MATH 417 – FOURTH WEEK

BRUCE REZNICK
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

September 14, 2020, in advance

Today, at first, I'd like to revisit S_3 from a different, more abstract, point of view.

First, let's review what we've seen of S_3:

$$\rho_0 = \begin{pmatrix}123\\123\end{pmatrix} = (1)(2)(3), \quad \rho_1 = \begin{pmatrix}123\\231\end{pmatrix} = (123),$$
$$\rho_2 = \begin{pmatrix}123\\312\end{pmatrix} = (132), \quad \mu_1 = \begin{pmatrix}123\\132\end{pmatrix} = (1)(23),$$
$$\mu_2 = \begin{pmatrix}123\\321\end{pmatrix} = (13)(2), \quad \mu_3 = \begin{pmatrix}123\\213\end{pmatrix} = (12)(3).$$

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Now, I'll try to make a more abstract group $(G, *)$ out of this. The element ρ_0 is the identity, so I will call it e. Next, let's call $\rho_1 = a$; then $\rho_2 = \rho_1^2 = a^2$ and $a^3 = e$. In our abstract group, we have $\langle a\rangle = \{e, a, a^2\}$ and $a^3 = e = a^0$, and, as a small reminder, $a^{-1} = a^2, (a^2)^{-1} = a$.

That's not all we have in the group, so I'll let $\mu_1 = b$. I know two things about b: $b \notin \{e, a, a^2\}$ and $b^2 = e$. Now G is a group and $a, a^2, b \in G$. Since $*$ is a binary operation, we know that $a*b, a^2*b \in G$ as well. I'll drop $*$ and use juxtaposition from now on, so call these ab and a^2b. If you look at the table for S_3, you'll see that ab should be μ_2 and a^2b should be μ_3.

The first thing I want to do is show that these six abstract elements

$$\{e, a, a^2, b, ab, a^2b\}$$

are all different. We know this is true for the first four. If $a^ib = a^jb$, then you can multiply on the right by b (always assume associativity).

$$a^ib = a^jb \implies (a^ib)b = (a^jb)b \implies a^i(b^2) = a^j(b^2) \implies a^i = a^j$$

Thus b, ab, a^2 are different. Finally,

$$a^ib = a^j \implies a^{-i}(a^ib) = a^{-i}a^j \implies (a^{-i}a^i)b = a^{-i}a^j \implies b = a^{j-i}.$$

We now have six elements. Let's assume this is all of G (a big assumption!) and try to make the multiplication table. We don't know everything here, but we know a lot

G	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	?	?	e	?	?
ab	ab	?	?	?	?	?
a^2b	a^2b	?	?	?	?	?

I count 14 openings. Now we can't just multiply these together, because they're abstract, and not permutations. We don't know what to do. The most obvious issue is ba. Because we are assuming this is a group, it has to be in G. And by the uniqueness of elements in rows and columns in a multiplication table, we may assume that it isn't in $\{e, a, a^2, b\}$. So either $ba = ab$ or $ba = a^2b$. As we'll see, both are possible. (for different groups of course.)

Let's look at our model: $a = \rho_1$, $a^2 = \rho_2$, $b = \mu_1$. We have

$$ba \iff \mu_1 \circ \rho_1 = \begin{pmatrix}123\\132\end{pmatrix}\begin{pmatrix}123\\231\end{pmatrix} = \begin{pmatrix}123\\321\end{pmatrix} = \mu_2$$

$$ab \iff \rho_1 \circ \mu_1 = \begin{pmatrix}123\\231\end{pmatrix}\begin{pmatrix}123\\132\end{pmatrix} = \begin{pmatrix}123\\213\end{pmatrix} = \mu_3$$

$$a^2b \iff \rho_2 \circ \mu_1 = \begin{pmatrix}123\\312\end{pmatrix}\begin{pmatrix}123\\132\end{pmatrix} = \begin{pmatrix}123\\321\end{pmatrix} = \mu_2$$

What this means is that if we want to make a group that looks like S_3, it would be good to assume $ba = a^2b$. (For later reference, this is $ba = a^{-1}b$.)

I'll put this entry in now.

G	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	?	e	?	?
ab	ab	?	?	?	?	?
a^2b	a^2b	?	?	?	?	?

It turns out that this actually lets us finish the whole table. First let's finish the "$b*$" row. There are many choices here, and it doesn't matter so much which one you choose.

Let me say in advance that these calculations may seem very strange to you. Just remember that we have three rules: $a^3 = e, b^2 = e, ba = a^2b$ and we can apply them to any computation. We are also assuming that associativity holds. The first time you see this, it might seem like a magician doing card tricks, but there are no tricks here.

$$ba^2 = b(aa) = (ba)a = (a^2b)a = a^2(ba) = a^2(a^2b) = (a^2a^2)b = a^4b = ab$$
$$b(ab) = (ba)b = (a^2b)b = a^2b^2 = a^2$$
$$b(a^2b) = b(a^2b) = (ba^2)b = (ab)b = ab^2 = a$$

G	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	?	?	?	?	?
a^2b	a^2b	?	?	?	?	?

The other two rows are easier, because $(ab)g = a(bg)$ and $(a^2b)g = a^2(bg)$, and we've already calculated bg.

G	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Define Φ by:

$$\Phi(e) = \rho_0, \quad \Phi(a) = \rho_1, \quad \Phi(a^2) = \rho_2,$$
$$\Phi(b) = \mu_1, \quad \Phi(ab) = \mu_2, \quad \Phi(a^2b) = \mu_3.$$

Then Φ gives an isomorphism from G to S_3.

We can even try to make "rules" for the multiplication table (I think the some pretty nice patterns in this table are easier to see than in the one for S_3.) This will be going over what we've done earlier, but with a better perspective:

The elements of G have the form a^i or a^ib.

$$a^ia^j = a^{i+j}, \qquad a^ia^jb = a^{i+j}b$$

As we saw, it's a bit more complicated when the first factor is a^ib, and the easiest way to see what happens for a^iba^j is to split the three cases: $j = 0, 1, 2$.

$$a^ib * e = a^ib$$
$$a^ib * a = a^i(ba) = a^i(a^2b) = a^{i+2}b$$
$$a^ib * a^2 = a^i(ba)a = a^i(a^2b)a = a^{i+2}ba = a^{i+2}(ba) = a^{i+2}(a^2b) = a^{i+4}b$$

(As always, we can and should reduce the exponent of a by using $a^3 = e$.) The succinct version of this is

$$a^ib\ a^j = a^{i+2j}b, \qquad a^ib\ a^jb = (a^iba^j)b = a^{i+2j}b^2 = a^{i+2j}.$$

A final remark: $e = a^{-3j}$, so you can replace a^{i+2j} by $a^{-3j}a^{i+2j} = a^{i-j}$ above if you like.

Remember all the way back at the beginning of class, when I talked about the choice we made for ba. We chose $ba = a^2b$. What would have happened if we had chosen the other one, $ba = ab$? I'll call this group H. Recall that we had

H	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	?	?	e	?	?
ab	ab	?	?	?	?	?
a^2b	a^2b	?	?	?	?	?

