A CHILD'S GARDEN OF GROUPS

Dihedral Groups, Symmetric Groups, Alternating Groups, Direct Products, and Semidirect Products!

(Part 3)

by

Doc Benton

CONTENTS (PART 3)

INTRODUCTION (PART 3)

There is so much about *groups* that we have covered, and yet there is so much that is still left to cover. We will never exhaust the well of what is already known! Nonetheless, in this third part we do add some very important pieces to the puzzle. Primarily, we begin to look at the different types of *groups* that you may encounter. We've already discussed *cyclic groups* and how we can think of all *groups* as being built from *cycles* that either commute with one another or don't. In this portion, we'll add a little bit more to what we've already learned about *cyclic groups* and we'll introduce some other very important classes of groups such as the *dihedral groups*, the *symmetric groups*, the *alternating groups*, *direct products* of *groups*, and *semidirect products* of *groups*. Following this, we'll introduce you to the *quaternion group* which doesn't fit into any of the more familiar patterns, and we'll also talk about generators for a *group*. Additionally, we look at how we may use GAP software to explore some of these new items that we introduce. There is much to enjoy in Part 3!

CYCLIC GROUPS

We introduced *cyclic groups* back in Part 1 along with the notion that cycles are found everywhere within our lives. In Part 3, we are just going to add a little more to what we have already seen. In particular, a *group* is *cyclic* if we can generate it by multiplying just a single element by itself over and over again until things begin to repeat. Also, the length of a *cycle* tells us beforehand what the size or order of the *group* will be. For example, the *cycle* $(1,2)$ generates a *cyclic group* with just two elements, $(\ )$ and $(1,2)$. However, what may not be immediately apparent is that the permutation $(1,2)(3,4)$ also generates a *group* with two elements, $(\ )$ and $(1,2)(3,4)$. We can easily verify this using GAP.

```
gap> a:=(1,2);
(1,2)

gap> g1:=Group(a);
Group([ (1,2) ])

gap> Size(g1);
2

gap> Elements(g1);
[ (), (1,2) ]

gap> a:=(1,2)*(3,4);
(1,2)(3,4)

gap> g2:=Group(a);
Group([ (1,2)(3,4) ])

gap> Size(g2);
2

gap> Elements(g2);
[ (), (1,2)(3,4) ]
```

Similarly, if we wanted to generate a *cyclic group* of order 6 from scratch, the most obvious thing to do would be to look a multiples of $(1,2,3,4,5,6)$. However, the permutation $(1,2)(3,4,5)$ will also generate a *cyclic group* of order 6, and you can see this by noting that $(1,2)(3,4,5)$ is the product of a 2-*cycle* and a 3-*cycle*. Hence, since 6 is the least common multiple of 2 and 3, it will take 6 applications

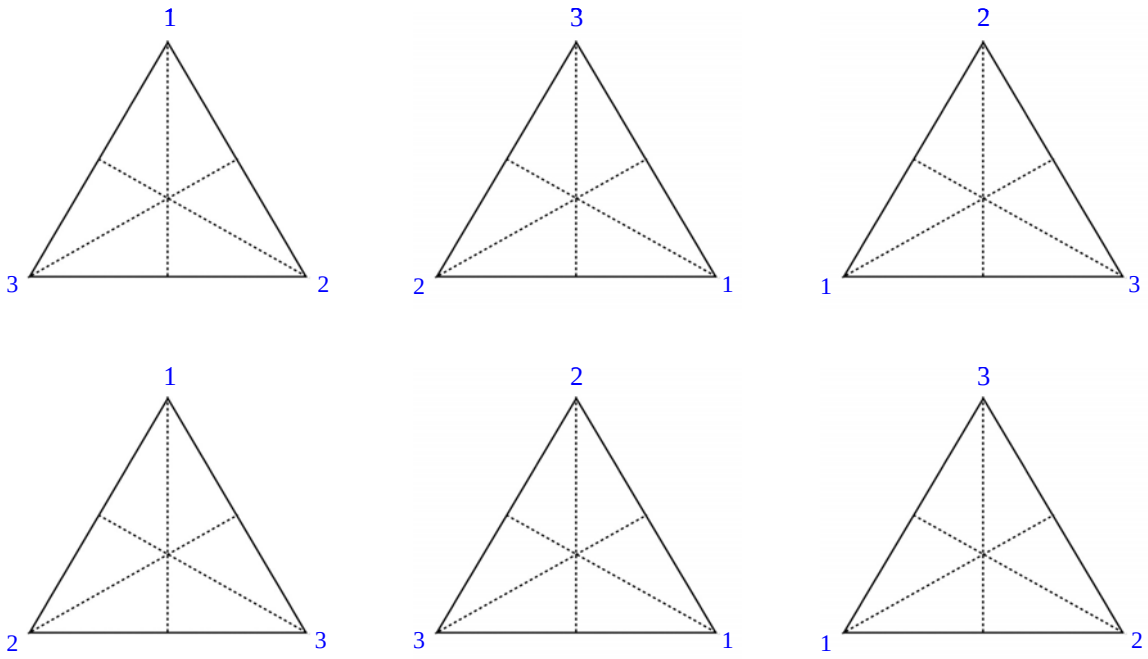
of this permutation before we arrive at the *identity element*. Also, here is some confirmation from GAP.

```
gap> a:=(1,2,3,4,5,6);
(1,2,3,4,5,6)

gap> g:=Group(a);
Group([ (1,2,3,4,5,6) ])

gap> Size(g);
6

gap> IsCyclic(g);
true

gap> a:=(1,2)*(3,4,5);
(1,2)(3,4,5)

gap> g:=Group(a);
Group([ (1,2)(3,4,5) ])

gap> Size(g);
6

gap> IsCyclic(g);
true
```

DIHEDRAL GROUPS

There are a few basic types of *groups* that we need to be familiar with. The first type, *cyclic groups*, we've already talked about, and we've seen that every *cyclic group* is generated by a single element. And in many ways, *cyclic groups* or *cycles* are the building blocks from which all *groups* are made. The next class of *groups* we want to learn about are the *dihedral groups*. These are the *groups* related to the symmetry of a regular polygon (i.e. a polygon such that all the sides have the same length), and they are pretty simple.

The word "*dihedral*" basically means "*two faces*," and this term comes from the fact that when we take a regular polygon, the *group* corresponding to the symmetry of that regular polygon consists of all the rotations about its center and all reflections about axes of symmetry that "flip" the top and bottom faces while leaving the orientation of the polygon appearing unchanged. We've already looked at, for example, rotations through multiples of $120°$ for an equilateral triangle, but if we add to this reflections across axes of symmetry, then six possible orientations are possible. And by labeling the vertices, we can easily display each possible orientation that results from a rotation, a flip, or a combination of both.



To generate the *group* corresponding to the symmetries in this triangle, we rotate the triangle through angles that are integer multiples of $120°$, and we do reflections about each of the three axes of symmetry. The result is what is called the *dihedral group* D_3, and notice that the subscript of three refers to the number of sides in our regular polygon, and the order or number of elements of D_3 is $|D_3| = 2 \cdot 3 = 6$. In general, every *dihedral group* is generated this way. That is, by looking at the permutations of the corner points that can be created either through rotations or reflections about axes of symmetry, and if our regular polygon has *n* sides, then $|D_n| = 2n$. Furthermore, it can be shown that every *dihedral group* can be generated by combining the rotations with a flip about a single axis of symmetry. So, for example, let's do this with our equilateral triangle. Let *e* be the identity (no rotations or flips), let *r* be a clockwise rotation through an angle of $120°$, and let *f* be the flip about the vertical axis. Then we can write the elements of D_3 as follows, and as usual, we do all multiplication from left to right, though remember that many others do it from right to left. Hence, be prepared to switch when necessary!

$e = (\ )$

$r = (1,2,3)$

$r^2 = (1,3,2)$

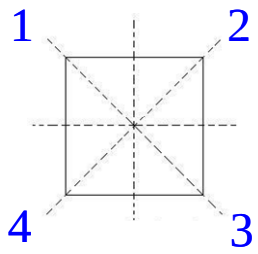
$f = (2,3)$

$fr = (2,3)(1,2,3) = (1,2)$

$fr^2 = (2,3)(1,3,2) = (1,3)$

Notice, too, that $rf = (1,2,3)(2,3) = (1,3) = fr^2$ and $r^2 f = (1,3,2)(2,3) = (1,2) = fr$. In other words, $rf = fr^2$ and $r^2 f = fr$. We might also add to this list that $r^3 = e = f^2$, and equations such as these are often referred to as ***relations*** within a *group*. One way of specifying a *group* is by giving not only a list of elements that generate the *group* through the various products that can be formed, but also a list of equations or *relations* that, along with the *generators*, define that *group*.

Below is a square with the corner vertices labeled, and we can easily list all the elements in the *dihedral group* D_4 in terms of combinations of clockwise rotations through angles of $90°$ and flips about the vertical axis. And we can represent each *group* element as a permutation of the vertices. Notice that the *group* generated by these movements has order $|D_4| = 2 \cdot 4 = 8$.



$e = (\ )$

$r = (1,2,3,4)$

$r^2 = (1,3)(2,4)$

$r^3 = (1,4,3,2)$

$f = (1,2)(3,4)$

$fr = (1,2)(3,4)(1,2,3,4) = (1,3)$

$fr^2 = (1,2)(3,4)(1,3)(2,4) = (1,4)(2,3)$

$fr^3 = (1,2)(3,4)(1,4,3,2) = (2,4)$

Notice also that,

$rf = (1,2,3,4)(1,2)(3,4) = (2,4) = fr^3$

$r^2 f = (1,3)(2,4)(1,2)(3,4) = (1,4)(3,2) = fr^2$

$r^3 f = (1,4,3,2)(1,2)(3,4) = (1,3) = fr$

Hence, we have the following *relations* in this group.

$r^4 = e$

$f^2 = e$

$rf = fr^3$

$r^2 f = fr^2$

$r^3 f = fr$

Additionally, below is a multiplication table for D_4 generated by GAP. You might need a magnifying glass!

