MA294 Lecture

Timothy Kohl

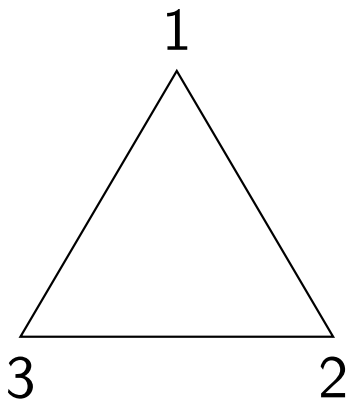
Boston University

July 8, 2021

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.

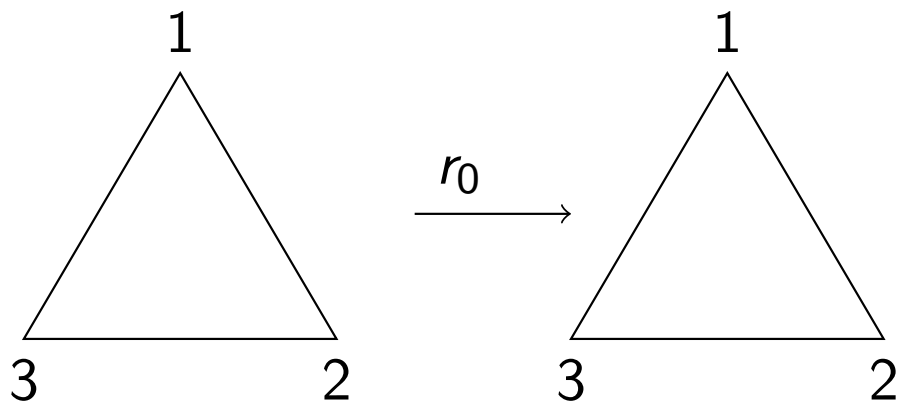


where by plane symmetries we mean rotations and 'flips' of the triangle which leave the triangle as it was, except perhaps for moving its vertices.

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).

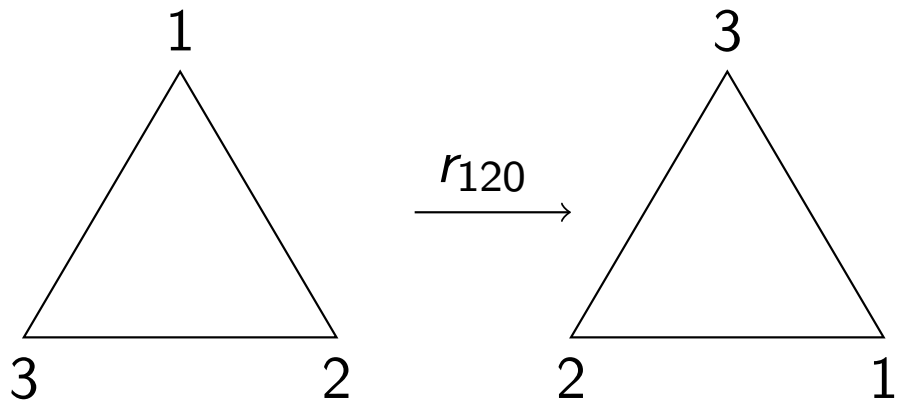
We'll get to the flips in a moment.