Multiplication in H is much easier than in G. Since $ab = ba$, multiplication turns out to be commutative, and we can just move factors around directly $a^ib *_H a^j$ consists of i a's, followed by one b, followed by j $a's$. But whenever we see ba, we can replace it with ab, and send it over to the right, so $a^ib *_H a^j = a^{i+1}ba^{j-1}$ and, eventually, $a^{i+j}b$. Similarly, $a^ib *_H a^jb = a^{i+j}b^2 = a^{i+j}$. This gives us

H	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	ab	a^2b	e	a	a^2
ab	ab	a^2b	b	a	a^2	e
a^2b	a^2b	b	ab	a^2	e	a

Is this a group we know? Yes it is! In fact, we know it two ways. First, look at $\langle ab\rangle$:

$$(ab)^0 = e, (ab)^1 = ab, (ab)^2 = a^2b^2 = a^2, (ab)^3 = ab * (ab)^2 = aba^2 = b,$$
$$(ab)^4 = ab * (ab)^3 = ab * b = a, (ab)^5 = ab * (ab)^4 = aba = a^2b,$$
$$(ab)^6 = ab * (ab)^5 = aba^2b = a^3b^2 = e.$$

So if we write $ab = x$, then the powers of x are: $\{e, ab, a^2, b, a, a^2b\} = H$. That is, H is a cyclic group of order six! I'll permute the rows and columns of the multiplication table to make this clear:

H	e	ab	a^2	b	a	a^2b
e	e	ab	a^2	b	a	a^2b
ab	ab	a^2	b	a	a^2b	e
a^2	a^2	b	a	a^2b	e	ab
b	b	a	a^2b	e	ab	a^2
a	a	a^2b	e	ab	a^2	b
a^2b	a^2b	e	ab	a^2	b	a

There's a second way to look at this group. We have elements of the form a^jb^k, where $a^3 = e$ and $b^2 = e$, and so what really matters is j mod 3 and k mod 2. The multiplication rule is even simpler than I said:

$$a^jb^k * a^mb^n = a^{j+m}b^{k+n}$$

Let us define a function Φ from H to $((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}), \oplus)$ by

$$\Phi(a^jb^k) = ([k]_2, [j]_3)$$

Then because $a^3 = e$ and $b^2 = e$, the group operation above tells us that

$$\Phi(a^jb^k * a^mb^n) = ([k+n]_2, [j+m]_3) =$$
$$([k]_2, [j]_3) \oplus ([n]_2, [m]_3) = \Phi(a^jb^k) \oplus \Phi(a^mb^n)$$

The function Φ is a bijection and respects the operation, so it is an isomorphism.

This is an example of what mathematicians do. We can put together a bunch of rules and then see what the consequences of the rules are.

I made things easier by saying that $\{e, a, a^2, b, ab, a^2b\}$ was the whole group. But as it turns out, if all I had said was "let's look at all products of powers of a and b", looking at objects like

$$(a^{i_1}b)(a^{i_2}b)\cdots(a^{i_n}b)$$

we would still only get these six. Our rules were powerful enough to reduce everything.

Pretty soon, we'll look at $\{a^jb^k : a^4 = e, b^2 = e, ba = a^{-1}b = a^3b\}$. If you're interested, this is the description of the dihedral group D_4, which has order 8, and describes the rotations and flips of a square. If there's time in class today, I'll start talking about it.

There is one more idea that turns out to be extremely important, and that is the coset. I won't prove anything today, but I want to get you used to the idea.

Suppose H is a subgroup of G and $g \in G$ (not necessarily in H). The *left coset* gH and the *right coset* Hg are defined by

$$gH = \{g * h \mid h \in H\}, \quad Hg = \{h * g \mid h \in H\}.$$

Let's look at our "abstract" version of S_3, with its multiplication table.

G	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

I will take $H = \{e, b\}$, which is a group of order two because $b^2 = e$. With all six choices for g in H, we get

$$eH = e\{e,b\} = \{e,b\} \qquad He = \{e,b\}e = \{e,b\}$$
$$aH = a\{e,b\} = \{a,ab\} \qquad Ha = \{e,b\}a = \{a,a^2b\}$$
$$a^2H = a^2\{e,b\} = \{a^2,a^2b\} \qquad Ha^2 = \{e,b\}a^2 = \{a^2,ab\}$$
$$bH = b\{e,b\} = \{b,e\} \qquad Hb = \{e,b\}b = \{b,e\}$$
$$abH = ab\{e,b\} = \{ab,a\} \qquad Hab = \{e,b\}ab = \{ab,a^2\}$$
$$a^2bH = a^2b\{e,b\} = \{a^2b,a^2\} \qquad Ha^2b = \{e,b\}a^2b = \{a^2b,a\}$$

Things to notice (all of which will be proved later).

The number of elements in each coset is the same as the number of elements in H.

Any two left cosets xH and yH are either equal as sets or disjoint. The same thing is true for any two right cosets. This is *not* true when you compare one left coset with one right coset.

The distinct left cosets of H in G are $\{e, b\}, \{a, ab\}, \{a^2, a^2b\}$ and the distinct right cosets of H in G are $\{e, b\}, \{a, a^2b\}, \{a^2, ab\}$. These are different!

If we let $[G : H]$ denote the number of distinct left cosets and count the elements of G, it turns out that $[G : H] \cdot |H| = |G|$ and this gives us the extremely important result called LaGrange's Theorem, that $|H| \mid |G|$.

September 14, 2020, in class

First a correction. The matrix form of ρ_2 was incorrect on p.1 of yesterday's material; now fixed here.

I'd like to start by saying a bit more about cosets. For cyclic groups and abelian groups, they are very easy!

Suppose H is a subgroup of G and $g \in G$ (not necessarily in H). The left coset gH and the right coset Hg are defined by

$$gH = \{gh \mid h \in H\}, \quad Hg = \{hg \mid h \in H\}.$$

For today, we'll assume that G is a finite abelian group, such as C_n, and H is a subgroup and $H = \{h_1, \ldots, h_m\}$, so

$$gH = \{gh_1, \ldots, gh_m\}, \quad Hg = \{h_1g, \ldots, h_mg\}.$$

Since G is abelian, $gh_j = h_jg$ for every j and so $gH = Hg$ automatically. We've seen this doesn't happen necessarily for a non-abelian group.

In general (even if G is not abelian) if $H = \{e\}$, which is a subgroup of G, then for any $x \in G$,

$$xH = \{x\} = Hx.$$

So the coset is just the one-element set. If $H = G$, then

$$xH = xG = \{xg : g \in G\}$$

Suppose $y \in G$. Take $g = x^{-1}y$ to see that

$$xg = x(x^{-1}y) = (xx^{-1})y = ey = y \in xH.$$

This is true for every $y \in G$ is in xH, so $xH = G$. The same thing is true for Hx when $H = G$. For a finite group, xG is just the x row of the multiplication table and Gx is the x column.

Let's take $G = C_6 = \langle a \rangle, a^6 = e$. The four divisors of 6 are 1, 2,3,6, and G has two proper subgroups: $H_1 = \langle a^2 \rangle = \{e, a^2, a^4\}$ and $H_2 = \langle a^3 \rangle = \{e, a^3\}$. Let's find the cosets.

$$\begin{aligned} eH_1 = \{e, a^2, a^4\}, \qquad & aH_1 = \{a, a^3, a^5\}, \\ a^2H_1 = \{a^2, a^4, a^6\} = H_1, \qquad & a^3H_1 = \{a^3, a^5, a\} = aH_1, \\ a^4H_1 = \{a^4, e, a^2\} = H_1, \qquad & a^5H_1 = \{a^5, a, a^3\} = aH_1 \\ eH_2 = \{e, a^3\}, \qquad & a^3H_2 = \{a^3, e\} = eH_2 \\ aH_2 = \{a, a^4\}, \qquad & a^4H_2 = \{a^4, a\} = aH_2 \\ a^2H_2 = \{a^2, a^5\} \qquad & a^5H_2 = \{a^5, a^2\} = a^2H_2. \end{aligned}$$

Notice for later reference, that $x \in H_1 \implies xH_1 = H_1$ and $x \in aH_1 \implies xH_1 = aH_1$ and similarly for H_2. This will hold in general.

