Groups, Mappings, 'Morphisms

Damien Sullivan

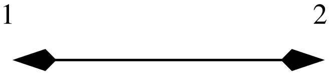
December 22, 2002

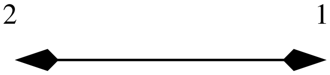
Contents

Abstract

An introduction to groups automorphisms, endomorphisms, characteristic and fully invariant subgroups, commutators and their subgroups, and centers.

1 Some sample groups

Consider a line with labeled ends. 

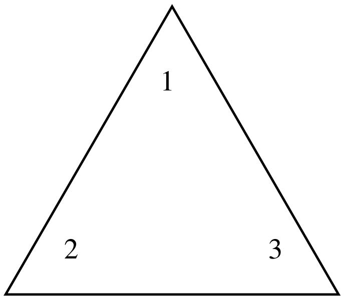
There are two things we can do to it while leaving the line in place. We can "do nothing" (think of adding zero to a number) and we can flip the line. (Or rotate it 180 degrees, with the same effect.) 

We can combine these operations, although the only interesting combination is flipping the line twice, which gives us the original figure. We can make a multiplication table of the operations:

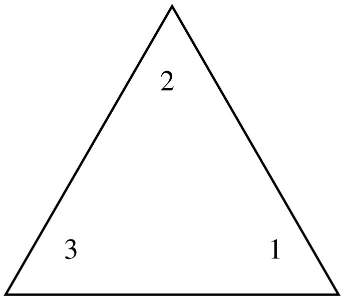
	do nothing	flip
do nothing	original	flipped
flip	flipped	original

or

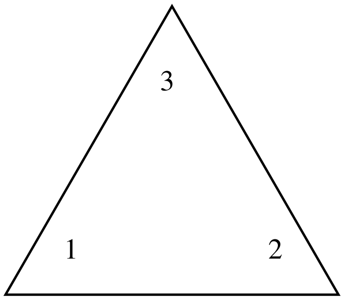
	I	s
I	I	s
s	s	I



Not very exciting. But consider an equilateral triangle cutout, pinned to some cardboard, so you can rotate it. There are two other positions leaving the triangle in place, corresponding to rotations of 120 and 240 degrees.



rotation 120 degrees (s)



rotation 240 degrees (s^2)

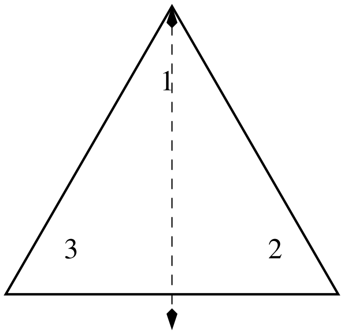
If we call the rotations s and s^2 and ”do nothing” I we can make the following table, whose values the reader should be able to verify:

	I	s	s^2
I	I	s	s^2
s	s	s^2	I
s^2	s^2	I	s

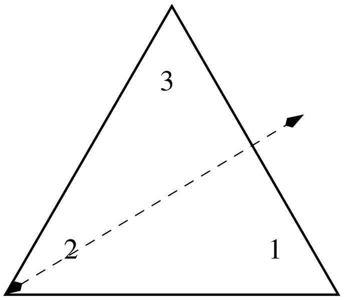
Similarly we can make regular polygons with any number of sides, and consider their rotations, keeping the outline of the figure constant. We can also extend the idea to a circle with a mark somewhere on it; there are infinitely many rotations in this case, giving us a group with an (uncountable) infinite number of members. These groups are called *cyclic*, or Cyc_n[1] where $_n$ is the number of sides. So our first group is Cyc_2, the triangle Cyc_3, the square Cyc_4, and so on.

The next step is to take the polygons, in our case the triangle, off the cardboard. Now we can not only rotate them, but we can flip them around an axis, giving us three new states (and operations to generate the states.)