*	()	(2,4)	(1,2)(3,4)	(1,2,3,4)	(1,3)	(1,3)(2,4)	(1,4,3,2)	(1,4)(2,3)
()	()	(2,4)	(1,2)(3,4)	(1,2,3,4)	(1,3)	(1,3)(2,4)	(1,4,3,2)	(1,4)(2,3)
(2,4)	(2,4)	()	(1,2,3,4)	(1,2)(3,4)	(1,3)(2,4)	(1,3)	(1,4)(2,3)	(1,4,3,2)
(1,2)(3,4)	(1,2)(3,4)	(1,4,3,2)	()	(1,3)	(1,2,3,4)	(1,4)(2,3)	(2,4)	(1,3)(2,4)
(1,2,3,4)	(1,2,3,4)	(1,4)(2,3)	(2,4)	(1,3)(2,4)	(1,2)(3,4)	(1,4,3,2)	()	(1,3)
(1,3)	(1,3)	(1,3)(2,4)	(1,4,3,2)	(1,4)(2,3)	()	(2,4)	(1,2)(3,4)	(1,2,3,4)
(1,3)(2,4)	(1,3)(2,4)	(1,3)	(1,4)(2,3)	(1,4,3,2)	(2,4)	()	(1,2,3,4)	(1,2)(3,4)
(1,4,3,2)	(1,4,3,2)	(1,2)(3,4)	(1,3)	()	(1,4)(2,3)	(1,2,3,4)	(1,3)(2,4)	(2,4)
(1,4)(2,3)	(1,4)(2,3)	(1,2,3,4)	(1,3)(2,4)	(2,4)	(1,4,3,2)	(1,2)(3,4)	(1,3)	()

Recall now that since $|D_4| = 2 \cdot 4 = 8$, every *subgroup* of D_4 must have an order that is a divisor of 8, and hence, the only possible orders for *subgroups* are 1, 2, 4, or 8. As it turns out, D_4 has 10 *subgroups*, and since D_4 has 8 elements, that means that we can generate eight *cyclic groups* from those elements. However, as we'll see, some of those *cyclic subgroups* are the same. Also, another *subgroup* is D_4, the entire *group*, which, in this case, is not *cyclic*. We can list the *cyclic subgroups* generated by the eight elements as follows.

$$\langle e \rangle = \langle (\ ) \rangle = \{(\ )\}$$

$$\langle r \rangle = \langle (1,2,3,4) \rangle = \{(\ ), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$$

$$\langle r^2 \rangle = \langle (1,3)(2,4) \rangle = \{(\ ), (1,3)(2,4)\}$$

$$\langle r^3 \rangle = \langle (1,4,3,2) \rangle = \{(\ ), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} = \langle r \rangle$$

$$\langle f \rangle = \langle (1,2)(3,4) \rangle = \{(\ ), (1,2)(3,4)\}$$

$$\langle fr \rangle = \langle (1,3) \rangle = \{(\ ), (1,3)\}$$

$$\langle fr^2 \rangle = \langle (1,4)(2,3) \rangle = \{(\ ), (1,4)(2,3)\}$$

$$\langle fr^3 \rangle = \langle (2,4) \rangle = \{(\ ), (2,4)\}$$

Additionally,

$$D_4 = \langle f, r \rangle = \langle (1,2)(3,4), (1,2,3,4) \rangle$$
$$= \{(\ ), (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,2)(3,4), (1,3), (1,4)(2,3), (2,4)\}$$

Since $\langle r \rangle = \{(\ ), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} = \langle r^3 \rangle$, this list of *cyclic groups* plus D_4 gives us only eight distinct *subgroups*, and so we still need to find two more. The two additional groups are,

$$\langle f, fr^2 \rangle = \langle (1,2)(3,4), (1,4)(2,3) \rangle = \{(\ ), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

$$\left\langle r^2,\, fr \right\rangle = \left\langle (1,3)(2,4),(1,3) \right\rangle = \left\{ (\ ),(2,4),(1,3),(1,3)(2,4) \right\}$$

Again, notice that all of these *subgroups* have orders which divide 8, the order of D_4.

SYMMETRIC GROUPS

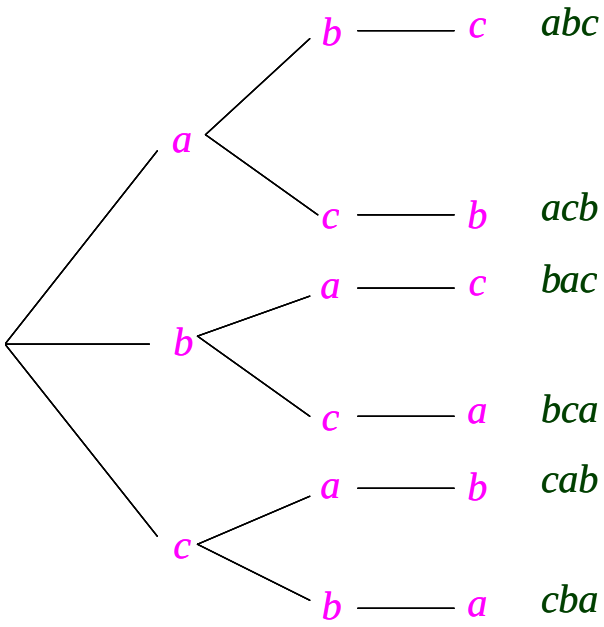
So far we've talked about two main classes of *groups* – *cyclic groups* which can be generated by a single element, and *dihedral groups* which arise from the rotational and mirror symmetry of regular polygons. Now we want to learn about a third class of *groups*, the *symmetric groups*.

The *symmetric group* S_n is essentially the *group* of all permutations that can be made of a set of *n* objects. There are a couple of things, though, that we should realize at the start. First, this is yet another example of a *group acting on a set*. Our underlying set *X* is a set containing *n* objects, and our *group* S_n is the *group* of all permutations we can make of those *n* objects. For example, if $X = \{a,b,c\}$, then the group S_3 represents the number of permutations we can make of these three letters. In this case, if $(a,b,c) \in S_3$, then we'll interpret that permutation as meaning the letter *a* becomes *b*, the letter *b* changes to *c*, and the letter *c* becomes *a*. This permutation would, thus, change abc to bca.

A question we want to ask now, however, is how many elements are in a *group* like S_n? Fortunately, this is easy to answer. Just consider S_3 *acting on* $X = \{a,b,c\}$. If we want to count up how many different permutations there are of the three letters *a*, *b*, and *c*, then we just need to think about how we would construct a single permutation. To do this we need to pick a first letter and then a second letter and then the third letter. However, when we start, we have 3 choices for the first letter, and then only 2 choices left for the second letter, and then just 1 choice for the third letter. Thus, the number of distinct permutations we can make from these three letters is $3 \cdot 2 \cdot 1 = 6$. Furthermore, we can easily list all six permutations.

$$abc \quad acb \quad bac \quad bca \quad cab \quad cba$$

Additionally, we have a special notation for a product like $3\cdot 2\cdot 1$. We call it "3 factorial," and we write it as $3!=3\cdot 2\cdot 1$. Also, the tree diagram below provides a good visual explanation as to why the number of permutations you can make of three objects is equal to $3!=3\cdot 2\cdot 1=6$.



You might recall that D_3, the *group* of rotational and mirror symmetries of an equilateral triangle, also contains six elements. Since we can think of the rotations and reflections in D_3 as creating permutations of the three vertices and since the number of permutations in D_3 is the same as the total number of possible permutations of three objects, it must follow that D_3 is *isomorphic* to S_3. Thus, D_3 and S_3 are essentially the same *group* expressed through different notations, and in mathematics we denote the fact that they are *isomorphic* by writing $D_3 \cong S_3$.

$$D_3 \cong S_3 = \{(),(1,2,3),(1,3,2),(1,2),(2,3),(1,3)\}$$

Since $D_3 \cong S_3$, an obvious question to ask is are *symmetric groups* always basically the same as the *dihedral groups*? Well, the answer is no, and all we have to do to see that is to determine the size of S_4, the *group* of permutations of 4 objects. Let's let our set of objects be $X = \{1,2,3,4\}$, and once again let's think about how many permutations we can make of these four objects. If we are constructing a single permutation, then we have 4 choices for the first number, 3 choices for the next one, 2 choices for the third number, and only 1 choice left for the last number. Hence, the number of permutations we can make of four objects is $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$, and, thus, $|S_4| = 24$. However, since $|D_4| = 8$, it should be clear that D_4 is not *isomorphic* to S_4. Also, since the elements of both *groups* represent permutations of four objects, we can consider D_4 to be a *subgroup* of S_4. And more generally, we always have that $|S_n| = n!$, and D_n is always a subgroup of S_n.

Now let's examine something rather interesting. First, let's consider the following three permutations - $(1,2,3), (1,4), \text{ and } (5,6)$. The latter two permutations, $(1,4), \text{ and } (5,6)$, are called ***transpositions*** since each one switches only two elements. We also say that those two particular permutations are ***disjoint*** since they move entirely different elements, and when two permutations are *disjoint*, they commute with one another. In other words, $(1,4)(5,6) = (5,6)(1,4)$. On the other hand, $(1,2,3) \text{ and } (1,4)$ are not *disjoint* and they do not commute with one another since when we multiply left to right, $(1,2,3)(1,4) = (1,2,3,4)$, but $(1,4)(1,2,3) = (1,4,2,3)$.

Now for the good part. Every permutation can be written as a product of *transpositions*, and there's an easy way to do it. We'll illustrate with the permutation $(1,2,3)$ from S_3. All you have to do is write $(1,2,3) = (1,2)(1,3)$. And now there are two things to notice. First, the *transpositions* on the right are not *disjoint*, and second, we have an even number of *transpositions*. In general, we'll

call a permutation an *even permutation* if it can be written as the product of an even number of *transpositions*, and we'll call a permutation an *odd permutation* if it can be written as an odd number of *transpositions* using the method indicated above. Notice that since we can often write the identity as a product of two *tranpositions* such as $( ) = (1,2)(1,2)$, we will also think of the identity as being an *even permutation*. By the way, there exists a theorem that says that if you can write a permutation as a product of *transpositions* in more than one way, then all those various ways will contain either an even number of *transpositions* or an odd number of *transpositions*. And now what is quite remarkable is that the set of all *even permutations* in S_n forms a *subgroup* of S_n that we call the *alternating group*, A_n. To verify that this is a *subgroup*, it suffices to show that the product of two *even permutations* is even. The reason this is all you need to show is because (1) we get the associative law for free since we're already working within a group, and (2) if your group is finite, then if we pick any *even permutation* and start multiplying it by itself over and over again, we will eventually begin repeating values. In particular, before you repeat your original value, you will get a product that is equal to the identity, and that means that the product before that one is the inverse of your *even permutation*. And now, it should be obvious that the product of any two *even permutations* is an *even permutation* since if you multiply an even number of *transpositions* by an even number of *transpositions*, you still have an even number of *transpositions*. Thus, the set of *even permutations* is closed under multiplication, and for any *finite group*, closure under multiplication is all you need to verify to show that some subset of the *group* forms a *subgroup*. Here now are the elements in the *alternating group* A_3.

$$A_3 = \{(), (1,2,3) = (1,2)(1,3), (1,3,2) = (1,3)(1,2)\}$$

Notice that this *subgroup* contains 3 elements, and that is half of the 6 elements in S_3. That is no accident. In any *symmetric group* S_n with $n \geq 2$, half of the

elements will be *even permutations* and half will be odd. Thus, it is always true, for $n \geq 2$, that $\frac{|S_n|}{|A_n|} = 2$.