Now, I want to talk to you about another group you will get to know well: D_4, which is the group of symmetries of a square.

There are 8 of them. You can believe this as follows: you can rotate the square in 4 ways (none, 90, 180 or 270 degrees) and then you can flip it over and rotate that 4 ways. I'll use the same names as in the book, and introduce them one at a time, as I did with S_3.

Here is the square:

$$\begin{array}{cc} 1 & 2 \\ \\ 4 & 3 \end{array}$$

This is the first element, ρ_0. Under ρ_0,

$$1 \mapsto 1, \quad 2 \mapsto 2, \quad 3 \mapsto 3, \quad 4 \mapsto 4$$

$$\rho_0 = \begin{pmatrix} 1234 \\ 1234 \end{pmatrix} = (1)(2)(3)(4), \qquad \begin{array}{cc} 1 & 2 \\ \\ 4 & 3 \end{array}$$

Thus $\rho_0 = e$ is the identity element (again). The square at the end to show the motions of these permutations and this is the starting configuration. Think of the numbers as labels that can move, and also indicate the name of the position.

This is the second element, ρ_1. Under ρ_1,

$$1 \mapsto 2, \quad 2 \mapsto 3, \quad 3 \mapsto 4, \quad 4 \mapsto 1$$

$$\rho_1 = \begin{pmatrix} 1234 \\ 2341 \end{pmatrix} = (1234), \qquad \begin{array}{cc} 4 & 1 \\ \\ 3 & 2 \end{array}$$

Thus $\rho_1 = e$ represents clockwise rotation by $\frac{\pi}{2}$ or 90 degrees. It's very much like the ρ_1 of S_3, but it's in a different group: S_4. A small calculation shows that $\rho_1^4 = \rho_0 = e$. Or you can think about the square.

This is the third element, ρ_2. Under ρ_2,

$$1 \mapsto 3, \quad 2 \mapsto 4, \quad 3 \mapsto 1, \quad 4 \mapsto 2$$

$$\rho_2 = \begin{pmatrix} 1234 \\ 3412 \end{pmatrix} = (13)(24), \qquad \begin{matrix} 3 & 4 \\ \\ 2 & 1 \end{matrix}$$

Thus ρ_2 is rotation by π or 180 degrees, so $\rho_2 = \rho_1^2$ and $\rho_2^2 = \rho_0 = e$. This element will be of special interest when we start talking about subgroups.

This is the fourth element, ρ_3. Under ρ_3,

$$1 \mapsto 4, \quad 2 \mapsto 1, \quad 3 \mapsto 2, \quad 4 \mapsto 3$$

$$\rho_3 = \begin{pmatrix} 1234 \\ 4123 \end{pmatrix} = (1432), \qquad \begin{matrix} 2 & 3 \\ \\ 1 & 4 \end{matrix}$$

Here, ρ_3 represents clockwise rotation by $\frac{3\pi}{2}$ or 270 degrees, or counterclockwise by 90 degrees. We have $\rho_3 = \rho_1^3 = \rho_1^{-1}$ and $\rho_3^4 = \rho_0 = e$. This is the final rotation in D_4.

There are two kinds of flips, and I'll keep the notation of the book. This is the fifth element, μ_1. Under μ_1,

$$1 \mapsto 2, \quad 2 \mapsto 1, \quad 3 \mapsto 4, \quad 4 \mapsto 3$$

$$\mu_1 = \begin{pmatrix} 1234 \\ 2143 \end{pmatrix} = (12)(34), \qquad \begin{matrix} 2 & 1 \\ \\ 3 & 4 \end{matrix}$$

I hope you can see that μ_1 is equivalent to flipping on a vertical axis through the center of the square, and if there were a front and a back, the back would now be on front; also, $\mu_1^2 = \rho_0$.

This is the sixth element, μ_2. Under μ_2,

$$1 \mapsto 4 \quad 2 \mapsto 3, \quad 3 \mapsto 2, \quad 4 \mapsto 1.$$

$$\mu_2 = \begin{pmatrix} 1234 \\ 4321 \end{pmatrix} = (14)(23), \qquad \begin{matrix} 4 & 3 \\ \\ 1 & 2 \end{matrix}$$

I hope you can see that μ_2 is equivalent to flipping on a horizontal axis through the center of the square, and if there were a front and a back, the back would now be on front, and $\mu_2^2 = \rho_0$.

What is $\mu_1 \circ \mu_2$? Since it's two flips, the front is back to the front and it has to be a rotation and $\mu_1 \circ \mu_1 = \mu_2 \circ \mu_2 = \rho_0$, so it can't be that.

$$\mu_1 \circ \mu_2 = \binom{1234}{2143}\binom{1234}{4321} = \binom{1234}{3412} = \rho_2.$$

You should check that $\mu_2 \circ \mu_1 = \rho_2$ as well. Try to visualize.

Now the second kind of flip. This is the seventh element, δ_1. Under δ_1,

$$1 \mapsto 3, \quad 2 \mapsto 2, \quad 3 \mapsto 1, \quad 4 \mapsto 4$$

$$\delta_1 = \binom{1234}{3214} = (13)(2)(4), \qquad \begin{matrix} 3 & 2 \\ \\ 4 & 1 \end{matrix}$$

I hope you can see that δ_1 is equivalent to flipping on a NE-SW diagonal axis, and those corners don't move; and if there were a front and a back, the back would now be on front; also, $\delta_1^2 = \rho_0$.

This is the eighth and final element, δ_2. Under δ_2,

$$1 \mapsto 1, \quad 2 \mapsto 4, \quad 3 \mapsto 3, \quad 4 \mapsto 2$$

$$\delta_2 = \binom{1234}{1432} = (24)(1)(3), \qquad \begin{matrix} 1 & 4 \\ \\ 2 & 3 \end{matrix}$$

I hope you can see that δ_2 is equivalent to flipping on a NW-SE diagonal axis, and those corners don't move; and if there were a front and a back, the back would now be on front; also, $\delta_2^2 = \rho_0$.

What is $\delta_1 \circ \delta_2$? Since it's two flips, the front is back to the front and it has to be a rotation and $\mu_1 \circ \mu_1 = \mu_2 \circ \mu_2 = \rho_0$, so it can't be that.

$$\delta_1 \circ \delta_2 = \binom{1234}{3214}\binom{1234}{1432} = \binom{1234}{3412} = \rho_2.$$

You should check that $\delta_2 \circ \delta_1 = \rho_2$ as well.

Here are some computations.

$$\mu_1 \circ \rho_1 = \begin{pmatrix}1234\\2143\end{pmatrix} \circ \begin{pmatrix}1234\\2341\end{pmatrix} = \begin{pmatrix}1234\\1432\end{pmatrix} = \delta_2$$
$$\rho_1 \circ \mu_1 = \begin{pmatrix}1234\\2341\end{pmatrix} \circ \begin{pmatrix}1234\\2143\end{pmatrix} = \begin{pmatrix}1234\\3214\end{pmatrix} = \delta_1$$
$$\mu_1 \circ \delta_1 = \begin{pmatrix}1234\\2143\end{pmatrix} \circ \begin{pmatrix}1234\\3214\end{pmatrix} = \begin{pmatrix}1234\\4123\end{pmatrix} = \rho_1^3$$
$$\delta_1 \circ \mu_1 = \begin{pmatrix}1234\\3214\end{pmatrix} \circ \begin{pmatrix}1234\\2143\end{pmatrix} = \begin{pmatrix}1234\\2341\end{pmatrix} = \rho_1$$

So we have the rotations and two kinds of flips. As before rotations and rotations or flips and flips combine to be rotations and rotations and flips in either order combine to be flips. But the two kind of flips are the μ's and the δ's. It will turn out that two μ's or two δ's combine to give something in $\{e, \rho_1^2\}$ and a μ and a δ, in either order, combine to give something in $\{\rho_1, \rho_3^2\}$. See the full table on p.80.

