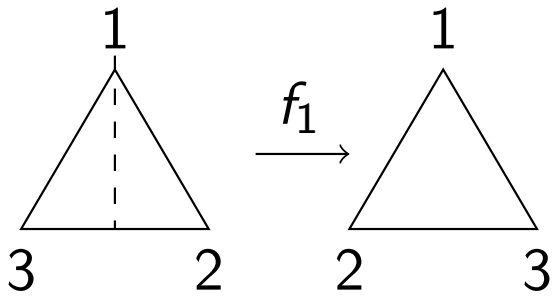


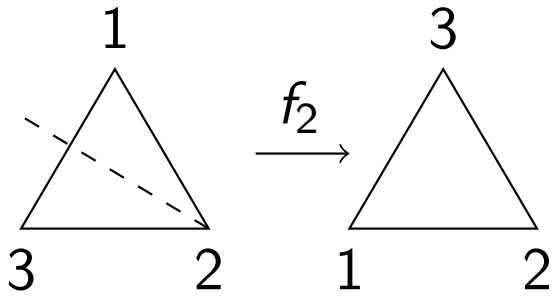
which, as you can see, cyclically moves the vertices in a clockwise fashion, and similarly

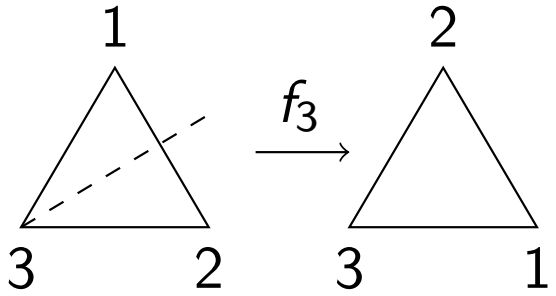


which rotates a further (1/3) turn which can, again, be seen by looking at the vertices.

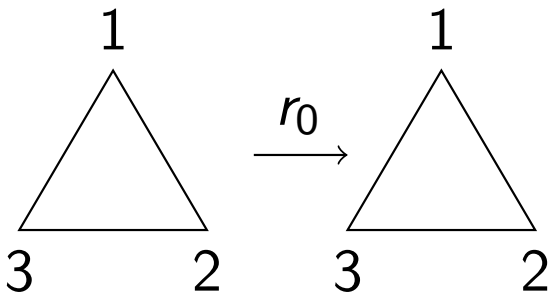
The three flips f_1, f_2, f_3 are obtained by drawing a line through a vertex to the opposite side and then flipping it over the line, thereby exchanging the other two vertices.

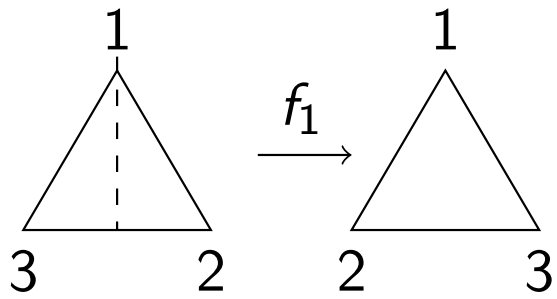


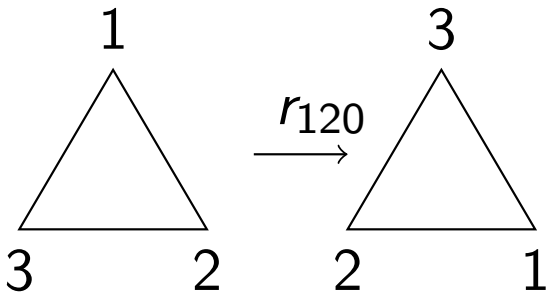


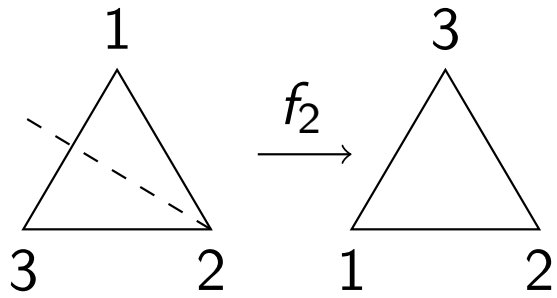


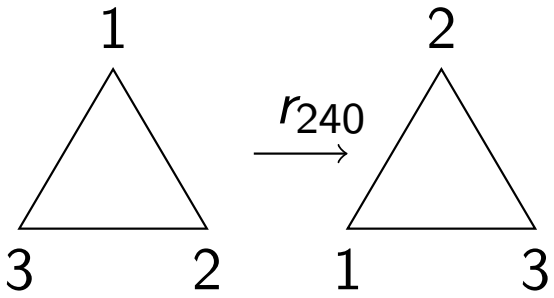
$D_3 = \{r_0, r_{120}, r_{240}, f_1, f_2, f_3\}$

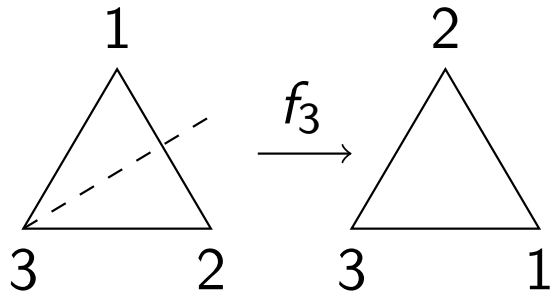












To set the stage for the group 'multiplication' we shall define for D_3 we should point out that the elements of D_3 (or any D_n for that matter) are functions whose input is the triangle, and whose output is yet another triangle (basically the same one) but has been 'repositioned'.