And finally, one important bit of information in closing is that $D_3 \cong S_3$ is the smallest example one can find of a *nonabelian group*. In other words, $|D_3| = |S_3| = 6$, and any group of smaller order will automatically be *abelian*!

ALTERNATING GROUPS

We'll now examine something I find rather interesting. First, let's consider the following three permutations - $(1,2,3),(1,4),\text{ and }(5,6)$. The latter two permutations, $(1,4),\text{ and }(5,6)$, are called ***transpositions*** since each one switches only two elements. We also say that those two particular permutations are ***disjoint*** since they move entirely different elements, and when two permutations are *disjoint*, they commute with one another. In other words, $(1,4)(5,6)=(5,6)(1,4)$. On the other hand, $(1,2,3)\text{ and }(1,4)$ are not *disjoint* and they do not commute with one another since when we multiply left to right, $(1,2,3)(1,4)=(1,2,3,4)$, but $(1,4)(1,2,3)=(1,4,2,3)$.

Now for the good part. Every permutation can be written as a product of *transpositions*, and there's an easy way to do it. We'll illustrate with the permutation $(1,2,3)$ from S_3. All you have to do is write $(1,2,3)=(1,2)(1,3)$. And now there are two things to notice. First, the *transpositions* on the right are not *disjoint*, and second, we have an even number of *transpositions*. In general, we'll call a permutation an *even permutation* if it can be written as the product of an even number of *transpositions*, and we'll call a permutation an *odd permutation* if it can be written as an odd number of *transpositions* using the method indicated above. Notice that since we can often write the identity as a product of two *tranpositions* such as $(\ )=(1,2)(1,2)$, we will also think of the identity as being an *even permutation*. By the way, there exists a theorem that says that if you can write a permutation as a product of *transpositions* in more than one way, then all those various ways will contain either an even number of *transpositions* or an odd number of *transpositions*. And now what is quite remarkable is that the set of all *even permutations* in S_n forms a *subgroup* of S_n that we call the *alternating group*, A_n. To verify that this is a *subgroup*, it suffices to show that the product of

two *even permutations* is even. The reason this is all you need to show is because (1) we get the associative law for free since we're already working within a group, and (2) if your group is finite, then if we pick any *even permutation* and start multiplying it by itself over and over again, we will eventually begin repeating values. In particular, before you repeat your original value, you will get a product that is equal to the identity, and that means that the product before that one is the inverse of your *even permutation*. And now, it should be obvious that the product of any two *even permutations* is an *even permutation* since if you multiply an even number of *transpositions* by an even number of *transpositions*, you still have an even number of *transpositions*. Thus, the set of *even permutations* is closed under multiplication, and for any *finite group*, closure under multiplication is all you need to verify to show that some subset of the *group* forms a *subgroup*. Here now are the elements in the *alternating group* A_3.

$$A_3 = \{(), (1,2,3) = (1,2)(1,3), (1,3,2) = (1,3)(1,2)\}$$

Notice that this *subgroup* contains 3 elements, and that is half of the 6 elements in S_3. That is no accident. In any *symmetric group* S_n with $n \geq 2$, half of the elements will be *even permutations* and half will be odd. Thus, it is always true, for $n \geq 2$, that $\frac{|S_n|}{|A_n|} = 2$.

And finally, one important bit of information in closing is that $D_3 \cong S_3$ is the smallest example one can find of a *nonabelian group*. In other words, $|D_3| = |S_3| = 6$, and any group of smaller order will automatically be *abelian*!

DIRECT PRODUCTS

So far we've talked about *cyclic groups*, *dihedral groups*, and *symmetric groups*. Now we're going to learn a standard way to construct new *groups* from old that's called a *direct product of groups*. The idea behind it is very simple. We simply take two *groups* and form coordinate pairs where the first element comes from one *group* and the second element comes from the other *group*. Next, we add or multiply *group* elements by doing it coordinatewise using the addition or multiplication for each individual *group*.

As an example, let's consider the *direct product* of the *integers modulo* 2 with the *integers modulo* 2. This is essentially the same as the direct product of the *cyclic group* of order two with itself, but in the *integers modulo* 2 we tend to specify our operation by addition rather than multiplication. Thus, recall that if $\mathbb{Z}_2 = \{0,1\}$, then addition is defined such that $1+1=0$. Hence, we get the following addition table.

+	**0**	**1**
0	0	1
1	1	0

The general notation for the *direct product* of $\mathbb{Z}_2$ with $\mathbb{Z}_2$ is $\mathbb{Z}_2 \times \mathbb{Z}_2$, but when both groups are *abelian*, i.e. *comnmutative*, you also see it written as $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. We'll stick with the former notation, though. Also, as a set, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is going to consist of all ordered pairs we can form where the first element comes from $\mathbb{Z}_2$ and the second element also comes from $\mathbb{Z}_2$. That's going to give us four ordered pairs in all. In the particular, the elements in this *direct product* will be $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0,),(1,0),(0,1),(1,1)\}$. And the multiplication (addition) table for this group is as follows.

+	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

Notice that each non-identity element in this *group* has order 2. That means that when you multiply (add) any element by itself, you get back the identity which in this case is $(0,0)$. Another way to say that is that each non-identity element generates a *cyclic subgroup* of order 2. Also, notice that based upon the mirror symmetry with respect to the diagonal in our multiplication table, we can definitely say that this *group* is *abelian*. However, since this *group* has four elements and since none of them generate the whole *group*, this *group* is not *cyclic*. In fact, this is the smallest example one can find of an *abelian group* that is not *cyclic*. And finally, this group has a special name in mathematics. It is known as the *Klein 4-group*. Also, if we replace (0,0) by *e*, (1,0) by *a*, 0,1) by *b*, and (1,1) by *c*, then we can rewrite the multiplication table for our *Klein 4-group* as follows.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Now comes the tricky part (or the good part, as I say). Below are the two multiplication tables we've constructed, and on the one hand, since they use different notations, we could say that they are two different *groups*. But on the other hand, the multiplication tables suggest that the two *groups* have essentially the same structure. In other words, we can establish a correspondence between the elements in such a way that addition in the first table corresponds to multiplication in the second table. For example, with *a* corresponding to (1,0), *b* corresponding to (0,1), and *c* corresponding to (1,1), we can see from the tables that just as $(1,0)+(0,1)=(1,1)$, so does $a*b=c$. Hence, our two *groups* are essentially the same, but expressed using different notations. Recall that when

this happens, we say that the two *groups* are *isomorphic*. That is just a nice word that means "*equal shape*." Additionally, we can use the multiplication tables below to verify that our correspondence or coding works for other elements, too. Using our coding, we'll always have that a sum of elements in the first group corresponds to a product of elements in the second group.

+	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

We can also give a real-world example of a *Klein 4-group*. Below is a picture of two light switches.

Clearly, we can flip each switch independently of the other. Thus, let's define some operations as follows:

e means that you flip no switches
f_1 means that you flip the first switch
f_2 means that you flip the second switch
$f_1 f_2$ means that you flip both switches

These operations will now generate the following multiplication table for a *group*. By studying the multiplication table, you can see that this *group* is *isomorphic* to the *Klein 4-group*.

*	**e**	**f_1**	**f_2**	**f_1f_2**
e	e	f_1	f_2	f_1f_2
f_1	f_1	e	f_1f_2	f_2
f_2	f_2	f_1f_2	e	f_1
f_1f_2	f_1f_2	f_2	f_1	e

Here are another couple of examples of *direct products*. If we look at $\mathbb{Z}_2 \times \mathbb{Z}_3$, then we are going to get a group with 6 elements since the first group has 2 elements and the second group has 3. Specifically, $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0,),(1,0),(0,1),(0,2),(1,1),(1,2)\}$. Furthermore, if you do *addition modulo* 2 with the first coordinate and *addition modulo* 3 with the second coordinate, then you can verify that (1,1) generates the *group*. Hence, $\mathbb{Z}_2 \times \mathbb{Z}_3$ is *isomorphic* to C_6, the *cyclic group* of order 6, and we usually denote this by writing $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong C_6$. This result also illustrates an important theorem. Namely, if a *cyclic group* has order *mn* where *m* and *n* are relatively prime (in other words, their only common divisor is 1), then our *cyclic group* is *isomorphic* to $\mathbb{Z}_m \times \mathbb{Z}_n$.

We can also form the *direct product* of more than two *groups* just by extending our earlier definitions. Thus, for example, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 8 elements, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0,0),(1,0,0),(0,1,0),(0,0,1),(1,1,0),(1,0,1),(0,1,1),(1,1,1)\}$. Notice, again, that every non-identity element in this *direct product* has order 2, and so it is not a *cyclic group*. However, it is *abelian*.

But if you want to construct a *direct product* that is not *abelian*, then all you have to do is throw in a factor that is *nonabelian* such as is the case with $\mathbb{Z}_2 \times D_3$. Also, notice that we can consider both $\mathbb{Z}_2$ and D_3 not only as *subgroups* of $\mathbb{Z}_2 \times D_3$ but also as *normal subgroups*, even though, technically, we would write the elements of these *groups* in this case as $\mathbb{Z}_2 = \{(0,0),(1,0)\}$ and $D_3 = \{(0,0),(0,r),(0,r^2),(0,f_1),(0,f_2),(0,f_3)\}$. Furthermore, it's not that difficult to see that the elements of $\mathbb{Z}_2$ and D_3 generate the *group* $\mathbb{Z}_2 \times D_3$ by multiplying elements from the two *subgroups* together, and that the only element $\mathbb{Z}_2$ and D_3 have in common is the identity element, $\mathbb{Z}_2 \cap D_3 = (0,0)$. There is a theorem in *group theory* that says that whenever something like this happens, that is whenever we have a *group G* with two *normal subgroups M* and *N* such that $MN = G$ and $M \cap N = e$, then we can think of *G* as the *direct product* of *M* and *N*, $G \cong M \times N$.

And as a final note, you've probably noticed that the notation for an element of a *direct product* (for example, $(1,2) \in \mathbb{Z}_2 \times \mathbb{Z}_3$) looks just like what we write for a permutation expressed in *cycle notation*. Consequently, you will only know from the context whether we are talking about a permutation in *cycle notation* or an element of a *direct product* expressed in *coordinate notation*.