WORKSHEET PROBLEMS

1. Let $G = C_{12} = \langle a \rangle, a^{12} = e$. Write down all 12 left cosets of the subgroup $H = \{e, a^4, a^8\}$. How many different left cosets are there? (This is the abelian case, so left cosets = right cosets, and we usually just say "cosets".)

2. Recall the following four elements of D_4:

$$\rho_0 = \begin{pmatrix}1234\\1234\end{pmatrix} = (1)(2)(3)(4), \quad \rho_2 = \begin{pmatrix}1234\\3412\end{pmatrix} = (13)(24),$$
$$\mu_1 = \begin{pmatrix}1234\\2143\end{pmatrix} = (12)(34), \quad \mu_2 = \begin{pmatrix}1234\\4321\end{pmatrix} = (14)(23),$$

Show that $H = \{\rho_0, \rho_2, \mu_1, \mu_2\}$ is a subgroup by constructing the multiplication table to show that it is closed under $\circ$. This subgroup is isomorphic to one we've spent a lot of time with already. Which one?

WORKSHEET SOLUTIONS

1. There are four different cosets. We have

$$H = a^4H = a^8H = \{e, a^4, a^8\},$$
$$aH = a^5H = a^9H = \{a, a^5, a^9\},$$
$$a^2H = a^6H = a^{10}H = \{a^2, a^6, a^{10}\},$$
$$a^3H = a^7H = a^{11}H = \{a^3, a^7, a^{11}\}$$

Notice that in C_{12}, the element a^k is determined by $k \mod 12$, while membership in a coset is determined by $k \mod 4$. This can be generalized.

I'll repeat the entries:

$$\rho_0 = \begin{pmatrix}1234\\1234\end{pmatrix} = (1)(2)(3)(4), \quad \rho_2 = \begin{pmatrix}1234\\3412\end{pmatrix} = (13)(24),$$
$$\mu_1 = \begin{pmatrix}1234\\2143\end{pmatrix} = (12)(34), \quad \mu_2 = \begin{pmatrix}1234\\4321\end{pmatrix} = (14)(23),$$

Here ρ_0 is the identity, and each of the other three elements squares to ρ_0. There are a bunch of multiplications, all of which have a familiar ring; for example

$$\mu_1 \circ \rho_2 = \begin{pmatrix}1234\\2143\end{pmatrix} \circ \begin{pmatrix}1234\\3412\end{pmatrix} = \begin{pmatrix}1234\\4321\end{pmatrix} = \mu_2.$$

What we have here is yet another incarnation of V.

H	ρ_0	ρ_2	μ_1	μ_2
ρ_0	ρ_0	ρ_2	μ_1	μ_2
ρ_2	ρ_2	ρ_0	μ_2	μ_1
μ_1	μ_1	μ_2	ρ_0	ρ_2
μ_2	μ_2	μ_1	ρ_2	ρ_0

September 16, 2020, in advance

Notation that is standard and in the book: if H is a subgroup of G, we often write $H \leq G$ or $G \geq H$, with $H < G$ and $G > H$ meaning that H is a subgroup of G and $H \neq G$.

I'd like to return to cosets, in general. There will be examples later. Once again, recall the definition: Suppose H is a subgroup of G and $g \in G$ (not necessarily in H). The left coset gH and the right coset Hg are defined by

$$gH = \{gh \mid h \in H\}, \quad Hg = \{hg \mid h \in H\}.$$

Before we prove some important results about them, I'd like to give an example involving infinite groups that shows we've already been working with cosets.

Consider the group $(\mathbb{Z}, +)$; that is, the integers under addition. We have already seen that this is a group: 0 is the identity $-n$ is the inverse of $n \in \mathbb{Z}$ and ordinary addition is associative. Suppose $d \in \mathbb{N}$, so $d \geq 1$. Then we saw early on

$$d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\} = \{\dots, -3d, -2d, -d, 0, d, 2d, 3d, \dots\}$$

is a group with the same identity and inverses, and as strange as it may look, $\mathbb{Z} \geq d\mathbb{Z}$. What are the cosets of $d\mathbb{Z} \in \mathbb{Z}$? Since the operation is addition, a typical coset is

$$a + d\mathbb{Z} = \{\dots, a - 3d, a - 2d, a - d, a, a + d, a + 2d, a + 3d, \dots\}.$$

We've seen this before: $x \in a + d\mathbb{Z} \iff x \equiv a \mod d$. In other words $a + d\mathbb{Z} = [a]_d$, and these are the cosets of $d\mathbb{Z} \subset \mathbb{Z}$.

LEMMA If $G \geq H$ and H is a finite group, then for every $g \in G$, we have $|H| = |gH| = |Hg|$; that is, every left and right coset has the same number of elements as H.

PROOF Suppose $H = \{h_1, \ldots, h_m\}$. Then $gH = \{gh_1, \ldots, gh_m\}$, so the statement is true provided $h_i \neq h_j \implies gh_i \neq gh_j$. But the contrapositive of that statement is $gh_i = gh_j \implies h_i = h_j$, which we know to be true upon multiplication of both sides by g^{-1}. The same argument works for Hg. □

The next result is sort of surprising and really important.

THEOREM If $G \geq H$ and xH and yH are two left cosets, then either $xH = yH$ as sets, or xH and yH are disjoint; that is, $xH \cap yH = \emptyset$. Furthermore, $xH = yH$ if and only if $x = yh, y = xh'$ for some $h, h' \in H$. The same thing holds for right cosets. The same thing holds for right cosets, with the last condition changed to $x = hy, y = h'x$.

PROOF. Suppose $z \in xH \cap yH$, so the intersection is not empty. By definition, this means that there exist $h_1, h_2 \in H$ so that

$$z = xh_1 = yh_2 \implies x = yh_2h_1^{-1}.$$

Since H is a subgroup, $h_2h_1^{-1} \in H$. Suppose now that $u \in xH$. Then for some $h \in H$,

$$u = xh = (yh_2h_1^{-1})h = y(h_2h_1^{-1}h)$$

and, again, H is a subgroup, so $h_2h_1^{-1}h \in H$. This implies that $u \in yH$. Thus $xH \subseteq yH$.

But also $y = xh_1h_2^{-1}$, so an almost identical argument shows that $yH \subseteq xH$, and so $xH = yH$.

We have seen that if $x = yh$ or $y = xh'$, then $xH = yH$. The converse is easier: if $xH = yH$, then $x \in xH \implies x \in yH \implies x = yh, y = xh^{-1}$ f or some $h \in H$.

The identical argument (up to the order in which you write elements) applies to right cosets. □

COROLLARY If $G \geq H$, then we may write G as a union of disjoint cosets of H.

PROOF Observe that $x \in G$, $e \in H$ (because it's a group) imply that $x = xe \in xH$. Thus, every $x \in G$ belongs to some coset, so

$$G = \bigcup_{x \in G} xH.$$

Delete duplicate cosets, so the remaining ones are disjoint. □.