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

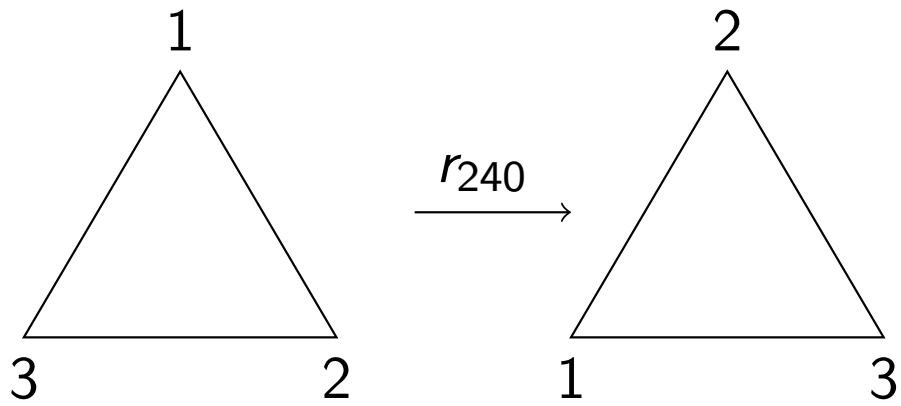


which doesn't do anything to the triangle, but that's fine, and we'll see how this operation will be the identity element of the group D_3.

The other two rotations act as follows:

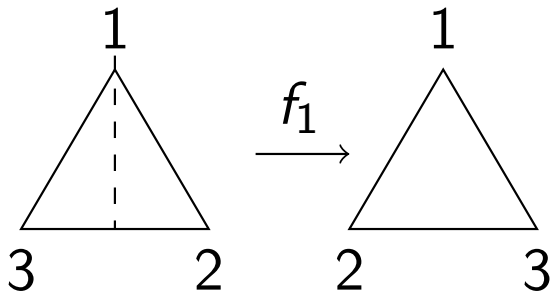


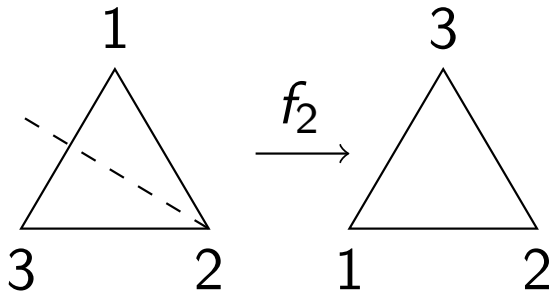
which, as you can see, cyclically moves the vertices in a clockwise fashion, and similarly

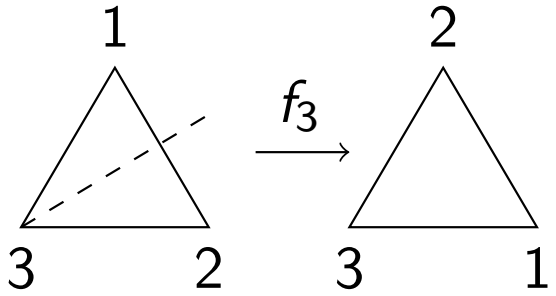


which rotates a further (1/3) turn which can, again, be seen by looking at the vertices.

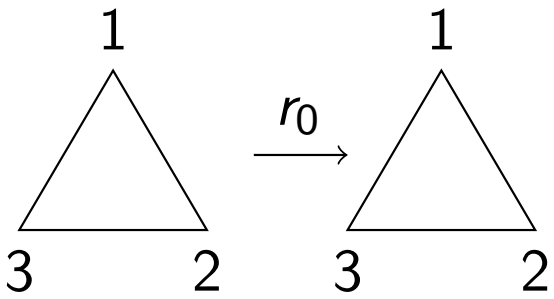
The three flips f_1, f_2, f_3 are obtained by drawing a line through a vertex to the opposite side and then flipping it over the line, thereby exchanging the other two vertices.