SEMIDIRECT PRODUCTS

At this point we've learned about three very important classes of *groups*: *cyclic groups*, *dihedral groups*, and *symmetric groups*. We've also leaned in the past about *factor* or *quotient groups*, and we've more recently learned how to construct new *groups* from old by forming *direct products* of *groups*. We've also pointed out that if a *group G* has two *normal subgroups M* and *N* such that $MN = G$ and $M \cap N = e$, then we can think of *G* as the *direct product* of *M* and *N*. What we really mean by this is that *G* is *isomorphic* to $M \times N$, and we'll often just write this as an equality, $G = M \times N$. However, let's now suppose that we have two *subgroups M* and *N* of a *group G* such that $MN = G$ and $M \cap N = e$, but only *M* is a *normal subgroup* of *G,* $M \lhd G$. In this case, we call *G* a *semidirect product* of *M* and *N*, and we write $G = M \rtimes N$ where we put the *normal subgroup* first.

If you come across a *semidirect product*, then nine times out of ten it will be a *dihedral group*. In particular, while not every *semidirect product* is a *dihedral group*, every *dihedral group* is a *semidirect product* of its *rotation subgroup* with the *subgroup* generated by a *flip* about one of its axes of symmetry. Thus, for example, we think of $D_3 = R_3 \rtimes F$ and $D_4 = R_4 \rtimes F$, where R_n represents the *subgroup* generated by *n* rotations, and *F* represents the *subgroup* generated by a flip about an axis of symmetry. Furthermore, *semidirect products* are always *nonabelian.*

THE QUATERNION GROUP

The *quaternion group* is a very special *group* that consists of eight elements. It can be generated by the permutations $(1,2,5,6)(3,8,7,4)$ and $(1,4,5,8)(2,7,6,3)$ acting on the set $\{1,2,3,4,5,6,7,8\}$. What makes the *quaternion group* special is that it doesn't fit into any of the convenient categories that many of the other groups you explore will likely fit into. For example, it's a *nonabelian group* and yet all of its *subgroups* are *normal*. In fact, it's the smallest *nonabelian group* to have this property. In particular, for a *nonabelian group* such ubiquitous normality is quite abnormal! The *quaternion group* is also not a *cyclic, dihedral, symmetric,* or *alternating group*, and it's not a *direct product* or *semidirect product* of simpler *groups*. In GAP we can create the *quaternion group* in at least two different ways. One is by using the generators above to create the group, and the other is to use the special "*QuaternionGroup*" command. Notice, though, that the version of the *quaternion group* generated by this command uses different generators than the ones given above. Also, the other permutations in the *group* also look different, but, nonetheless, the two *groups* are *isomorphic* to one another. Recall that that means that their multiplication tables are essentially the same except for how the elements are labled.

```
gap> a:=(1,2,5,6)*(3,8,7,4);
(1,2,5,6)(3,8,7,4)

gap> b:=(1,4,5,8)*(2,7,6,3);
(1,4,5,8)(2,7,6,3)

gap> q:=Group(a,b);
Group([ (1,2,5,6)(3,8,7,4), (1,4,5,8)(2,7,6,3) ])

gap> Size(q);
8
gap> Elements(q);
[ (), (1,2,5,6)(3,8,7,4), (1,3,5,7)(2,4,6,8), (1,4,5,8)(2,7,6,3),
(1,5)(2,6)(3,7)(4,8), (1,6,5,2)(3,4,7,8),
  (1,7,5,3)(2,8,6,4), (1,8,5,4)(2,3,6,7) ]

gap> q:=QuaternionGroup(IsPermGroup,8);
Group([ (1,5,3,7)(2,8,4,6), (1,2,3,4)(5,6,7,8) ])

gap> Size(q);
8
```

```
gap> Elements(q);
[ (), (1,2,3,4)(5,6,7,8), (1,3)(2,4)(5,7)(6,8), (1,4,3,2)(5,8,7,6),
(1,5,3,7)(2,8,4,6), (1,6,3,8)(2,5,4,7),
  (1,7,3,5)(2,6,4,8), (1,8,3,6)(2,7,4,5) ]
```

GENERATORS

We've talked before about *generators* for a *group*, and this refers to a set of elements in the *group* whose finite products with one another give us back or "generate" the entire *group*. Now clearly the set of all elements in a *group* will generate that *group*, but usually we are looking for something smaller. For example, one requirement that we generally want for our set of *generators* is that they are essentially independent of one another, and by that we mean that if a *group* is generated by elements *a, b,* and *c*, then we don't want to be able to write, for instance, *c* as a finite product of combinations of *a* and *b*. Clearly, if we are able to do that, then we don't need *c* in our set of *generators* since *a* and *b* by themselves could generate *c* and, hence, the entire *group*. Another way to express this condition would be to say that our *generators* are independent of one another if the removal of any one element from our set leaves us with something that can no longer generate the whole *group*. Also, you would think that a set of independent *generators* as described above would guarantee that our set of generators is as small as possible, but that is not necessarily the case. For example, the set $\{(1,2),(3,4,5)\}$ consists of two independent *generators* that generate C_6, a *cyclic group* of order 6, but then again one element sets like $\{(1,2)(3,4,5)\}$ or $\{(1,2,3,4,5,6)\}$ also generate *cyclic groups* of order 6. Hence, knowing that your *generators* are independent from one another doesn't always mean that you've picked the smallest possible set of *generators*.

Most of the time when using GAP, we know some specific *generators* for a *group* because we begin by using those *generators* to construct our *group* as in the example below.

```
gap> a:=(1,2);
(1,2)
```

```
gap> b:=(3,4,5);
(3,4,5)

gap> g:=Group(a,b);
Group([ (1,2), (3,4,5) ])
```

If, however, we have used specific commands, rather than *generators*, in GAP to create a *group*, then it may not be entirely clear what we might use as *generators* for that *group*. In such a case, we can use GAP to apply the command *GeneratorsOfGroup* to find a set of independent *generators.*

```
gap> g:=AlternatingGroup(3);
Alt( [ 1 .. 3 ] )

gap> Size(g);
3
gap> GeneratorsOfGroup(g);
[ (1,2,3) ]


gap> g:=AlternatingGroup(4);
Alt( [ 1 .. 4 ] )

gap> Size(g);
12

gap> GeneratorsOfGroup(g);
[ (1,2,3), (2,3,4) ]
```

HOW TO USE GAP (PART 3)

For both convenience and continuity, we will always include the GAP commands presented in earlier parts of this book in black followed by the new commands which are printed in red.

1. *How can I redisplay the previous command in order to edit it?*

   Press down on the control key and then also press p. In other words, “Ctrl p”.

2. *If the program gets in a loop and shows you the prompt “brk>” instead of “gap>”, how can I exit the loop?*

   Press down on the control key and then also press d. In other words, “Ctrl d”.

3. *How can I exit the program?*

   Either click on the “close” box for the window, or type “quit;” and press “Enter.”

4. *How do I find the inverse of a permutation?*

   ```
   gap> a:=(1,2,3,4);
   (1,2,3,4)
   gap> a^-1;
   (1,4,3,2)
   ```

5. *How can I multiply permutations and raise permutations to powers?*

```
gap> (1,2)*(1,2,3);
(1,3)

gap> (1,2,3)^2;
(1,3,2)

gap> (1,2,3)^-1;
(1,3,2)

gap> (1,2,3)^-2;
(1,2,3)

gap> a:=(1,2,3);
(1,2,3)

gap> b:=(1,2);
(1,2)

gap> a*b;
(2,3)

gap> a^2;
(1,3,2)

gap> a^-2;
(1,2,3)

gap> a^3;
()
```

```
gap> a^-3;
()

gap> (a*b)^2;
()

gap> (a*b)^3;
(2,3)
```

6. *How can I create a group from permutations, find the size of the group, and find the elements in the group?*

```
gap> a:=(1,2);
(1,2)

gap> b:=(1,2,3);
(1,2,3)

gap> g1:=Group(a,b);
Group([ (1,2), (1,2,3) ])

gap> Size(g1);
6

gap> Elements(g1);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> g2:=Group([(1,2),(1,2,3)]);
Group([ (1,2), (1,2,3) ])
```

```
gap> g3:=Group((1,2),(2,3,4));
Group([ (1,2), (2,3,4) ])
```

7. *How can I create a cyclic group of order 3?*

```
gap> a:=(1,2,3);
(1,2,3)

gap> g1:=Group(a);
Group([ (1,2,3) ])

gap> Size(g1);
3

gap> Elements(g1);
[ (), (1,2,3), (1,3,2) ]

gap> g2:=Group((1,2,3));
Group([ (1,2,3) ])

gap> g3:=CyclicGroup(IsPermGroup,3);
Group([ (1,2,3) ])
```

8. *How can I create a multiplication table for the cyclic group of order 3 that I just created?*

gap> ShowMultiplicationTable(g1);

```
*         | ()        (1,2,3)    (1,3,2)
--------+--------------------------------
()        | ()        (1,2,3)    (1,3,2)
(1,2,3)   | (1,2,3)   (1,3,2)    ()
(1,3,2)   | (1,3,2)   ()         1,2,3)
```

9. *How do I determine if a group is abelian?*

gap> g1:=Group((1,2,3));
Group([(1,2,3)])

gap> IsAbelian(g1);
true

gap> g2:=Group((1,2),(1,2,3));
Group([(1,2), (1,2,3)])

gap> IsAbelian(g2);
false

10. *What do I type in order to get help for a command like "Elements?"*

gap> ?Elements

11. *How do I find all subgroups of a group?*

```
gap> a:=(1,2,3);
(1,2,3)

gap> b:=(2,3);
(2,3)

gap> g:=Group(a,b);
Group([ (1,2,3), (2,3) ])
```

```
gap> Size(g);
6

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> h:=AllSubgroups(g);
[ Group(()), Group([ (2,3) ]), Group([ (1,2) ]), Group([ (1,3) ]),
Group([ (1,2,3) ]), Group([ (1,2,3), (2,3) ]) ]

gap> List(h,i->Elements(i));
[ [ () ], [ (), (2,3) ], [ (), (1,2) ], [ (), (1,3) ], [ (), (1,2,3),
(1,3,2) ], [ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ] ]

gap> Elements(h[1]);
[ () ]

gap> Elements(h[2]);
[ (), (2,3) ]

gap> Elements(h[3]);
[ (), (1,2) ]

gap> Elements(h[4]);
[ (), (1,3) ]


gap> Elements(h[5]);
[ (), (1,2,3), (1,3,2) ]

gap> Elements(h[6]);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
```