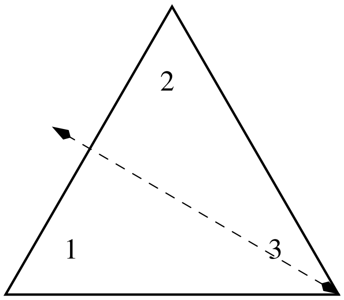
Flip or reflection around the top vertex (t)



Flip or reflection around the left vertex (l)



Flip or reflection around the right vertex (r)



[1] More commonly known as C_n or Z_n, due to Z being a name for the integers. This is all part of the tendency for any field of mathematics to adopt the Roman and Greek alphabets for its own exclusive use, which is fine as long as you don't try to change fields. As I am a generalist writing for generalists, I strive for a larger namespace. Judging by the diversity of the group theory books I have looked at, choosing my own notation is no great act of rebellion.

And we get an expanded multiplication table:

	I	s	s^2	t	l	r
I	I	s	s^2	t	l	r
s	s	s^2	I	r	t	l
s^2	s^2	I	s	l	r	t
t	t	l	r	I	s	s^2
l	l	r	t	s^2	I	s
r	r	t	l	s	s^2	I

Notice something different here: s followed by t gives r, but t followed by s is l. Unlike the previous groups, or the arithmetic we learn as children, the rotations and reflections of the triangle, simple though this group is, are not commutative. Some elements (s, s^2) commute with each other, but only the identity element I commutes (trivially) with everything in the group. Also note that while we defined all three flips of the triangle, in a real sense we only need one. We started out being able to rotate the triangle; given the ability to flip it on its back, we can keep on rotating, and reach all of the configurations of the other flips. As illustration here's a table where l has been replaced by ts and r by st.

	I	s	s^2	t	ts	st
I	I	s	s^2	t	ts	st
s	s	s^2	I	st	t	ts
s^2	s^2	I	s	ts	st	t
t	t	ts	st	I	s	s^2
ts	ts	st	t	s^2	I	s
st	st	t	ts	s	s^2	I

For comparsion, look at the table for Cyc_6, the rotations of the hexagon (chosen for having the same number of elements):

	I	s	s^2	s^3	s^4	s^5
I	I	s	s^2	s^3	s^4	s^5
s	s	s^2	s^3	s^4	s^5	I
s^2	s^2	s^3	s^4	s^5	I	s
s^3	s^3	s^4	s^5	I	s	s^2
s^4	s^4	s^5	I	s	s^2	s^3
s^5	s^5	I	s	s^2	s^3	s^4

If you flip this table (or those of the other Cyc groups) around a diagonal from the top left to the bottom right, you get the same table, which is not the full table of the triangle.

Just as we can look at the rotations of any polygon, we can look at the rotations+flips of any polygon. This class of groups is known as dihedral (”two-faced”) groups, or Dih_n,[2] and the full group of the triangle is Dih_3.

[2] Usually D_n.

There's something else we can learn from the triangle. Look at the sequence of numbers of each triangle figure, starting from the top vertex and going counterclockwise. The first three, the members of Cyc_3, give (1,2,3), (2,3,1), and (3,1,2) – (1,2,3) on a cyclic conveyor belt. The other three give us (1,3,2), (3,2,1) and (2,1,3). Together the six sequences form all the possible permutations of three elements. This is actually a coincidence, given how we defined the group; in general Dih_n has $2n$ elements – n rotations and n flips – while permutations have n! $n!$ elements. But the permutations of n elements do in fact constitute a group $Perm_n$,[3] and it just happens that $Perm_3$ equals Dih_3.

2 Abstraction of Groups

So why are we calling these things "groups", anyway? Technically, a group is a set of elements and an operation on the set, which takes two elements and returns a third. (Also called binary operation.) There's closure – take two elements, operate, and you get another element, not something else. There's associativity – the order of a sequence operations matters, as we've seen with Dih_3, but given a sequence it doesn't matter how you group them. $a(bc) = (ab)c$. And groups have an identify element, and a unique inverse for every element. All of the groups we've seen have these properties – closure, identity, and for every element there's some element such that when you combine them you get the identity. $tt = I$. $ss^2 = I$.

Note that technically, the group of Dih_3, say, isn't the set of positions of the triangle, it's the set of the *motions* of the triangle, and the group operation is simply that of doing one operation after another, with the result being whichever motion would have given the current position of the triangle. The labels s and t can applied both to positions of the triangle and to the motions which produce the positions; the set of group elements is actually the motions.

The ideas here can be made more general and more specific. Semi-groups just have closure and associativity; think of an arbitrary graph. There are also rings and fields, as well as other categories, which are groups with more constraints on them. But I won't go into details about those.