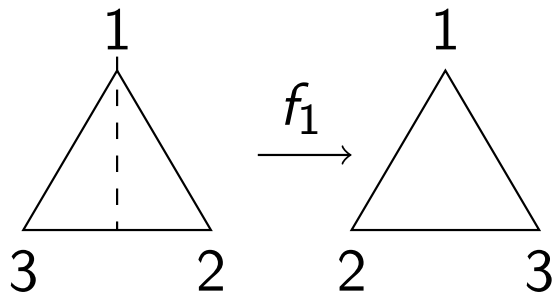


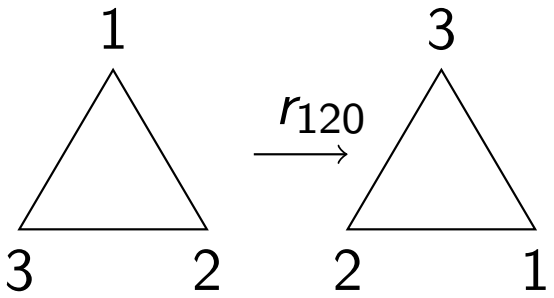


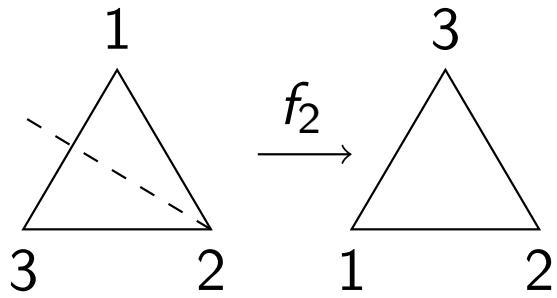


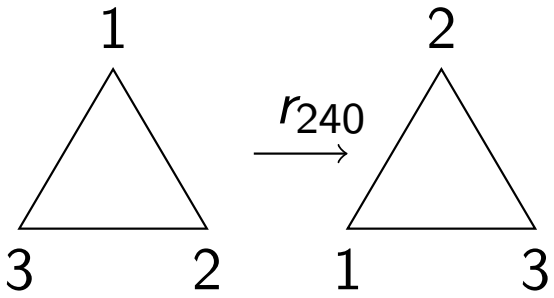
$D_3 = \{r_0, r_{120}, r_{240}, f_1, f_2, f_3\}$

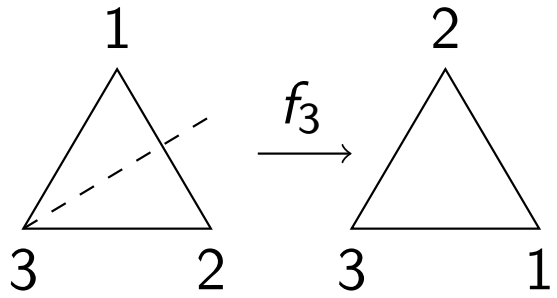












To set the stage for the group 'multiplication' we shall define for D_3 we should point out that the elements of D_3 (or any D_n for that matter) are functions whose input is the triangle, and whose output is yet another triangle (basically the same one) but has been 'repositioned'.

i.e. Literally

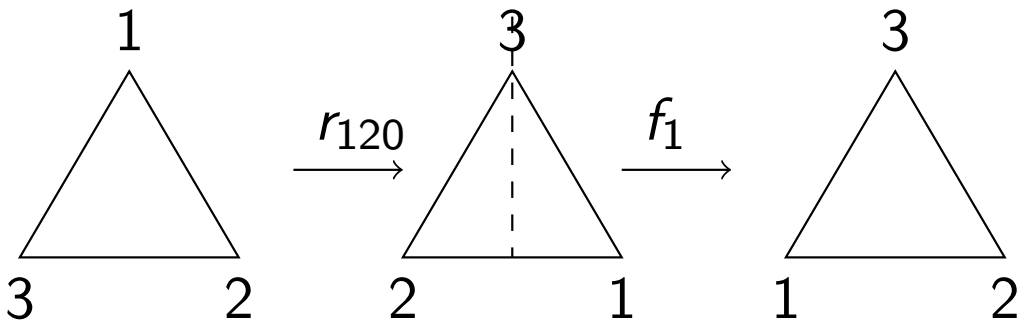
$$r_{120}\left(\begin{array}{ccc} & 1 & \\ 3 & \triangle & 2 \end{array}\right) = \begin{array}{ccc} & 3 & \\ 2 & \triangle & 1 \end{array}$$

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?