For example, if, say $d = 3$, then

$$\mathbb{Z} = (0 + 3\mathbb{Z}) \cup (1 + 3\mathbb{Z}) \cup (2 + 3\mathbb{Z}) = [0]_3 \cup [1]_3 \cup [2]_3.$$

For the rest of today, I will assume that G is a finite group. It makes sense to define $[G : H]_L$ – the number of distinct left cosets of H in G and $[G : H]_R$ – the number of distinct right cosets of H in G. Don't get too attached to the subscripts!

We've seen examples of this earlier. If $G = C_6 = \langle a \rangle, a^6 = e$, then as we have already seen, G has four subgroups: $H_1 = \{e\}$, $H_2 = \{e, a^3\}$, $H_3 = \{e, a^2, a^4\}$ and G itself, and we have seen that

$$[G : H_1]_L = [G : H_1]_R = 6, \quad [G : H_2]_L = [G : H_2]_R = 3$$
$$[G : H_3]_L = [G : H_3]_R = 2, \quad [G : G]_L = [G : G]_R = 1.$$

The pattern isn't an accident. The following was the first major theorem in the subject.

LAGRANGE'S THEOREM If G is a finite group and $G \geq H$, then

$$[G : H]_L = [G : H]_R = \frac{|G|}{|H|}.$$

In particular, $|H|$ is a divisor of $|G|$.

We have already seen this in the special case of the cyclic group. PROOF. Suppose that $|G| = n$ and $H = \{h_1, \ldots, h_m\}$ and $[G : H]_L = r$. Write down G as a union of the distinct cosets of H: a_1H, $\ldots$, a_rH.

$$a_1H = \{a_1h_1, \ldots a_1h_m\}$$
$$a_2H = \{a_2h_1, \ldots a_2h_m\}$$
$$\ldots$$
$$a_rH = \{a_rh_1, \ldots a_rh_m\}.$$

Now count elements.

$$G = \bigcup_{k=1}^{r} a_kH = \{a_1h_1, \ldots a_1h_m, a_2h_1, \ldots a_2h_m \ldots, a_rh_1, \ldots a_rh_m\}$$

There are n elements in G and $r \cdot m = [G : H]_L \cdot |H|$ elements on the right hand side, so $|G| = [G : H]_L \cdot |H|$. The exact same argument would work with right cosets as well, so $|G| = [G : H]_R \cdot |H|$, hence $[G : H]_L = [G : H]_R$ and we get the desired formula. $\square$.

We now define $[G : H] = [G : H]_L = [G : H]_R$.

COROLLARY Suppose G is a finite group with $|G| = n$ and suppose $x \in G$. Then the order of x is a divisor of n.

PROOF Consider the subgroup $\langle x \rangle = \{e, x, \ldots, x^{d-1}\}$ of G, where $x^d = e$. Then the order of x is d, which is the size of the subgroup $\langle x \rangle$, and by LaGrange, $d \mid n$.

COROLLARY If G is a finite group and $|G| = p$ is prime, then G is a cyclic group of order p, and every non-identity element is a generator.

PROOF Suppose $x \in G, x \neq e$. Then $x^1 \neq e$, so d, the order of x, is ≥ 2. But $d \mid p$ and p is prime, so $d = p$. That is, x has order p, so $\{e, x, \ldots, x^{p-1}\}$ are all distinct, and they constitute all of G. □

COROLLARY If $G > H$, and $[G : H] = 2$, then the cosets of H (left or right) are H and $G \setminus H$, the elements of G which are not in H.

PROOF The coset associated with e is $eH = He = H$, so we may take one of the left (or right) cosets to be H, so

$$G = H \cup aH; \qquad G = H \cup Hb$$

for some $a, b \in G$. But these are disjoint unions, so aH (and Hb) consist of the elements in G which are not in H,

Well this might seem very abstract, so let's look at the cosets of the subgroups of S_3. I'll cut and paste the multiplication table again.

$$\rho_0 = \begin{pmatrix}123\\123\end{pmatrix} = (1)(2)(3), \quad \rho_1 = \begin{pmatrix}123\\231\end{pmatrix} = (123),$$
$$\rho_2 = \begin{pmatrix}123\\312\end{pmatrix} = (132), \quad \mu_1 = \begin{pmatrix}123\\132\end{pmatrix} = (1)(23),$$
$$\mu_2 = \begin{pmatrix}123\\321\end{pmatrix} = (13)(2), \quad \mu_3 = \begin{pmatrix}123\\213\end{pmatrix} = (12)(3).$$

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

We have already seen that the subgroups of S_3 are the trivial ones ($\{\rho_0\}$, S_3), plus $\{\rho_0, \rho_1, \rho_2\}$ and $\{\rho_0, \mu_1\}$, $\{\rho_0, \mu_2\}$, $\{\rho_0, \mu_3\}$.

First let $H = \{\rho_0, \rho_1, \rho_2\}$. Then $|H| = 3$ and $|S_3| = 6$, so $[S_3 : H] = 2$ and the corollary applies, so the other coset has to be $S_3 \setminus H$; that is, $\{\mu_1, \mu_2, \mu_3\}$. Let's check:

$$\mu_1 H = \{\mu_1\rho_0, \mu_1\rho_1, \mu_1\rho_2\} = \{\mu_1, \mu_2, \mu_3\}$$
$$H\mu_1 = \{\rho_0\mu_1, \rho_1\mu_1, \rho_2\mu_1\} = \{\mu_1, \mu_3, \mu_2\}$$

Now let $K = \{\rho_0, \mu_1\}$; recall $\rho_0 = (1)(2)(3)$ and $\mu_1 = (1)(23)$. So one left coset is $\rho_0 K = K$. How to we find another left coset? Well $e \in H$ in general, so $x \in xH$. Find an element that isn't used yet. How

about μ_2:

$$\begin{aligned}\mu_2 K = \{\mu_2\rho_0, \mu_2\mu_1\} &= \{(13)(2)(1)(2)(3), (13)(2)(1)(23)\} \\ &= \{(13)(2), (132)\} = \{\mu_2, \rho_2\}.\end{aligned}$$

What's not here yet?: μ_3, ρ_1, and it's a good guess that this is the last left coset, but let's check:

$$\begin{aligned}\rho_1 K = \{\rho_1\rho_0, \rho_1\mu_1\} &= \{(123)(1)(2)(3), (123)(1)(23)\} \\ &= \{(123), (12)(3)\} = \{\rho_1, \mu_3\}.\end{aligned}$$

So the left cosets of K are:

$$\{\rho_0, \mu_1\}, \{\mu_2, \rho_2\}, \{\rho_1, \mu_3\}$$

Let's do the right cosets as well. One right coset is $K\rho_0 = K$. Now, ρ_1 hasn't appeared yet, so let's look for $K\rho_1$.

Important note: there are four elements you could have picked here, and any one of them is a valid choice.

$$\begin{aligned}K\rho_1 = \{\rho_0\rho_1, \mu_1\rho_1\} &= \{(1)(2)(3)(123), (1)(23)(123)\} \\ &= \{(123), (13)(2)\} = \{\rho_1, \mu_2\}.\end{aligned}$$

The two elements not accounted for are ρ_2 and μ_3, and

$$\begin{aligned}K\rho_2 = \{\rho_0\rho_2, \mu_1\rho_2\} &= \{(1)(2)(3)(132), (1)(23)(132)\} \\ &= \{(132), (12)(3)\} = \{\rho_2, \mu_3\}.\end{aligned}$$

So the right cosets of K are

$$\{\rho_0, \mu_1\}, \{\rho_1, \mu_2\}, \{\rho_2, \mu_3\}$$

while the left cosets are

$$\{\rho_0, \mu_1\}, \{\mu_2, \rho_2\}, \{\rho_1, \mu_3\}$$

These aren't the same. Except for K, there are lots of partial overlaps.