3 Applying the abstraction; More Groups

For a very different example, consider the set of integers, the binary operation of addition. (Here the group elements aren't motions, they're just numbers!) We have closure – integers + integer gives an integer. We've got an identity, zero. And every postive number n has an inverse, which is $-n$, and vice versa.

[3] Usually S_n, for "symmetric group. So why aren't I calling it $Symm_n$? Because then I'd have to say why it's called symmetric, and I can't. It's not obviously symmetric, and Douglas Hofstadter, who aimed at visualization and intuitive understanding, skipped this. The books mumble about "symmetric polynomials", which work, but have no obvious motivation.

But the books clearly and early define S_n as the group of permutations of n elements, so I may as well *call* it that.

Voila, it's a group! A commutative [4] one, too. The fractions under addition and the reals under addition also are groups.

The fractions or the reals, not including zero, under multiplication, are also groups. Here the identify is 1, and inverses are reciprocals. We have to exclude zero, since it has no inverse, and the integers aren't a group – they're closed under multiplication, but you need fractions to get inverses. They'd be another example of a semi-group which wasn't a group, though.

We also find that the even integers under addition are a group. Or the multiples of three, or four, or any integer. So the even integers are a subset of the integers, but a self-contained group under the same group operation. We call this a subgroup, a group which is contained within another. Similarly the positive fractions (or reals) are a subgroup of all the non-zero fractions (or reals) under multiplication. And going back to our earlier examples, we can see that Cyc_3 is a subgroup of Dih_3, as are $\{I,t\},\{I,l\},\{Ir\}$. Cyc_6 has the subgroups $\{I,s^3\},\{I,s^2,s^4\}$.

We can also see that just as a single flip of the triangle expanded the range of positions, from the three rotations to the 6 rotations+reflections, just adding -1 to the group of the positive fractions under multiplication doubles the size of the group, bringing in all the negative fractions. (And likewise for the reals.) Ditto for adding 1 to the even integers under addition.

4 Non-Groups

In learning a new category it helps to have examples of things not in it, as well as things that are. So what are things which might look like groups but aren't, and why? As we've already touched upon, *all* the fractions or reals under multiplication aren't a group, because zero has no inverse. The integers under multiplication aren't either, for the different reason that no integer except 1 and -1 has an inverse under multiplication. The negative numbers under multiplication aren't; no identity or inverse, plus it's not closed. The non-negative numbers under addition lack inverses; the positive numbers under addition also lack an identity. The integers under division lack closure (or, depending on how you look at it, a fully defined operation.) Numbers under absolute value aren't; absolute value isn't even a binary operation.

5 Mappings and 'Morphisms

An automorphism is an isomorphism of a group to itself. An isomorphism is a 1-1 homomorphism. A homomorphism is a mapping which preserves group structure.

Let us work our way back up. A group is a set of elements and an operation upon them; a mapping is simply that, a map from the set of group elements to some other set, or in general a map of any set to another set, as

[4] Or *abelian*, after the mathematician Abel

long as each element in the first set is mapped to only one element in the second. One could map the group of the triangle Dih_3, $\{I, s, s^2, t, l, r\}$ to $\{cat, dog, icecream, monkey, 4, 2\}$ quite legitimately, although there would be little obvious reason to do so. [5] Usually we map the group elements to the set of elements of another group, and in particular we usually require homomorphism: preserving group structure. The identity of one group should map to the identity of the second group; pairs of inverses in the first group should map to pairs of inverses in the second group; elements which commute should map to elements which commute. This is captured by

$$\phi(a)\phi(b) = \phi(ab)$$

where ϕ is the mapping under consideration. We can see that this does express the conditions above:

$$\phi(x) = \phi(Ix) = \phi(I)\phi(x)$$

so $\phi(I)$ must be the identity of the second group. And

$$\phi(I) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$$

so $\phi(x^{-1})$ must equal $\phi(x)^{-1}$. Finally

$$ab = ba$$

$$f(ab) = f(ba)$$

$$f(a)f(b) = f(b)f(a)$$

Then an endomorphism is a homomorphism of a group to itself, e.g. mapping $\{I, s, s^2\}$ of Dih_3 to $\{I\}$ and the other three elements to $\{t\}$. An isomorphism is a homomorphism which is one-to-one, and an automorphism is a one-to-one isomorphism, e.g mapping $\{I, s, s^2, t, l, r\}$ to $\{I, s^2, s, t, r, l\}$