i.e. Literally

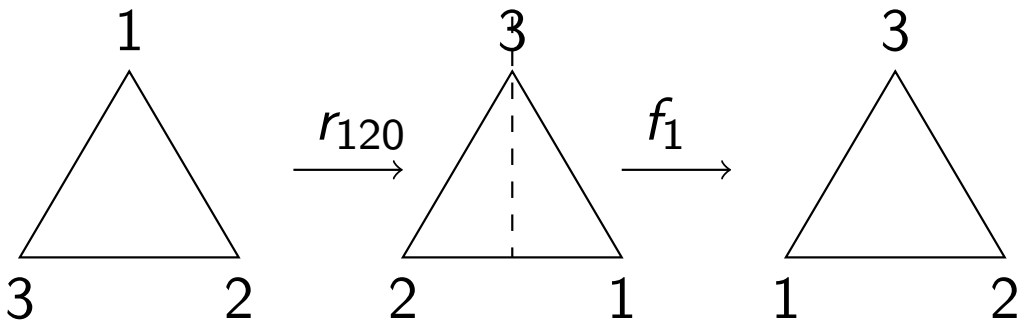
$$r_{120}\left(\begin{array}{ccc} & 1 & \\ 3 & \triangle & 2 \end{array}\right) = \begin{array}{ccc} & 3 & \\ 2 & \triangle & 1 \end{array}$$

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?

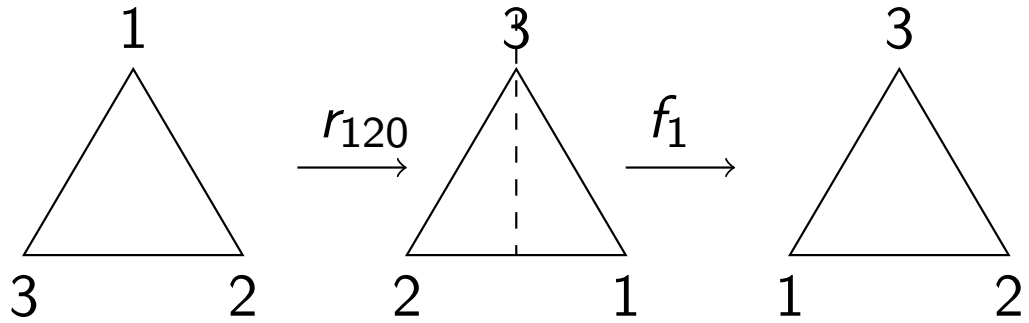
For example, $f_1 \circ r_{120}$ means first apply r_{120}, and then apply f_1,



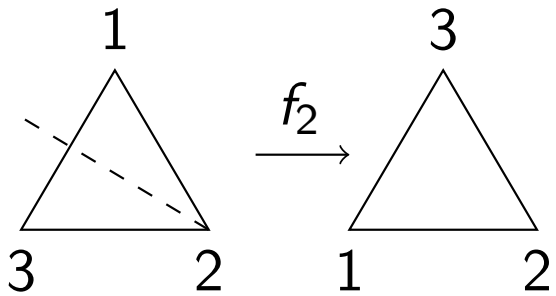
and keep in mind that in the f_1 operation we applied, the flip was about the line through where the 1 vertex is at the *beginning*.

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?

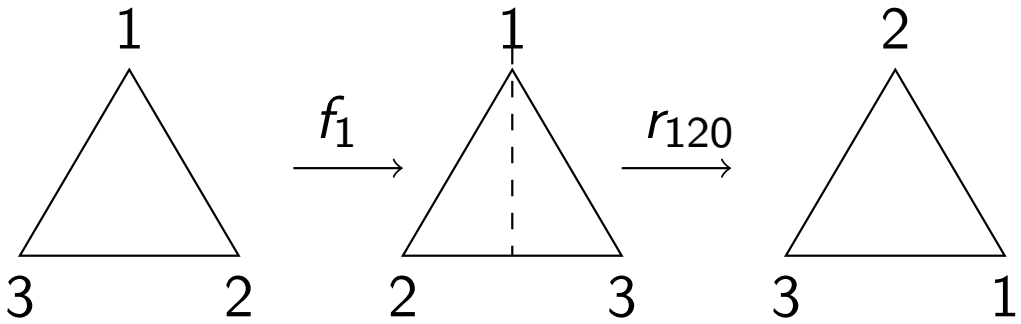
Observe that $f_1 \circ r_{120}$



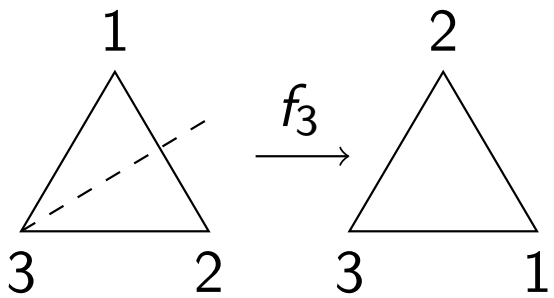
equals f_2, namely



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!