I hope you paid attention to the logic here. One worksheet exercise on Wednesday will be to do the same thing with the group $L = \{\rho_0, \mu_2\}$.

I'd like to return to D_4, and talk briefly about subgroups, even before we have worked out all of the multiplication table. Here are the

elements:

$$\rho_0 = \begin{pmatrix}1234\\1234\end{pmatrix} = (1)(2)(3)(4) \quad \rho_1 = \begin{pmatrix}1234\\2341\end{pmatrix} = (1234),$$
$$\rho_2 = \begin{pmatrix}1234\\3412\end{pmatrix} = (13)(24) \quad \rho_3 = \begin{pmatrix}1234\\4123\end{pmatrix} = (1432),$$
$$\mu_1 = \begin{pmatrix}1234\\2143\end{pmatrix} = (12)(34), \quad \mu_2 = \begin{pmatrix}1234\\4321\end{pmatrix} = (14)(23),$$
$$\delta_1 = \begin{pmatrix}1234\\3214\end{pmatrix} = (13)(2)(4), \quad \delta_2 = \begin{pmatrix}1234\\1432\end{pmatrix} = (1)(24)(3).$$

This is a group and $|D_4| = 8$, so by LaGrange's Theorem, all subgroups have order dividing 8, and the proper subgroups have order 2 or 4.

We can first list the cyclic groups generated by the elements (I'll ignore the identity ρ_0.) We have a cyclic subgroup of order 4, since $\rho_k = \rho_1^k$, and a bunch a cyclic subgroups of order 2.

$$\langle \rho_1 \rangle = \langle \rho_3 \rangle = \{\rho_0, \rho_1, \rho_2, \rho_3\},$$
$$\langle \rho_2 \rangle = \{\rho_0, \rho_2\},$$
$$\langle \mu_1 \rangle = \{\rho_0, \mu_1\}, \qquad \langle \mu_2 \rangle = \{\rho_0, \mu_2\},$$
$$\langle \delta_1 \rangle = \{\rho_0, \delta_1\}, \qquad \langle \delta_2 \rangle = \{\rho_0, \delta_2\}.$$

If H is a subgroup and $\rho_1 \in H$, then $\langle \rho_1 \rangle \subset H$, and that's already four elements, so if H has any more elements, then $|H| \geq 5$. Thus $H = D_4$. In other words, no other proper subgroup can contain ρ_1, and the same for ρ_3.

If a subgroup is not $\langle a \rangle$, then it has to have more than two elements, and so it has exactly four, the identity ρ_0 and three chosen from $\{\rho_2, \mu_1, \mu_2, \delta_1, \delta_2\}$.

We saw in Monday's worksheet that $\{\rho_0, \rho_2, \mu_1, \mu_2\}$ is a subgroup. It will turn out that $\{\rho_0, \rho_2, \delta_1, \delta_2\}$ is also a subgroup, but that's the only other one. Its table looks remarkably similar.

As a reminder,

$$\rho_0 = \begin{pmatrix}1234\\1234\end{pmatrix} = (1)(2)(3)(4), \quad \rho_2 = \begin{pmatrix}1234\\3412\end{pmatrix} = (13)(24),$$
$$\delta_1 = \begin{pmatrix}1234\\3214\end{pmatrix} = (13)(2)(4), \quad \delta_2 = \begin{pmatrix}1234\\1432\end{pmatrix} = (1)(24)(3).$$

It is very easy to check that $\rho_2\delta_1 = \delta_1\rho_2 = \delta_2$, etc, and we get another copy of the Klein 4 group.

H	ρ_0	ρ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_2	δ_1	δ_2
ρ_2	ρ_2	ρ_0	δ_2	δ_1
δ_1	δ_1	δ_2	ρ_0	ρ_2
δ_2	δ_2	δ_1	ρ_2	ρ_0

Finally, suppose H is a subgroup of D_4 and H has both a μ and a δ:

$$\mu_1 = \begin{pmatrix}1234\\2143\end{pmatrix} = (12)(34), \quad \mu_2 = \begin{pmatrix}1234\\4321\end{pmatrix} = (14)(23),$$

$$\delta_1 = \begin{pmatrix}1234\\3214\end{pmatrix} = (13)(2)(4), \quad \delta_2 = \begin{pmatrix}1234\\1432\end{pmatrix} = (1)(24)(3).$$

It's not hard to see that

$$\mu_1\delta_1 = \begin{pmatrix}1234\\4123\end{pmatrix} = \rho_3$$

$$\mu_1\delta_2 = \begin{pmatrix}1234\\2341\end{pmatrix} = \rho_1$$

$$\mu_2\delta_1 = \begin{pmatrix}1234\\2341\end{pmatrix} = \rho_1$$

$$\mu_2\delta_2 = \begin{pmatrix}1234\\4123\end{pmatrix} = \rho_3.$$

Thus, any subgroup that contains μ_i and δ_j is forced to contain ρ_1 or ρ_3, and so is all of D_4.

September 16, 2020, in class

I have gotten several useful emails suggesting that I review some of the ideas of the last lecture. Suppose, for the moment, that G is a finite group. (Most of what I say still applies when it's infinite, but this will allow us to count.)

Suppose $G > H$ so H is a subgroup of G. We can look at the cosets, which come in two flavors, the left cosets gH and the right cosets Hg. Basically everything we can prove about left cosets can also be proved about right cosets. Some facts:

(i) G can be written as a union of left cosets which are disjoint. The number of cosets, $r = [G : H]$, is equal to $|G|/|H|$.

$$G = a_1H \cup \cdots \cup a_rH; \quad i \neq j \implies a_iH \cap a_jH = \emptyset.$$

(You can do the same thing with right cosets.) Two left cosets are disjoint, because $z \in xH \cap yH \implies xH = yH$.

(ii) Are cosets subgroups? Well, $eH = H$ is a subgroup, and it contains e. The other cosets can't contain the identity, and so they can't be subgroups.

(iii) When G is not abelian, it is possible for the left cosets and the right cosets to have different arrangements of the elements of G. If H is a special kind of subgroup, then $gH = Hg$ *as sets*, for every $g \in G$. Ironically, this special kind of subgroup is called a *normal* subgroup. Every subgroup of an abelian group is normal. If $[G : H] = 2$, then H turns out to be normal. We'll see, soon but not today, that $\{\rho_0, \rho_2\}$ is a normal subgroup of D_4.

(iv) How do we find all the cosets? One way is to take gH for every element $g \in G$, and eventually you get them all. As a shortcut, once we start with $eH = H$, we pick any $x \in G \setminus H$. We know that x has to be in a coset and it's in xH, so construct xH. If we're done, we're done. If not, look at $G \setminus (H \cup xH)$ to find elements we are still missing, etc.

(v) Here's an example. Look at $C_8 = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7\}$, with $H = \{e, a^4\}$.

The theorem tells us that C_8 can be written as a union of disjoint cosets. Let's say my favorite element is a^5. I don't see it in a coset yet, so look at $a^5H = \{a^5 * e, a^5 * a^4\} = \{a^5, a^9\} = \{a^5, a\}$.