12. *How do I find the subgroup generated by particular permutations?*

```
gap> g:=Group((1,2),(1,2,3));
Group([ (1,2), (1,2,3) ])

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> h:=Subgroup(g,[(1,2)]);
Group([ (1,2) ])

gap> Elements(h);
[ (), (1,2) ]
```

13. *How do I determine if a subgroup is normal?*

```
gap> g:=Group((1,2),(1,2,3));
Group([ (1,2), (1,2,3) ])

gap> h1:=Group((1,2));
Group([ (1,2) ])
gap> IsNormal(g,h1);

gap> h2:=Group((1,2,3));
Group([ (1,2,3) ])
```

```
gap> IsNormal(g,h2);
true
```

14. *How do I find all normal subgroups of a group?*

```
gap> g:=Group((1,2),(1,2,3));
Group([ (1,2), (1,2,3) ])

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> n:=NormalSubgroups(g);
[ Group([ (1,2), (1,2,3) ]), Group([ (1,3,2) ]), Group(()) ]

gap> Elements(n[1]);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> Elements(n[2]);
[ (), (1,2,3), (1,3,2) ]

gap> Elements(n[3]);
[ () ]
```

15. *How do I determine if a group is simple?*

```
gap> g:=Group((1,2),(1,2,3));
Group([ (1,2), (1,2,3) ])

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> IsSimple(g);
false


gap> h:=Group((1,2));
Group([ (1,2) ])

gap> Elements(h);
[ (), (1,2) ]

gap> IsSimple(h);
true
```

16. *How do I find the right cosets of a subset H of G?*

```
gap> g:=Group([(1,2,3),(1,2)]);
Group([ (1,2,3), (1,2) ])
```

```
gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> h:=Subgroup(g,[(1,2)]);
Group([ (1,2) ])

gap> Elements(h);
[ (), (1,2) ]

gap> c:=RightCosets(g,h);
[ RightCoset(Group( [ (1,2) ] ),()), RightCoset(Group( [ (1,2) ] ),(1,3,2)),
RightCoset(Group( [ (1,2) ] ),(1,2,3)) ]

gap> List(c,i->Elements(i));
[ [ (), (1,2) ], [ (2,3), (1,3,2) ], [ (1,2,3), (1,3) ] ]
gap> Elements(c[1]);
[ (), (1,2) ]

gap> Elements(c[2]);
[ (2,3), (1,3,2) ]


gap> Elements(c[3]);
[ (1,2,3), (1,3) ]

gap> rc:=RightCoset(h,(1,2,3));
RightCoset(Group([ (1,2) ]),(1,2,3))

gap> Elements(rc);
[ (1,2,3), (1,3) ]

gap> rc:=h*(1,2,3);
RightCoset(Group([ (1,2) ]),(1,2,3))

gap> Elements(rc);
[ (1,2,3), (1,3) ]
```

17. *How can I create a quotient (factor) group?*

```
gap> g:=Group([(1,2,3),(1,2)]);
Group([ (1,2,3), (1,2) ])

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> n:=Group((1,2,3));
Group([ (1,2,3) ])

gap> Elements(n);
[ (), (1,2,3), (1,3,2) ]

gap> IsNormal(g,n);
true

gap> c:=RightCosets(g,n);
[ RightCoset(Group([ (1,2,3) ]),()), RightCoset(Group([ (1,2,3) ]),(2,3)) ]

gap> Elements(c[1]);
[ (), (1,2,3), (1,3,2) ]

gap> Elements(c[2]);
[ (2,3), (1,2), (1,3) ]

gap> f:=FactorGroup(g,n);
Group([ f1 ])
```

```
gap> Elements(f);
[ <identity> of ..., f1 ]

gap> ShowMultiplicationTable(f);
*                 | <identity> of ... f1
------------------+-----------------------------------
<identity> of ... | <identity> of ... f1
f1                | f1                <identity> of ...
```

18. *How do I find the center of a group?*

```
gap> a:=(1,2,3);
(1,2,3)

gap> b:=(2,3);
(2,3)

gap> g:=Group(a,b);
Group([ (1,2,3), (2,3) ])

gap> Center(g);
Group(())

gap> c:=Center(g);
Group(())

gap> Elements(c);
[ () ]


gap> a:=(1,2,3,4);
(1,2,3,4)

gap> b:=(1,3);
(1,3)

gap> g:=Group(a,b);
Group([ (1,2,3,4), (1,3) ])

gap> c:=Center(g);
Group([ (1,3)(2,4) ])

gap> Elements(c);
[ (), (1,3)(2,4) ]
```

19. *How do I find the commutator (derived) subgroup of a group?*

```
gap> a:=(1,2,3);
(1,2,3)

gap> b:=(2,3);
(2,3)

gap> g:=Group(a,b);
Group([ (1,2,3), (2,3) ])

gap> d:=DerivedSubgroup(g);
Group([ (1,3,2) ])
```

```
gap> Elements(d);
[ (), (1,2,3), (1,3,2) ]


gap> a:=(1,2,3,4);
(1,2,3,4)

gap> b:=(1,3);
(1,3)

gap> g:=Group(a,b);
Group([ (1,2,3,4), (1,3) ])

gap> d:=DerivedSubgroup(g);
Group([ (1,3)(2,4) ])

gap> Elements(d);
[ (), (1,3)(2,4) ]
```

20. *How do I find all Sylow p-subgroups for a given group?*

```
gap> a:=(1,2,3);
(1,2,3)

gap> b:=(2,3);
(2,3)

gap> g:=Group(a,b);
Group([ (1,2,3), (2,3) ])

gap> Size(g);
6

gap> FactorsInt(6);
[ 2, 3 ]

gap> sylow2:=SylowSubgroup(g,2);
Group([ (2,3) ])

gap> IsNormal(g,sylow2);
false

gap> c:=ConjugateSubgroups(g,sylow2);
[ Group([ (2,3) ]), Group([ (1,3) ]), Group([ (1,2) ]) ]

gap> Elements(c[1]);
[ (), (2,3) ]

gap> Elements(c[2]);
[ (), (1,3) ]

gap> Elements(c[3]);
[ (), (1,2) ]

gap> sylow3:=SylowSubgroup(g,3);
Group([ (1,2,3) ])

gap> IsNormal(g,sylow3);
true

gap> Elements(sylow3);
[ (), (1,2,3), (1,3,2) ]
```

21. *How can I create the Rubik's cube group using GAP?*

First you need to save the following permutations as a pure text file with the name rubik.txt to your C-drive before you can import it into GAP.

```
r:=(25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24);
l:=(9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35);
u:=(1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19);
d:=(41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40);
f:=(17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11);
b:=(33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27);
```

And now you can read the file into GAP and begin exploring.

```
gap> Read("C:/rubik.txt");

gap> rubik:=Group(r,l,u,d,f,b);
<permutation group with 6 generators>

gap> Size(rubik);
43252003274489856000
```

22. *How can I find the center of the Rubik's cube group?*

```
gap> c:=Center(rubik);
Group([ (2,34)(4,10)(5,26)(7,18)(12,37)(13,20)(15,44)(21,28)(23,42)(29,36)(31,4
5)(39,47) ])

gap> Size(c);
2

gap> Elements(c);
[ (), (2,34)(4,10)(5,26)(7,18)(12,37)(13,20)(15,44)(21,28)(23,42)(29,36)(31,45)
(39,47) ]
```

23. *How can I find the commutator (derived) subgroup of the Rubik's cube group?*

```
gap> d:=DerivedSubgroup(rubik);
<permutation group with 5 generators>

gap> Size(d);
21626001637244928000

gap> IsNormal(rubik,d);
true
```

24. *How can I find the quotient (factor) group of the Rubik's cube group by its commutator (derived) subgroup?*

```
gap> d:=DerivedSubgroup(rubik);
<permutation group of size 21626001637244928000 with 5 generators>
gap> f:=FactorGroup(rubik,d);
Group([ f1 ])

gap> Size(f);
2
```

25. *How can I find some Sylow p-subgroups of the Rubik's cube group?*

```
gap> Read("C:/rubik.txt");

gap> rubik:=Group(r,l,u,d,f,b);
<permutation group with 6 generators>

gap> Size(rubik);
43252003274489856000

gap> FactorsInt(43252003274489856000);
[ 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 5, 5, 5, 7, 7, 11 ]

gap> sylow2:=SylowSubgroup(rubik,2);
<permutation group of size 134217728 with 27 generators>

gap> sylow3:=SylowSubgroup(rubik,3);
<permutation group of size 4782969 with 14 generators>

gap> sylow5:=SylowSubgroup(rubik,5);
<permutation group of size 125 with 3 generators>

gap> sylow7:=SylowSubgroup(rubik,7);
<permutation group of size 49 with 2 generators>

gap> sylow11:=SylowSubgroup(rubik,11);
Group([ (4,36,31,39,42,12,5,21,15,13,7)(10,29,45,47,23,37,26,28,44,20,18) ])

gap> Elements(sylow11);
[ (), (4,5,36,21,31,15,39,13,42,7,12)(10,26,29,28,45,44,47,20,23,18,37),
(4,7,13,15,21,5,12,42,39,31,36)(10,18,20,44,28,26,37,23,47,45,29),
(4,12,7,42,13,39,15,31,21,36,5)(10,37,18,23,20,47,44,45,28,29,26),
(4,13,21,12,39,36,7,15,5,42,31)(10,20,28,37,47,29,18,44,26,23,45),
(4,15,12,31,7,21,42,36,13,5,39)(10,44,37,45,18,28,23,29,20,26,47),
(4,21,39,7,5,31,13,12,36,15,42)(10,28,47,18,26,45,20,37,29,44,23),
(4,31,42,5,15,7,36,39,12,21,13)(10,45,23,26,44,18,29,47,37,28,20),
(4,36,31,39,42,12,5,21,15,13,7)(10,29,45,47,23,37,26,28,44,20,18),
(4,39,5,13,36,42,21,7,31,12,15)(10,47,26,20,29,23,28,18,45,37,44),
(4,42,15,36,12,13,31,5,7,39,21)(10,23,44,29,37,20,45,26,18,47,28) ]

gap> IsNormal(rubik,sylow2);
false

gap> IsNormal(rubik,sylow3);
false


gap> IsNormal(rubik,sylow5);
false

gap> IsNormal(rubik,sylow7);
```

```
false

gap> IsNormal(rubik,sylow11);
false
```

NOTE: All of the *Sylow p-subgroups* found above have *conjugates*, but the sheer size of the *Rubik's cube group* makes it too difficult to pursue them on a typical desktop computer.