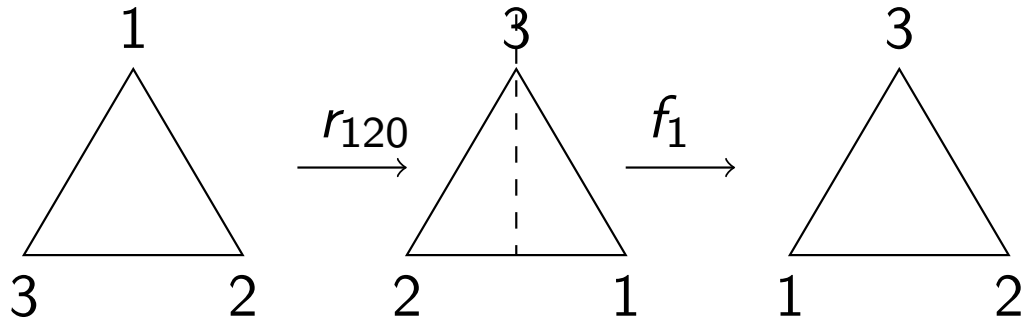
For example, $f_1 \circ r_{120}$ means first apply r_{120}, and then apply f_1,



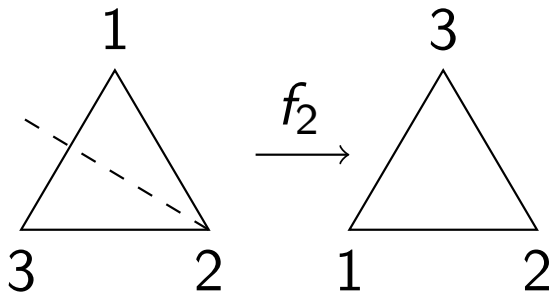
and keep in mind that in the f_1 operation we applied, the flip was about the line through where the 1 vertex is at the *beginning*.

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?

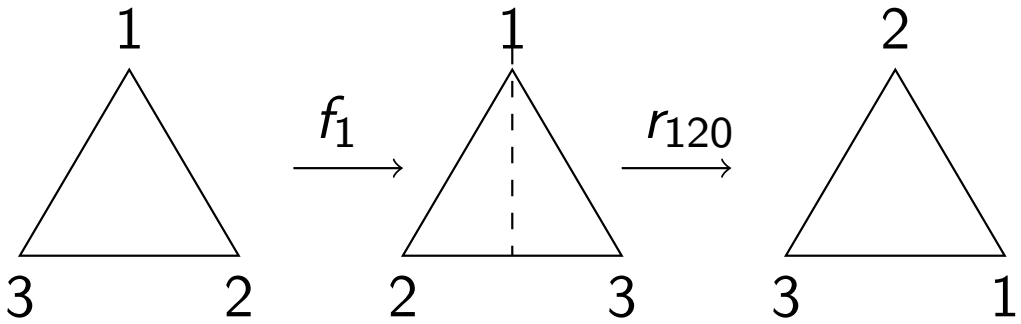
Observe that $f_1 \circ r_{120}$



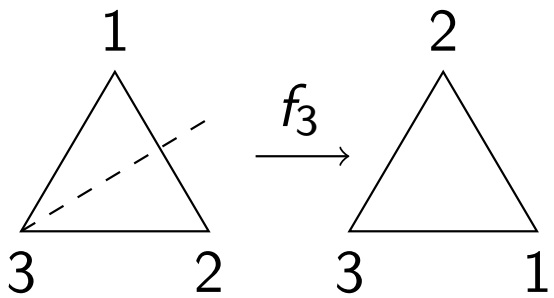
equals f_2, namely



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 considering 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.

We note again, for emphasis.

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 $\mathbb{R}$)

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

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

Other basic facts about groups:

Proposition

Let x, y, z, a, b be elements of a group $(G, *)$ then

$$x * y = x * z \rightarrow y = z \text{ (left cancellation)}$$
$$a * x = b * x \rightarrow a = b \text{ (right cancellation)}$$

Proof.

$$x * y = x * z$$
$$x^{-1} * x * y = x^{-1} * x * z \text{ (Note, we multiply both sides on the } \textit{left}.\text{)}$$
$$e * y = e * z$$
$$y = z$$

A similar argument works for the other statement. □

These 'cancellation' rules imply the following.