Sample mappings

	generic	$*s$	homom. (into Cyc^6)	endomorphic	automorphic	$*g$	$g^{-1}xg$
I	cat	s	I	I	I	x	IxI
s	dog	s^2	I	I	s	xs	s^2xs
s^2	4	I	I	I	s^2	xs^2	sxs^2
t	s	l	s^3	t	l	xt	txt
l	s	r	s^3	t	r	xl	lxl
r	4	t	s^3	t	$t\ xr$	rxr	

[5] There's a reason I emphasize this arbitrary nature of mappings. Automorphisms are a class of mappings of a group to itself which obey certain constraints, and it can be hard to find all the automorphisms just by looking for natural operations. There is always the option of generating all possible mappings and checking each one for satisfaction of the constraints. The same holds for homomorphisms between groups: one could always set up a generic mapping and check the homomorphism equation. This isn't an ideal option, but it's there.

6 Cosets and Normal Subgroups

A subgroup N of a group G is a subset of the set of elements of G (in which the group relations still hold.) If we multiply the elements of N by an element a not in N we get a set of products, distinct from N, and of the same size as N. This set is called a coset. If there are elements not in N or the coset we can multiply N by one of those and get a new coset, distinct from the first two sets. In general it matters which side we multiply on: $aN \neq Na$. If $aN = Na$, (meaning not that individual products are equal, but that the set of products are equal), then N is called normal or invariant. This is equivalent to being self-conjugating, where $g^{-1}Ng = N$, i.e. $g^{-1}n_1g = n_2$ where n_1 and n_2 are members of N. (See bottom of I)

Illustration: given Dih_3, one subgroup is I, s, s^2. We can multiply on the right by t, which is not in the subgroup, and get $t, st, s^2t = ts$. Or on the left to get $t, ts, ts^2 = st$. In this case it's the same coset, permuted a bit. If we multiply by st we get the same set: $st, s^t = ts, s^3t = t$. On the other hand, we can consider the subgroup I, t and multiply by s to get s, ts on right and s, st on the left. Not the same cosets. So I, s, s^2 is a normal subgroup of Dih_3, with a coset of t, st, s^2t, while I, t (or I, l and I, r) isn't a normal subgroup.

We could also have looked at conjugation, e.g. $tIt = I, tst = s^2, ts^2t = s$, and this is true for conjugation by any element in Dih_3.

7 Examples of Automorphisms

The familiar operation of conjugation $g^{-1}xg$ is an automorphism. It obviously maps group elements to other group elements; it is one-to-one (if you assume otherwise, that $x \neq y$ but $g^{-1}xg = g^{-1}yg$, you find that g and its inverse cancel and that $x = y$, contradicting your assumption.) And it is a homomorphism:

$$Conj(x)Conj(y) = g^{-1}xgg^{-1}yg = g^{-1}xyg = Conj(xy)$$

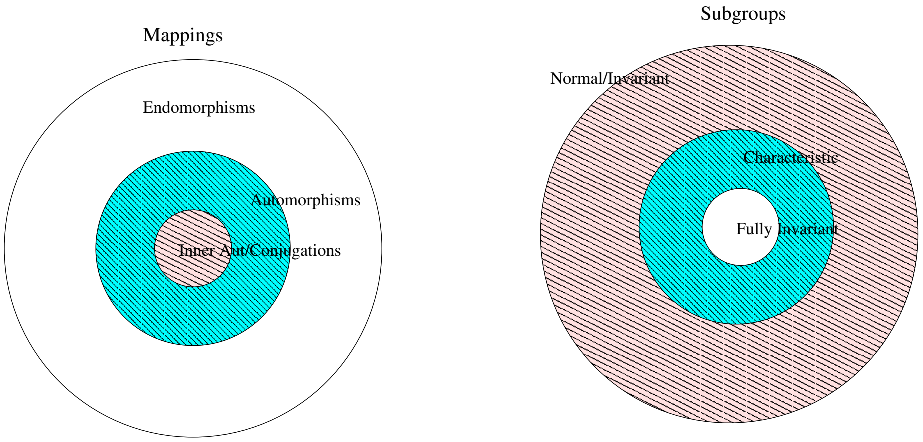
Conjugations are also called inner automorphisms.