26. *How do I determine if a group is cyclic?*

```
gap> a:=(1,2,3)*(4,5,6,7);
(1,2,3)(4,5,6,7)

gap> g:=Group(a);
Group([ (1,2,3)(4,5,6,7) ])

gap> Size(g);
12

gap> IsCyclic(g);
true
```

27. *How do I create a dihedral group with 2n elements for an n-sided regular polygon?*

```
gap> d4:=DihedralGroup(IsPermGroup,8);
Group([ (1,2,3,4), (2,4) ])

gap> Elements(d4);
[ (), (2,4), (1,2)(3,4), (1,2,3,4), (1,3), (1,3)(2,4), (1,4,3,2), (1,4)(2,3) ]
```

28. *How can I express the elements of a dihedral group as rotations and flips rather than as permutations?*

```
gap> d3:=DihedralGroup(6);
<pc group of size 6 with 2 generators>

gap> Elements(d3);
[ <identity> of ..., f1, f2, f1*f2, f2^2, f1*f2^2 ]

gap> ShowMultiplicationTable(d3);
*               | <identity> of ... f1              f2              f1*f2           f2^2            f1*f2^2
----------------+-------------------------------------------------------------------------------------------\
---------
<identity> of ... | <identity> of ... f1              f2              f1*f2           f2^2            f1*f2^2
f1              | f1              <identity> of ... f1*f2           f2              f1*f2^2         f2^2
f2              | f2              f1*f2^2           f2^2            f1              <identity> of ... f1*f2
f1*f2           | f1*f2           f2^2              f1*f2^2         <identity> of ... f1              f2
f2^2            | f2^2            f1*f2             <identity> of ... f1*f2^2         f2              f1
f1*f2^2         | f1*f2^2         f2                f1              f2^2            f1*f2
<identity> of ...
```

29. *How do I create a symmetric group of degree n with n! elements?*

```
gap> s4:=SymmetricGroup(4);
Sym( [ 1 .. 4 ] )

gap> Size(s4);
24

gap> Elements(s4);
[ (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2), (1,2)(3,4), (1,2,3),
(1,2,3,4), (1,2,4,3), (1,2,4), (1,3,2),
  (1,3,4,2), (1,3), (1,3,4), (1,3)(2,4), (1,3,2,4), (1,4,3,2), (1,4,2), (1,4,3),
(1,4), (1,4,2,3), (1,4)(2,3) ]
```

30. *How do I create an alternating group of degree n with* $\frac{n!}{2}$ *elements?*

```
gap> a4:=AlternatingGroup(4);
Alt( [ 1 .. 4 ] )

gap> Size(a4);
12
gap> Elements(a4);
[ (), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4), (1,3,2), (1,3,4),
(1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3) ]
```

31. *How do I create a direct product of two or more groups?*

```
gap> g1:=Group((1,2,3));
Group([ (1,2,3) ])

gap> g2:=Group((4,5));
Group([ (4,5) ])

gap> dp:=DirectProduct(g1,g2);
Group([ (1,2,3), (4,5) ])

gap> Size(dp);
6
gap> Elements(dp);
[ (), (4,5), (1,2,3), (1,2,3)(4,5), (1,3,2), (1,3,2)(4,5) ]

gap> ShowMultiplicationTable(dp);
*           | ()          (4,5)       (1,2,3)     (1,2,3)(4,5) (1,3,2)
(1,3,2)(4,5)
------------+-----------------------------------------------------------------
---
()          | ()          (4,5)       (1,2,3)     (1,2,3)(4,5) (1,3,2)
(1,3,2)(4,5)
(4,5)       | (4,5)       ()          (1,2,3)(4,5) (1,2,3)      (1,3,2)(4,5) (1,3,2)
(1,2,3)     | (1,2,3)     (1,2,3)(4,5) (1,3,2)      (1,3,2)(4,5) ()           (4,5)
(1,2,3)(4,5) | (1,2,3)(4,5) (1,2,3)     (1,3,2)(4,5) (1,3,2)      (4,5)        ()
(1,3,2)     | (1,3,2)     (1,3,2)(4,5) ()          (4,5)        (1,2,3)
(1,2,3)(4,5)
(1,3,2)(4,5) | (1,3,2)(4,5) (1,3,2)     (4,5)       ()           (1,2,3)(4,5) (1,2,3)
```

32. *How can I create the Quaternion group?*

```
gap> a:=(1,2,5,6)*(3,8,7,4);
(1,2,5,6)(3,8,7,4)

gap> b:=(1,4,5,8)*(2,7,6,3);
(1,4,5,8)(2,7,6,3)

gap> q:=Group(a,b);
Group([ (1,2,5,6)(3,8,7,4), (1,4,5,8)(2,7,6,3) ])

gap> Size(q);
8

gap> IsAbelian(q);
false

gap> Elements(q);
[ (), (1,2,5,6)(3,8,7,4), (1,3,5,7)(2,4,6,8), (1,4,5,8)(2,7,6,3),
(1,5)(2,6)(3,7)(4,8), (1,6,5,2)(3,4,7,8),
  (1,7,5,3)(2,8,6,4), (1,8,5,4)(2,3,6,7) ]

gap> q:=QuaternionGroup(IsPermGroup,8);
Group([ (1,5,3,7)(2,8,4,6), (1,2,3,4)(5,6,7,8) ])

gap> Size(q);
8


gap> IsAbelian(q);
false

gap> Elements(q);
[ (), (1,2,3,4)(5,6,7,8), (1,3)(2,4)(5,7)(6,8), (1,4,3,2)(5,8,7,6),
(1,5,3,7)(2,8,4,6), (1,6,3,8)(2,5,4,7),
  (1,7,3,5)(2,6,4,8), (1,8,3,6)(2,7,4,5) ]
```

33. *How can I find a set of independent generators for a group?*

```
gap> c6:=CyclicGroup(IsPermGroup,6);
Group([ (1,2,3,4,5,6) ])

gap> Size(c6);
6

gap> GeneratorsOfGroup(c6);
[ (1,2,3,4,5,6) ]


gap> d4:=DihedralGroup(IsPermGroup,8);
Group([ (1,2,3,4), (2,4) ])

gap> Size(d4);
8

gap> GeneratorsOfGroup(d4);
[ (1,2,3,4), (2,4) ]


gap> s5:=SymmetricGroup(5);
Sym( [ 1 .. 5 ] )
```

```
gap> Size(s5);
120

gap> GeneratorsOfGroup(s5);
[ (1,2,3,4,5), (1,2) ]


gap> a5:=AlternatingGroup(5);
Alt( [ 1 .. 5 ] )

gap> Size(a5);
60

gap> GeneratorsOfGroup(a5);
[ (1,2,3,4,5), (3,4,5) ]


gap> q:=QuaternionGroup(IsPermGroup,8);
Group([ (1,5,3,7)(2,8,4,6), (1,2,3,4)(5,6,7,8) ])

gap> Size(q);
8

gap> GeneratorsOfGroup(q);
[ (1,5,3,7)(2,8,4,6), (1,2,3,4)(5,6,7,8) ]
```

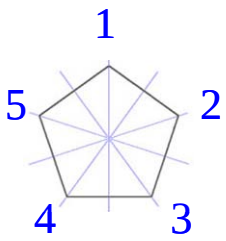
SUMMARY (PART 3)

In part 3 we explored some of the main types of *groups* you are likely to encounter. In particular, in addition to *cyclic groups*, you should now be familiar with the following the following:

- *Cyclic groups*
- *Dihedral groups*.
- *Symmetric groups*.
- *Alternating groups*.
- *Direct products*.
- *Semidirect products*.
- The *group* $D_3 \cong S_3$ of order 6 is the smallest *nonabelian group* there is.
- Since $D_3 \cong S_3$ is the smallest *nonabelian group*, that automatically means that all of its *proper subgroups* are *abelian*.
- The *quaternion group* Q_8 is the first *group* we encounter that doesn't fit into the classification scheme given above. Furthermore, it is the first *group* encountered that is *nonabelian* and yet all of its *subgroups* are *normal*.
- Generators for a *group*
- D_n
- S_n
- A_n
- $A \times B$
- $A >\!\lhd B$
- Q_8

PRACTICE (PART 3)

Consider the regular polygon below.



1. *Find* $|D_5|$.

2. *Find the elements in* D_5. *List these elements as permutations.*

3. *What are the possible orders for subgroups of* D_5*?*

4. *The dihedral group* D_5 *has 8 subgroups. Find all the subgroups of* D_5.

5. *Find the number of elements in* $S_5, S_6,$ and S_7.

6. *Find the number of elements in* $A_5, A_6,$ and A_7.

7. *Find* $\frac{|S_5|}{|A_5|}, \frac{|S_6|}{|A_6|},$ and $\frac{|S_7|}{|A_7|}$.

8. *Below is a list of the 24 elements in S_4. Find the 12 elements in A_4.*

   S_4 = { (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2), (1,2)(3,4), (1,2,3), (1,2,3,4), (1,2,4,3), (1,2,4), (1,3,2), (1,3,4,2), (1,3), (1,3,4), (1,3)(2,4), (1,3,2,4), (1,4,3,2), (1,4,2), (1,4,3), (1,4), (1,4,2,3), (1,4)(2,3) }

9. *Below is a multiplication table for D_3 where R represents a rotation and F represents a flip of an equilateral triangle.*

	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

   a. *How many elements are in $\mathbb{Z}_2 \times D_3$?*

   b. *List in coordinate form the elements in $\mathbb{Z}_2 \times D_3$.*

   c. *Is $\mathbb{Z}_2 \times D_3$ abelian? If not, then give two elements that do not commute with one another along with their products.*

10. *What two cyclic groups can we write $\mathbb{Z}_{10}$ as a direct product of?*

11. *With $\mathbb{Z}_{10}$ expressed as a product of two cyclic groups, list the elements in $\mathbb{Z}_{10}$ in coordinate form.*