Proposition

The Cayley table for a group $(G, *)$ is a latin square.

Why? If we look at a row of the Cayley table:

$*$		y	$\ldots$	z
x		$x * y$		$x * z$

we cannot have $x * y = x * z$ unless $y = z$ by left cancellation so there are no repeats in a given row.

And for columns:

$*$		x	$\ldots$	
a		$a * x$		
b		$b * x$		

we find that $a * x = b * x$ only if $a = b$ so there are no repeated elements in a column.

The Order of a Group Element

Definition

In a group $(G, *)$ if $a \in G$ and $n \geq 1$ is an integer, then

$$a^n = \underbrace{a * a * \cdots * a}_{n\text{-times}}$$

That is $a^1 = a$, $a^2 = a * a$, $a^3 = a * a * a$, and similar to how one defines a^0 for a *number*, we define $a^0 = e$, the identity of G.

And the use of the notation 'a^{-1}' for the inverse, fits in with this definition, since

$$a^{-1} * a = a^{-1} * a^1 = a^{(-1)+1} = a^0 = e$$

and similarly, we may define a^{-n} to be $a^{-1} * a^{-1} * \cdots * a^{-1} = (a^{-1})^n$. That is, exponents in groups, work like they do for numbers.

Notation Alert: If $*=$'$+$' like in $\mathbb{Z}$ or $\mathbb{Z}_m$ then instead of writing

$$a^n = a * a * \cdots a$$

we write

$$na = a + a + \cdots + a$$

so that, for example, if $2 \in \mathbb{Z}_5$ we have $3 \cdot 2 = 2 + 2 + 2 = 6 = 1$.

An important,yet not so obvious point is that for any $a \in G$ and any n the power $a^n \in G$ by the closure property.

The simplest way to see this is by noting that $a^n = \underbrace{a * a * \cdots * a}_{(n-1)\text{-times}} * a$

namely $a^{n-1} * a$.

So if we assume that $a^{n-1} \in G$ then $a^{n-1} * a \in G$ so $a^n \in G$.

And the same holds for negative powers.

Other examples:
In D_3, we have

$$r_{120}^0 = r_0$$
$$r_{120}^1 = r_{120}$$
$$r_{120}^2 = r_{120} \circ r_{120} = r_{240}$$
$$r_{120}^3 = r_{120}^2 \circ r_{120} = r_{240} \circ r_{120} = r_0 \text{ [Why?]}$$
$$r_{120}^4 = r_{120}^3 \circ r_{120} = r_0 \circ r_{120} = r_{120} \text{ [Note: We're back at } r_{120}\text{]}$$
$$r_{120}^{-1} = r_{240}$$
$$r_{120}^{-2} = r_{120}$$
$$r_{120}^{-3} = r_0$$

For the flips like f_1 the powers are a bit simpler

$$f_1^0 = r_0$$
$$f_1^1 = f_1$$
$$f_1^2 = r_0$$
$$f_1^3 = f_1$$
$$f_1^{-1} = f_1$$

And in $\mathbb{Z}_6$ we have

$$
\begin{aligned}
0 \cdot 2 &= 0 \\
1 \cdot 2 &= 2 \\
2 \cdot 2 &= 2 + 2 = 4 \\
3 \cdot 2 &= 2 + 2 + 2 = 0 \\
4 \cdot 2 &= 2 + 2 + 2 + 2 = 2 \\
(-1) \cdot 2 &= (-2) = 4 \\
(-2) \cdot 2 &= (-4) = 2
\end{aligned}
$$

etc...

The discussion of powers of elements leads naturally to the concept of 'order' of an element.

Definition

If $x \in G$ where G is finite, then the order of x is the least positive integer m such that $x^m = e$, in which case we write $|x| = m$.