Of course for commutative groups conjugates are not very interesting: $g^{-1}xg = g^{-1}gx = x$. But there is another operation which is an automorphism for these groups: mapping elements to their own inverses. Inverses are unique, so this is 1-1, and

$$Inv(x)Inv(y) = x^{-1}y^{-1}$$
$$Inv(xy) = y^{-1}x^{-1}$$

but the group commutes, so $x^{-1}y^{-1} = y^{-1}x^{-1}$ and $Inv(x)Inv(y) = Inv(xy)$

One automorphism of a group can be followed by another, yielding a third automorphism. Since automorphisms are one-to-one they have inverses, and there is the identity automorphism of mapping every group element to itself, so the set of automorphisms of a group is itself a set under the operation of doing successive automorphism of the group. This group is called Aut, and has a subgroup Inn of the conjugations, since the application of the homomorphism



Mappings/Morphisms and their Subgroups

Figure 1: Mappings hierarchy

equation above shows that a conjugation followed by a conjugation is a conjugation. If we map each element g of G to the conjugation $g^{-1}xg$ caused by that element we have a homomorphic mapping from G to $Inn(G)$.

8 Characteristic and Fully Invariant Subgroups

We have already seen that conjugations are automorphisms, and that normal subgroups are self-conjugate, i.e. preserved by conjugations on the group. A characteristic subgroup is one which is preserved by all automorphisms of the group, and may be seen as a refinement of normal subgroups. To be clear, any automorphism of G maps elements of the characteristic subgroup to a distinct and possibly not the same element of that characteristic subgroup. The only element which must map to itself is the identity, preserved by all homomorphisms.

In turn, *fully invariant* subgroups are mapped into themselves by all endormophisms of the group. Note use of the word “into” here, as opposed to “onto”. For example all groups have the trivial endormophism of mapping all elements to the identity; this does not preserve subgroups the same way conjugation and automorphisms preserve normal and characteristic subgroups. But an endormorphism will never map elements of a fully invariant subgroup to elements not in the subgroup. We will see an example of such a subgroup in the section on commutators.

9 Transitivity

Unlike normality, being characteristic or fully invariant subgroups is transitive. If $A \subset B \subset C$ and A is characteristic or fully invariant in B and likewise B is characteristic or fully invariant in C then A is characteristic or fully invariant in C. By definition an automorphism of C maps B to itself (in the characteristic case), and is thus in turn an automorphism of B, which by definition maps A to itself. Similarly an endomorphism of C maps a fully invariant B into itself, which is an endomorphism of B, which will map A into itself.

The reason this does not work for normal subgroups is that while a conjugation of C maps a normal B to itself, this mapping of B is only known to be an automorphism of B, not a conjugation of C, and thus A normal in B may not be preserved by the automorphism, and thus not be preserved by the conjugation of C.

For example Z_2 is normal in D_2 which is normal in D_4, but Z_2 is not normal in D_4.

10 Commutators

The commutator of two group elements a and b is the group element c such that $ab = bac$. It can be thought of as that element which allows a and b to commute. It may also be defined as $Comm(a, b) = a^{-1}b^{-1}ab$; it should be easy to see that this satisfies the role of c. It should also be clear from both definitions that if a and b commute then c is I, and $Comm(a, b)$ will come out to be I. If the group is abelian so that all pairs a, b commute then the only commutator is I and the commutator subgroup is I. The reverse is also true.

Commutators are preserved by homomorphisms.