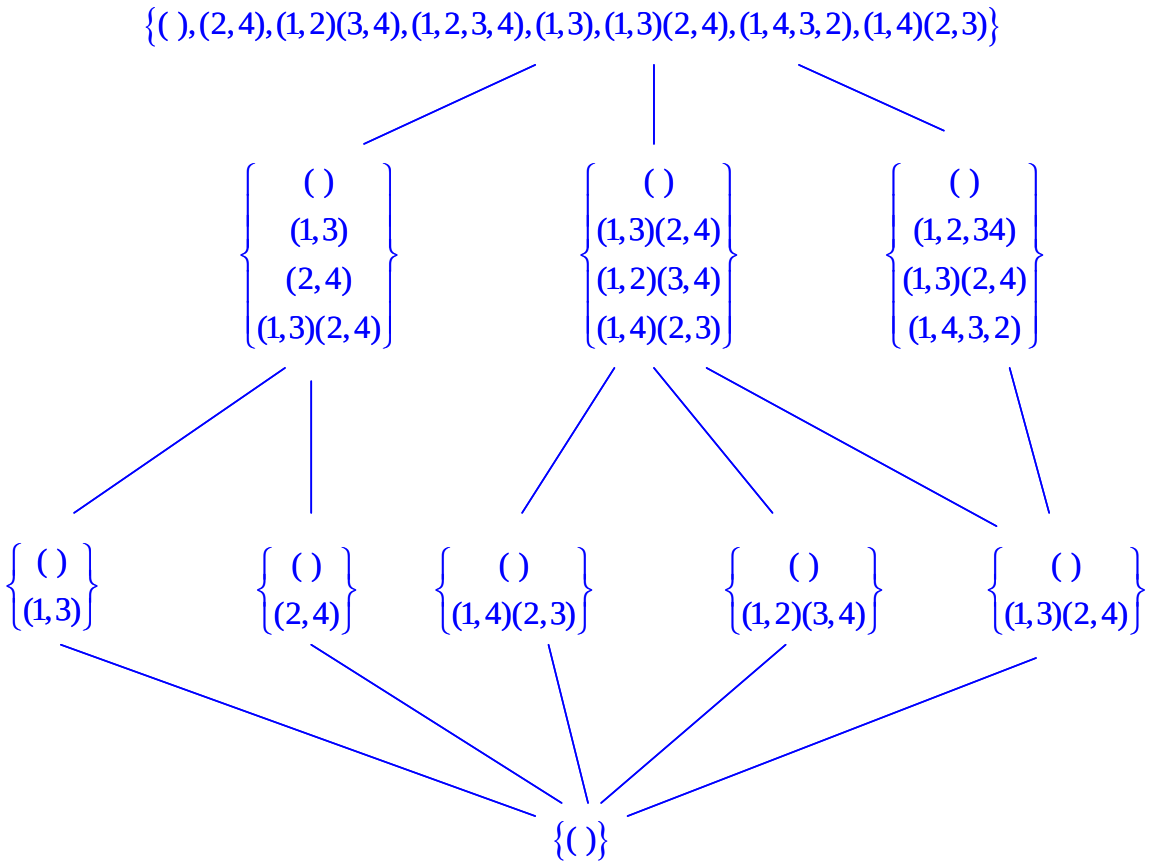
12. *Using your answer to the previous problem, find an element that generates $\mathbb{Z}_{10}$.*

13. *What is the order of $\mathbb{Z}_3 \times \mathbb{Z}_3$?*

14. *What is the order of every non-identity element in $\mathbb{Z}_3 \times \mathbb{Z}_3$? Conclude that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not isomorphic to $\mathbb{Z}_9$ since it has no element of order nine.*

Below is the subgroup lattice for D_4, the dihedral group of order 8 that is associated with the symmetries of a square.

D_4 = { (), (2,4), (1,2)(3,4), (1,2,3,4), (1,3), (1,3)(2,4), (1,4,3,2), (1,4)(2,3) }



Let $C_2 = \{( ),(1,3)\}$ and let $C_4 = \{( ),(1,2,3,4),(1,3)(2,4),(1,4,3,2)\}$.

15. *Verify that $C_2 \cap C_3 = ( )$, that the identity is the only element in the intersection of the two subgroups.*

16. *Verify that $C_2 \cdot C_3 = D_4$, that the product of the two subgroups gives us back the entire group.*

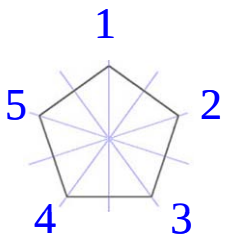
17. *Verify that $C_2 = \{( ),(1,3)\}$ is not a normal subgroup of D_4.*

18. *Verify that $C_4 = \{( ),(1,2,3,4),(1,3)(2,4),(1,4,3,2)\}$ is a normal subgroup of D_4.*

19. *Conclude that* D_4 *is isomorphic to the semidirect product of* C_4 *by* C_2*,* $D_4 \cong C_4 \rtimes C_2$.

PRACTICE (PART 3) - ANSWERS

Consider the regular polygon below.



1. Find $|D_5|$.

   $|D_5| = 10$

2. Find the elements in D_5. List these elements as permutations.

   $$D_5 = \left\{ \begin{array}{l} (), (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2), \\ (2,5)(3,4), (1,3)(4,5), (2,4)(1,5), (1,2)(3,5), (1,4)(2,3) \end{array} \right\}$$

3. What are the possible orders for *subgroups* of D_5?

   $1, 2, 5,$ or 10

4. The *dihedral group* D_5 has 8 *subgroups*. Find all the *subgroups* of D_5.

$\langle () \rangle = \{ () \}$

$\langle (1,2,3,4,5) \rangle = \{ (), (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2) \}$

$\langle (1,3,5,2,4) \rangle = \{ (), (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2) \}$

$\langle (1,4,2,5,3) \rangle = \{ (), (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2) \}$

$\langle (1,5,4,3,2) \rangle = \{ (), (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2) \}$

$\langle (2,5)(3,4) \rangle = \{ (), (2,5)(3,4) \}$

$\langle (1,3)(4,5) \rangle = \{ (), (1,3)(4,5) \}$

$\langle (2,4)(1,5) \rangle = \{ (), (2,4)(1,5) \}$

$\langle (1,2)(3,5) \rangle = \{ (1,2)(3,5) \}$

$\langle (1,4)(2,3) \rangle = \{ (1,4)(2,3) \}$

$$D_5 = \langle (1,2,3,4,5), (2,5)(3,4) \rangle \begin{Bmatrix} (), (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2), \\ (2,5)(3,4), (1,3)(4,5), (2,4)(1,5), (1,2)(3,5), (1,4)(2,3) \end{Bmatrix}$$

In the list above, we have 7 distinct *cyclic groups.* That plus the entire *group* D_5, gives us eight *subgroups* in all. Thus, all eight subgroups of D_5 are accounted for.

5. Find the number of elements in $S_5, S_6,$ and S_7.

$|S_5| = 5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$

$|S_6| = 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$

$|S_7| = 7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$

6. Find the number of elements in $A_5, A_6,$ and A_7.

$$|A_5| = \frac{|S_5|}{2} = \frac{120}{2} = 60$$

$$|A_6| = \frac{|S_6|}{2} = \frac{720}{2} = 360$$

$$|A_6| = \frac{|S_6|}{2} = \frac{5040}{2} = 2520$$

7. Find $\frac{|S_5|}{|A_5|}, \frac{|S_6|}{|A_6|}$, and $\frac{|S_7|}{|A_7|}$.

$\frac{|S_5|}{|A_5|} = 2$

$\frac{|S_6|}{|A_6|} = 2$

$\frac{|S_7|}{|A_7|} = 2$

8. Below is a list of the 24 elements in S_4. Find the 12 elements in A_4.

S_4 = { (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2), (1,2)(3,4), (1,2,3), (1,2,3,4), (1,2,4,3), (1,2,4), (1,3,2), (1,3,4,2), (1,3), (1,3,4), (1,3)(2,4), (1,3,2,4), (1,4,3,2), (1,4,2), (1,4,3), (1,4), (1,4,2,3), (1,4)(2,3) }

A_4 = { (), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4), (1,3,2), (1,3,4), (1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3) }

9. Below is a *multiplication table* for D_3 where *R* represents a rotation and *F* represents a flip of an equilateral triangle.

	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

a. How many elements are in $\mathbb{Z}_2 \times D_3$?

$|\mathbb{Z}_2 \times D_3| = |\mathbb{Z}_2| \cdot |D_3| = 2 \cdot 6 = 12$

b. List in coordinate form the elements in $\mathbb{Z}_2 \times D_3$.

$$\mathbb{Z}_2 \times D_3 = \left\{ \begin{matrix} (0,e),(0,R),(0,R^2),(0,F),(0,FR),(0,FR^2), \\ (1,e),(1,R),(1,R^2),(1,F),(1,FR),(1,FR^2) \end{matrix} \right\}$$

c. Is $\mathbb{Z}_2 \times D_3$ abelian? If not, then give two elements that do not commute with one another along with their products.

No, it's not abelian since $(0,R)*(0,F) = (0,FR^2)$, but $(0,F)*(0,R) = (0,FR)$.

10. What two *cyclic groups* can we write $\mathbb{Z}_{10}$ as a *direct product* of?

$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$

11. With $\mathbb{Z}_{10}$ expressed as a product of two *cyclic groups*, list the elements in $\mathbb{Z}_{10}$ in coordinate form.

$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5 = \{(0,0),(0,1),(0,2),(0,3),(0,4),(1,0),(1,1),(1,2),(1,3),(1,4)\}$

12. Using your answer to the previous problem, find an element that generates $\mathbb{Z}_{10}$.

$(1,1) = (1,1)$
$(1,1) + (1,1) = (0,2)$
$(1,1) + (1,1) + (1,1) = (1,3)$
$(1,1) + (1,1) + (1,1) + (1,1) = (0,4)$
$(1,1) + (1,1) + (1,1) + (1,1) + (1,1) = (1,0)$
$(1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) = (0,1)$
$(1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) = (1,2)$
$(1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) = (0,3)$
$(1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) = (1,4)$
$(1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) = (0,0)$