Now I have $H \cup a^5H = \{e, a^4\} \cup \{a^5, a\}$. What's missing? Well, there are four choices: a^2, a^3, a^6, a^7. Pick one, say a^7, and look at its coset: $a^7H = \{a^7 * e, a^7 * a^4\} = \{a^7, a^{11}\} = \{a^7, a^3\}$.

And $H \cup a^5H \cup a^7H = \{e, a^4\} \cup \{a^5, a\} \cup \{a^7, a^3\}$. What's missing? Only a^2, a^6, and $a^2H = \{a^2 * e, a^2 * a^4\} = \{a^2, a^6\}$. We're done.

$$G = H \cup a^5H \cup a^7H \cup a^2H = \{e, a^4\} \cup \{a^5, a\} \cup \{a^7, a^3\} \cup \{a^2, a^6\}.$$

The order of the cosets and the order of elements in the coset don't matter: as sets $\{a^5, a\} = \{a, a^5\}$, etc.

(vi) If we are looking for subgroups of G, the first step is to look at $\langle g \rangle$ for every $g \in G$. When G is a cyclic group, these are all the subgroups we find. This was also true for S_3, but not D_4. We can use Lagrange's Theorem to look at the size of the potential group.

I want to use Lagrange's Theorem to finish the description of groups of order 6.

What we did the other day was this: Suppose G is a group of order 6 with an element a so that $\{e, a, a^2\}$ are distinct and $a^3 = e$. Suppose b is another element of G and $b^2 = e$. We saw that either $ba = a^2b$ (and G is isomorphic to S_3) or $ba = ab$, (and G is isomorphic to C_6).

Today I'll make no hypotheses on G, except that $|G| = 6$, and show that these are the only possible groups.

Suppose $x \in G$, then the order of x is 1, 2, 3, 6. First suppose there exists $x \in G$ so that x has order 6. Then $\{e, x, x^2, x^3, x^4x^5\}$ are

distinct, $x^6 = e$, so G is a cyclic group of order 6. Henceforth, we can otherwise assume that there is no element in G of order 6.

We first need a simple result often assigned as a homework problem, even though the proof is not-conceptual, and a bizarre computation.

LEMMA If $g \in G \implies g^2 = e$ in a group G, then G is abelian.

PROOF We need to show that $a, b \in G \implies ab = ba$. There's a trick. Since $ab \in G$, $(ab)^2 = e$. Write this out as $abab = a(ba)b = e$. We also know that $a^2 = e$ and $b^2 = e$, so we have this chain of identities, multiplying by a on the left and b on the right:

$$(ab)^2 = a(ba)b = e \implies$$
$$a^2(ba)b = ae \implies bab = a \implies$$
$$bab^2 = ab \implies ba = ab.$$

Suppose now that G is a group of order 6 and G has no element of order 3 or order 6. I'll show that this is impossible.

If $x \in G$ and $x \neq e$, then x must have order 2. Pick such an x. G has 6 elements and $\{e, x\}$ only gives 2, so there has to be another element in G, call it y, so e, x, y are all different. What about xy? If $xy = e$, then $xy = x^2 \implies y = x$. If $xy = x = xe$, then $y = e$. If $xy = y = ey$, then $x = e$. These impossibilities say that $H = \{e, x, y, xy\}$ are all distinct. Look at the multiplication table for H. We know that $x^2 = y^2 = (xy)^2 = e$ and, say $y(xy) = (yx)y = (xy)y = xy^2 = x$. We can fill out the table completely.

H	e	x	y	xy
e	e	x	y	xy
x	x	e	xy	y
y	y	xy	e	x
xy	xy	y	x	e

Another copy of the Klein 4 group!

What could be wrong with that? Well, H is a subset of G and H is a group, so it's a subgroup of G, and $|H| = 4$, $|G| = 6$ and 4 doesn't divide 6.

What does this mean? It means that our assumption that there were *no* elements of order three leads to a contradiction, so suppose $a \in G$ and a has order 3, $\{e, a, a^2\}$ are in G, and let b be another element of G. Then ab, a^2b have to be in G, because it's closed under multiplication, and we've already shown that $\{e, a, a^2, b, ab, a^2b\}$ are all different.

But now we know something more: we know that $b^2 = e$ or $b^3 = e$. We did the work a few days ago to handle the case $b^2 = e$. Now suppose $b^3 = e$. I won't need to worry about ba.

Here is the multiplication table

G	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	?	?	?	?	?
ab	ab	?	?	?	?	?
a^2b	a^2b	?	?	?	?	?

It's not clear what b^2 is: from looking at the column, it might be e, a, a^2. We've already talked about $b^2 = e$, so consider $b^2 = a$ or $b^2 = a^2$. Now, multiplying on the right by b, these imply $b^3 = ab$ or $b^3 - a^2b$. Neither of these is e, so this case is a dead end too, and we've run out of cases.

THEOREM If G is a group and $|G| = 6$, then G is either isomorphic to C_6 or isomorphic to S_3.

Since 2,3,5,7 are prime, any group with those orders must be cyclic. We've also completely analyzed groups of order 4 and order 6. It turns out that there are five different groups of order 8: we've already seen three of them: C_8, D_4, and $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z})$. We'll see the other two eventually.

The number of non-isomorphic groups of a given order can get very large, especially when the order is a power of a prime.

There are 14 non-isomorphic groups of order $16 = 2^4$, 267 non-isomorphic groups of order $64 = 2^6$, 56092 non-isomorphic groups of order $256 = 2^8$ and 4948736522 non-isomorphic groups of order $1024 = 2^{10}$.

In fact 99.15% of all the groups of order < 2000 have order 1024.

WORKSHEET PROBLEM Recall S_3.

$$\rho_0 = \begin{pmatrix}123\\123\end{pmatrix} = (1)(2)(3), \quad \rho_1 = \begin{pmatrix}123\\231\end{pmatrix} = (123),$$

$$\rho_2 = \begin{pmatrix}123\\312\end{pmatrix} = (132), \quad \mu_1 = \begin{pmatrix}123\\132\end{pmatrix} = (1)(23),$$

$$\mu_2 = \begin{pmatrix}123\\321\end{pmatrix} = (13)(2), \quad \mu_3 = \begin{pmatrix}123\\213\end{pmatrix} = (12)(3).$$

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

As promised, find the left cosets and the right cosets for the subgroup $L = \{\rho_0, \mu_2\}$.

WORKSHEET SOLUTION

First the left cosets. As always, $L = L\rho_0 = \{\rho_0, \mu_2\}$ is one of the cosets. I don't see ρ_1 so I'll look at

$$\rho_1 L = \{\rho_1\rho_0, \rho_1\mu_2\} = \{\rho_1, \mu_1\}.$$

I don't see ρ_2, so I'll take that:

$$\rho_2 L = \{\rho_2\rho_0, \rho_2\mu_2\} = \{\rho_2, \mu_3\}.$$

So the left cosets are

$$\{\rho_0, \mu_2\}, \quad \{\rho_1, \mu_1\}, \quad \{\rho_2, \mu_3\}.$$

You could have taken other missing elements, but you should wind up with the same cosets.

Now the right cosets. As always, $L = L\rho_0 = \{\rho_0, \mu_2\}$ is one of the cosets. I don't see ρ_1 so I'll look at

$$L\rho_1 = \{\rho_0\rho_1, \mu_2\rho_1\} = \{\rho_1, \mu_3\}.$$

I don't see ρ_2, so I'll take that:

$$L\rho_2 = \{\rho_0\rho_2, \mu_2\rho_2\} = \{\rho_2, \mu_1\}.$$

So the right cosets are

$$\{\rho_0, \mu_2\}, \quad \{\rho_1, \mu_3\}, \quad \{\rho_2, \mu_1\}.$$

Again, a partial overlap of the left cosets and the right cosets.