$$\phi(a^{-1}b^{-1}ab) = \phi(a^{-1})\phi(b^{-1})\phi(a)\phi(b)$$

and remembering that homomorphisms map inverses to inverses we find

$$\phi(a)^{-1}\phi(b)^{-1}\phi(a)\phi(b)$$

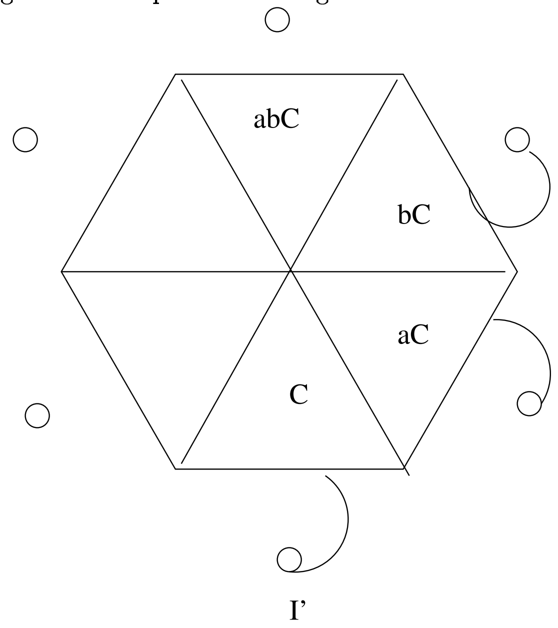
which is a commutator. So if the commutators and their products form a proper subgroup of the group, all endomorphisms will preserve this subgroup, and so it is fully invariant, characteristic, and normal.

The factor group of commutator subgroups is always abelian. It may help to recall what the factor group is, namely where a normal subgroup is mapped to the identity of some group and its cosets are mapped to the other elements of that group. So multiplication in the factor group can be thought of as membership in cosets of the starting group. If N is a normal subgroup of G, aN is in one coset and bN is in another, then in general $aNbN$ goes to one coset of G, and $bNaN$ may go to yet another. But not when $N = C$.

For multiplication of cosets to be commutative we need ab and ba to go to the same coset, $abC = baC$, or in terms of concrete elements $abc_1 = bac_2$.

But we can take c_1 to be I and get $ab = bac$, which is exactly the definition of commutators! If that was too fast there is a longer derivation: $aCbC = abCC = abC = baCC = bCaC$.

A third albeit currently less rigorous way of looking at it is that in making the factor group we have gathered up all the commutators of G into C and then mapped them all to I. For the factor group to not be abelian one of the other elements of G/C must be a commutator (if the only commutator is I the group is abelian). But the pre-image of this commutator cannot be a commutator or product of commutators in G, because those have all be mapped to I. Since homomorphism preserves group structure one might suspect this might not be the case. In a sense we have gathered all the non-commutativity of G into a bag and then squished the bag.



11 Higher Order Commutator Subgroups

But while the factor group of C is always abelian, C itself need not be, in which case we can look for the commutators of C and the subgroup in C they form; such are called higher order commutator subgroups (also derived subgroups). If the original group G is finite then this process must obviously terminate; either we find a subgroup whose commutator subgroup is itself, or we reach an abelian commutator subgroup whose own commutator subgroup is simply $\{I\}$. For example the tetrahedral group A_4 has a commutator subgroup isomorphic to the 4-group, which is abelian. Conversely the icosahedral group A_5 has no (proper) normal subgroups whatsoever, and its commutator subgroup is A_5.

This gets within sight of the unsolvability of the quintic, via results which this paper can only mention lightly. 'Solvable' groups are ones which have a chain of subgroups, each normal in the next larger subgroup, each with an abelian factor group, with the chain terminating in I. A_5 corresponds to some quintic equation, and is not solvable, having no normal subgroups to even start a chain.

12 Centers

The *center* of a group is the set of group elements which commute with every element in the group. Not to be confused with the commutators, which make two elements commute, but needn't themselves commute with anything. A central element c obviously obeys $gc = cg$ for all group elements g. The center is a subgroup: $gc_1c_2 = c_1gc_2 = c_1c_2g$, so the product of two central elements is itself a central element. And the inverse of a central element also commutes with everything:

$$gc^{-1} = h$$

$$g = hc$$

$$g = ch$$

$$c^{-1}g = h = gc^{-1}$$

The center is another example of a fully invariant subgroup, as commutativity is preserved by a homomorphism.

If a group is commutatative, the center is the whole group (all elements commute with everything) and the commutator subgroup is $\{I\}$. Otherwise the center will be a proper subgroup (possibly) $\{I\}$ and the commutator subgroup will be a non-trivial subgroup (and possibly the whole group.)

13 Acknowledgements

Much of this material was directly inspired by Kurosh(1955), and the idea and style owes much to Douglas Hofstadter and his M590 class at IU in 2002.