Therefore, $\langle (1,1) \rangle \cong \mathbb{Z}_{10}$

13. What is the order of $\mathbb{Z}_3 \times \mathbb{Z}_3$?

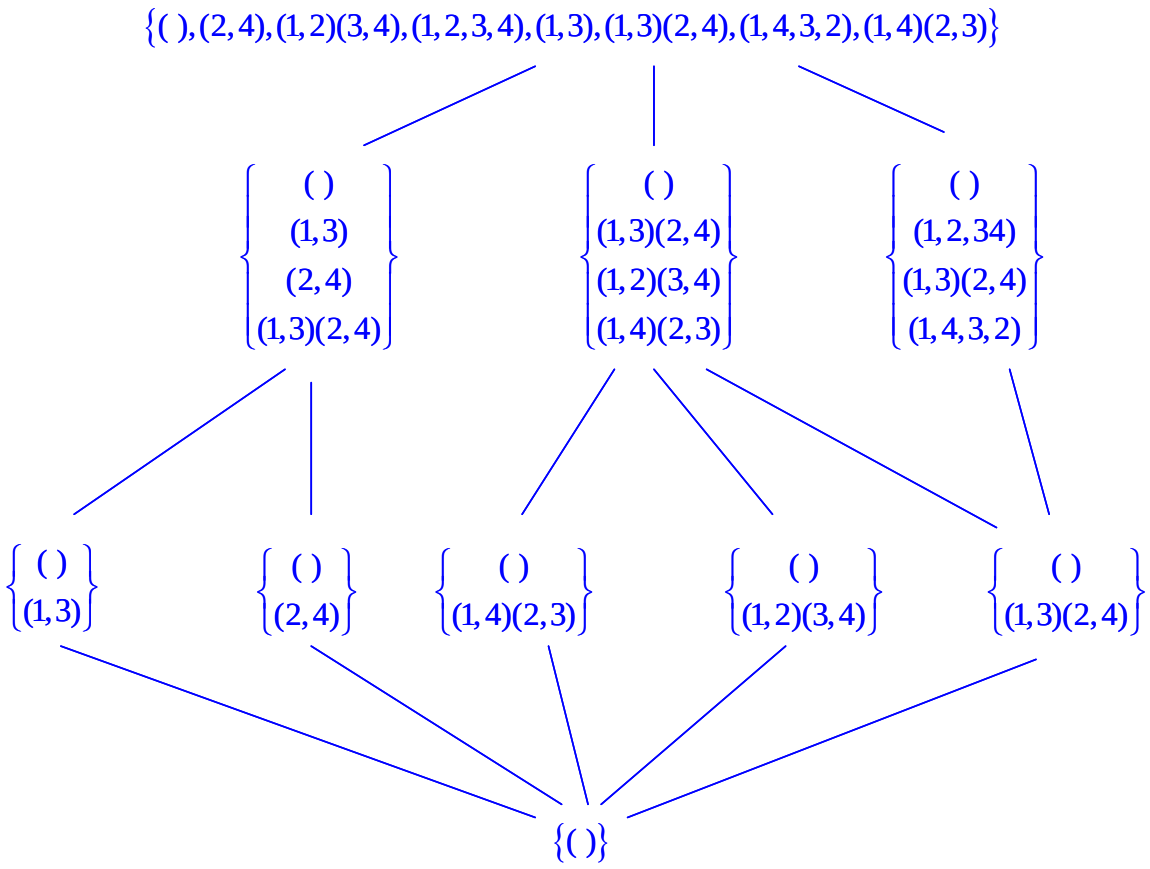
$|\mathbb{Z}_2 \times \mathbb{Z}_3| = |\mathbb{Z}_2| \cdot |\mathbb{Z}_3| = 3 \cdot 3 = 9$

14. What is the order of every non-identity element in $\mathbb{Z}_3 \times \mathbb{Z}_3$? Conclude that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not *isomorphic* to $\mathbb{Z}_9$ since it has no element of order nine.

Every non-identity element in $\mathbb{Z}_3 \times \mathbb{Z}_3$ has order 3. Therefore, it can't be isomorphic to $\mathbb{Z}_9$ which has an element of order 9.

Below is the *subgroup* lattice for D_4, the *dihedral group* of order 8 that is associated with the symmetries of a square.

D_4 = { (), (2,4), (1,2)(3,4), (1,2,3,4), (1,3), (1,3)(2,4), (1,4,3,2), (1,4)(2,3) }



Let $C_2 = \{( ),(1,3)\}$ and let $C_4 = \{( ),(1,2,3,4),(1,3)(2,4),(1,4,3,2)\}$.

15. Verify that $C_2 \cap C_3 = ( )$, that the identity is the only element in the intersection of the two *subgroups*.

Direct examination of the elements of the two *subgroups* confirms that

$C_2 \cap C_3 = ( )$.

16. Verify that $C_2 \cdot C_3 = D_4$, that the product of the two *subgroups* gives us back the entire group.

$$
\begin{array}{rcl}
( )( ) & = & ( ) \\
( )(1,2,3,4) & = & (1,2,3,4) \\
( )(1,3)(2,4) & = & (1,3)(2,4) \\
( )(1,4,3,2) & = & (1,4,3,2) \\
(1,3)( ) & = & (1,3) \\
(1,3)(1,2,3,4) & = & (1,4)(3,2) \\
(1,3)(1,3)(2,4) & = & (2,4) \\
(1,3)(1,4,3,2) & = & (1,2)(3,4)
\end{array}
$$

Therefore, $C_2 \cdot C_3 = D_4$.

17. Verify that $C_2 = \{( ),(1,3)\}$ is not a *normal subgroup* of D_4.

If $a = (1,2)$, then $a^{-1}C_2 a = (1,2)\begin{Bmatrix} ( ) \\ (1,3) \end{Bmatrix}(1,2) = \begin{Bmatrix} ( ) \\ (2,3) \end{Bmatrix} \neq C_2$. Hence, C_2 is not a *normal subgroup* of D_4.

18. Verify that $C_4 = \{( ),(1,2,3,4),(1,3)(2,4),(1,4,3,2)\}$ is a *normal subgroup* of D_4.

Every element of D_4 can be written as a product of an element in C_2 and an element in C_4. Hence, if *ab* is an element of D_4 where *a* is an element of C_2 and *b* is an element of C_4, then we need to argue that $(ab)^{-1}C_4(ab) = b^{-1}a^{-1}C_4 ab = C_4$. Well, it's clear that conjugation of C_4 by the

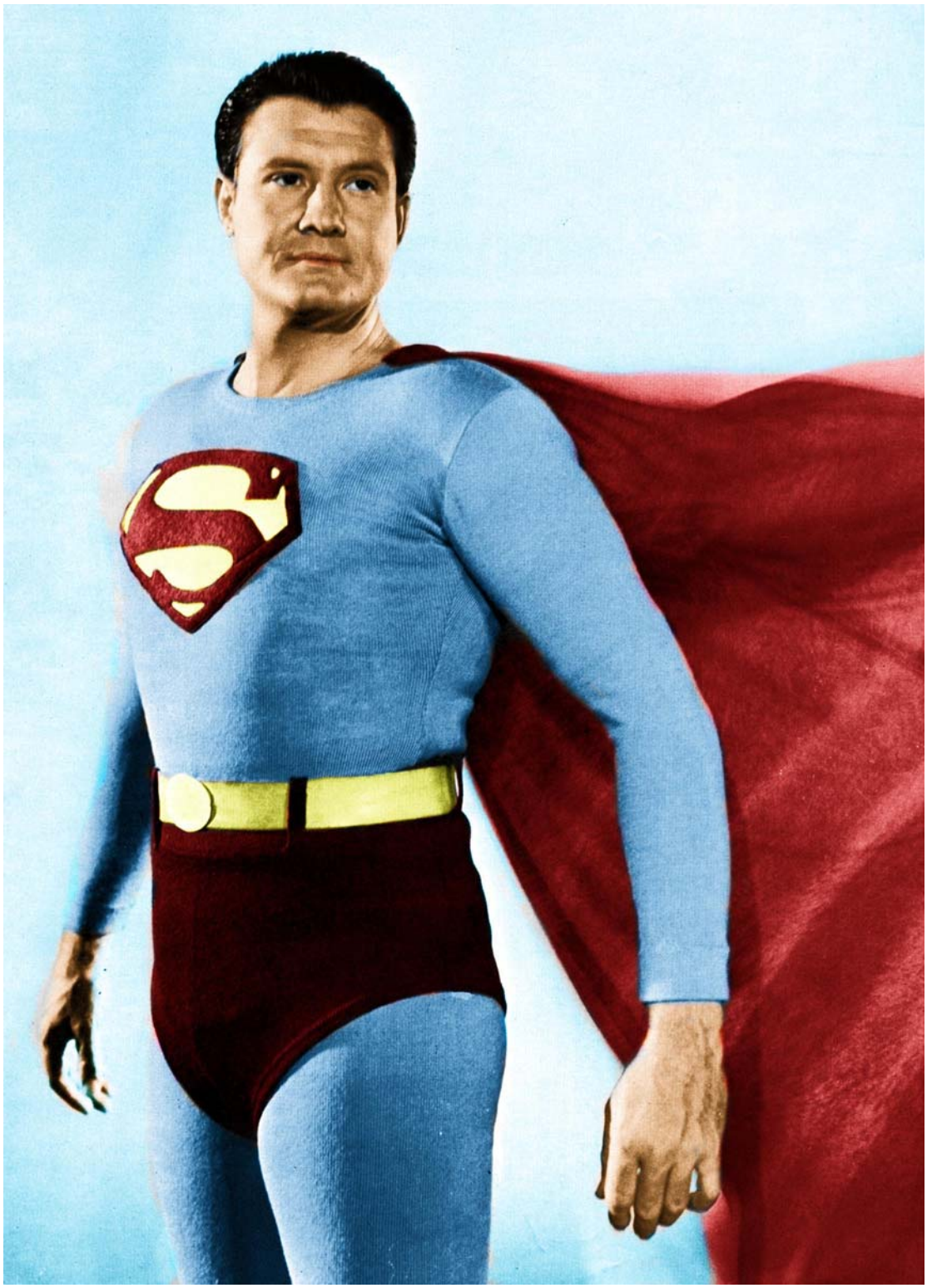
identity gives us back C_4, so we can assume that $a=(1,3)$ and

$$(1,3)C_4(1,3)=(1,3)\begin{Bmatrix}()\\(1,2,3,4)\\(1,3)(2,4)\\(1,4,3,2)\end{Bmatrix}(1,3)=\begin{Bmatrix}(1,3)()(1,3)\\(1,3)(1,2,3,4)(1,3)\\(1,3)(1,3)(2,4)(1,3)\\(1,3)(1,4,3,2)(1,3)\end{Bmatrix}=\begin{Bmatrix}()\\(1,4,3,2)\\(1,3)(2,4)\\(1,2,3,4)\end{Bmatrix}=C_4.$$ And

finally, since *b* is an element of C_4, conjugation of C_4 by *b* must also give us back C_4. Hence, $(ab)^{-1}C_4(ab)=b^{-1}a^{-1}C_4ab=C_4$, and C_4 is a *normal subgroup* of D_4.

19. Conclude that D_4 is *isomorphic* to the *semidirect product* of C_4 by C_2, $D_4\cong C_4>\!\!\triangleleft C_2$.

Since $C_2\cap C_3=()$, $C_2\cdot C_3=D_4$, and C_4 is a *normal subgroup* of D_4 while C_2 isn't, it follows that D_4 is the *semidirect product* of C_4 by C_2, $D_4=C_4>\!\!\triangleleft C_2$.



SYMMETRIC GROUP MAN!