If G is infinite, then it's possible that $x, x^2, x^3, \ldots$ are all distinct (non-identity) elements of G, in which case we say that x has infinite order and we write $|x| = \infty$.

Note, if G is infinite, (as a set) it's still possible that it has elements of finite order, there are many possibilities.

Examples:

For $2 \in \mathbb{Z}_6$ we have $1 \cdot 2 = 2$, $2 \cdot 2 = 4$ and $3 \cdot 2 = 0$ and so $|2| = 3$.

In D_3, $|r_{120}| = 3$ since $r_{120}^2 = r_{240}$ and $r_{120}^3 = r_{360} = r_0$

In contrast, $|f_1| = 2$ since $f_1^2 = r_0$.

For the element $1 \in \mathbb{Z}$ we have the multiples $1, 1+1 = 2, 1+1+1 = 3, \ldots$ none of which *ever* equals 0, so 1 has infinite order.

Note, for any group G, the identity element e has order 1, and it is the unique element of order 1.

If $x \in G$ has order m then $x^{2m} = (x^m)^2 = e^2 = e$, and similarly $x^{3m} = e$ etc.

Theorem

If $x \in G$ and $|x| = m$ then $x^t = e$ if and only if $m|t$.

Proof.

Suppose $x^t = e$, where t is *not* a multiple of m then by the division algorithm $t = qm + r$ where $r \in \{1, \ldots, m-1\}$ (i.e $r \neq 0$) which means $x^t = x^{qm+r} = x^{qm}x^r$.

But $x^{qm} = (x^m)^q = e$ so we have that $x^t = x^r$ but then since $x^t = e$ then $x^r = e$.

However, since $r < m$ this contradicts the fact that $|x| = m$, which is the *least* positive power of x which is the identity. □

What can happen is that for some groups G, there is an $x \in G$ such that $G = \{e, x, x^2, \ldots, x^{m-1}\}$ and one says that x *generates* G.

Also, we sometimes use the notation of '1' for the identity which is consistent with the usual view of raising a number to the zero-th power being 1, i.e. $x^0 = 1$, so that if G is generated by x, it consists of $\{1, x, x^2, \ldots, x^{m-1}\}$ if $|x| = m$.

If G is generated by x the we write $G = \langle x \rangle$, and we sometimes say G is a *cyclic* group since the powers of x 'cycle' through these distinct powers, i.e.

$$1, x, x^2, \ldots, x^{m-1}, x^m = 1, x^{m+1} = x, x^{m+2} = x^2, \ldots \text{ etc.}$$

If G is infinite, then it's possible that for some element x one has that $G = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$.

How does this work?

Well, it simply means that each non-zero power of x is not the identity of G, so that G consists of

$$\{\dots, x^{-3}, x^{-2}, x^{-1}, x^0 = 1, x^1 = x, x^2, x^3, \dots\}$$

in which case we say that G is an infinite cyclic group.
The prime example of this is $\mathbb{Z} = \langle 1 \rangle$ since every element of $\mathbb{Z}$ is a multiple of 1.

In fact, we can use this idea to actually *define* an infinite group consisting of powers of x.

For x a 'variable' (symbol, whatever), one can define 'the' infinite cyclic group

$$C_\infty = \{x^n \mid n \in \mathbb{Z}\}$$

with the group operation being based on the rules of exponents, namely that $x^i * x^j = x^{i+j}$ which is very naturally closed, and associative since $x^i * (x^j * x^k) = x^i * x^{j+k} = x^{i+j+k}$ which is the same as $(x^i * x^j) * x^k = x^{i+j} * x^k$.

Moreover, it contains an identity element $1 = x^0$ since clearly $x^0 * x^i = x^i$ and $x^i * x^0 = x^i$, and similarly every element x^i has inverse x^{-i}.

If you've observed that the operations in C_∞ mirror those of the integers, you are correct, but the interesting contrast is that C_∞ is 'multiplicative' but that $\mathbb{Z}$ is an additive group.