September 18, 2020, in advance

Biography of Lagrange was found at

https://mathshistory.st-andrews.ac.uk/Biographies/Lagrange/

Now I'd like to return to the group D_4, and construct its multiplication table with a hybrid approach. Recall the elements:

$$\rho_0 = \begin{pmatrix}1234\\1234\end{pmatrix} = (1)(2)(3)(4), \quad \rho_1 = \begin{pmatrix}1234\\2341\end{pmatrix} = (1234),$$

$$\rho_2 = \begin{pmatrix}1234\\3412\end{pmatrix} = (13)(24), \quad \rho_3 = \begin{pmatrix}1234\\4123\end{pmatrix} = (1432),$$

$$\mu_1 = \begin{pmatrix}1234\\2143\end{pmatrix} = (12)(34), \quad \mu_2 = \begin{pmatrix}1234\\4321\end{pmatrix} = (14)(23),$$

$$\delta_1 = \begin{pmatrix}1234\\3214\end{pmatrix} = (13)(2)(4), \quad \delta_2 = \begin{pmatrix}1234\\1432\end{pmatrix} = (1)(24)(3).$$

I will let $e = \rho_0$, and if $a = \rho_1$, then $a^2 = \rho_1^2 = \rho_2$ and $a^3 = \rho_1^3 = \rho_3$. Sort of arbitrarily (I have four choices), I will let $b = \mu_1$, so $b^2 = e$. It follows that

$$ab = \rho_1\mu_1 = \begin{pmatrix}1234\\2341\end{pmatrix}\begin{pmatrix}1234\\2143\end{pmatrix} = \begin{pmatrix}1234\\3214\end{pmatrix} = (13)(2)(4) = \delta_1,$$

$$a^2b = \rho_2\mu_1 = \begin{pmatrix}1234\\3412\end{pmatrix}\begin{pmatrix}1234\\2143\end{pmatrix} = \begin{pmatrix}1234\\4321\end{pmatrix} = (14)(23) = \mu_2,$$

$$a^3b = \rho_3\mu_1 = \begin{pmatrix}1234\\4123\end{pmatrix}\begin{pmatrix}1234\\2143\end{pmatrix} = \begin{pmatrix}1234\\1434\end{pmatrix} = (1)(24)(3) = \delta_2.$$

So all of the elements of the group are now accounted for. They are $\{a^jb^k \ : \ 0 \le j \le 3, 0 \le k \le 1\}$. What is ba?

$$ba = \mu_1\rho_1 = \begin{pmatrix}1234\\2143\end{pmatrix}\begin{pmatrix}1234\\2341\end{pmatrix} = \begin{pmatrix}1234\\1432\end{pmatrix} = (1)(24)(3) = \delta_2 = a^3b$$

This is the key, and I'll summarize:

$$a^4 = e, \qquad b^2 = e, \qquad ba = a^3b = a^{-1}b.$$

This will actually be enough information to finish the multiplication table. Let me first derive two other useful facts:

$$ba^2 = (ba)a = (a^3b)a = a^3(ba) = a^3(a^3b) = a^6b = a^2b$$
$$ba^3 = (ba^2)a = (a^2b)a = a^2(ba) = a^2(a^3b) = a^5b = ab.$$

To put this all together,

$$ba^j = a^{3j}b = a^{-j}b.$$

The elements of D_4 come in two flavors: a^i and a^ib, where $i \in \{0, 1, 2, 3\}$, and so there are four types of multiplications we need to compute. Two are immediate:

$$(a^i)(a^j) = a^{i+j}, \qquad (a^i)(a^jb) = a^{i+j}b.$$

The third is the trickiest, but once done, makes the fourth easy:

$$(a^ib)(a^j) = (a^i)(ba^j) = (a^i)(a^{-j}b) = a^{i-j}b,$$
$$(a^ib)(a^jb) = ((a^ib)(a^j)) * b = (a^{i-j}b)b = a^{i-j}b^2 = a^{i-j}.$$

How can we use this? Using the permutations, we found that $\mu_1 \circ \delta_1 = \rho_3$, This translates to

$$b(ab) = (a^0b)(a^1b) = a^{0-1} = a^3 = \rho_3.$$

All the others can be found this way too, and we get this huge table:

D_4	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Remember that

$$(e, a, a^2, a^3, b, ab, a^2b, a^3b) = (\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \delta_1, \mu_2, \delta_2).$$

In translating the table. It is actually illuminating of the structure to reorder the elements

$$(e, a^2, a, a^3, b, a^2b, ab, a^3b) = (\rho_0, \rho_2, \rho_1, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2),$$

which I will give in both forms.

D_4	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a^2	a	a^3	b	a^2b	ab	a^3b
a^2	a^2	e	a^3	a	a^2b	b	a^3b	ab
a	a	a^3	a^2	e	ab	a^3b	a^2b	b
a^3	a^3	a	e	a^2	a^3b	ab	b	a^2b
b	b	a^2b	a^3b	ab	e	a^2	a^3	a
a^2b	a^2b	b	ab	a^3b	a^2	e	a	a^3
ab	ab	a^3b	b	a^2b	a	a^3	e	a^2
a^3b	a^3b	ab	a^2b	b	a^3	a	a^2	e

Look at the patterns of the 2×2 squares! This table looks like a 4×4 array, each of whose elements is a 2×2 square.

If you assigned names to the 2×2 squares of I, X, Y, Z, you'd find that you had reproduced the multiplication table of V. This is not an accident, but the full explanation will have to wait a few weeks.

D_4	ρ_0	ρ_2	ρ_1	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_2	ρ_1	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_2	ρ_2	ρ_0	ρ_3	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_1	ρ_1	ρ_3	ρ_2	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_3	ρ_3	ρ_1	ρ_0	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	μ_2	δ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	μ_1	δ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	δ_2	μ_1	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	δ_1	μ_2	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

Two more thing about this nice pattern. By looking at the second row and second column, we see that ρ_2 commutes with every element: $g\rho_2 = \rho_2 g$. This means that the left cosets and the right cosets are the same. By looking at the first two columns, we can read off the left cosets of the subgroup $\{\rho_0, \rho_2\}$. Each one appears twice and these are:

$$\{\rho_0, \rho_2\}, \quad \{\rho_1, \rho_3\}, \quad \{\mu_1, \mu_2\}, \quad \{\delta_1, \delta_2\}$$

And by looking at the first two rows, we can read off the right cosets of the subgroup $\{\rho_0, \rho_2\}$. They are the same.

How special is ρ_2? It's easiest to do this with the "abstract" formulation and ask: when does $xy = yx$ for $x, y \in D_4$? We had these four rules:

$$a^i a^j = a^{i+j},\ a^i(a^j b) = a^{i+j}b,\ (a^i b)a^j = a^{i-jb},\ (a^i b)(a^j b) = a^{i-j}.$$

In the first case, clearly $a^i a^j = a^j a^i$. This is true for all i, j, and this is reasonable, because there are elements of $\langle a \rangle$: the ρ_j's commute with each other.

A trickier one is

$$(a^i b)a^j = a^j(a^i b) \implies a^{i-j}b = a^{i+j}b \implies a^{i-j} = a^{i+j} \implies e = a^{2j}.$$

The last condition holds if $4 \mid 2j \iff (2j)/4 \in \mathbb{Z} \iff j/2 \in \mathbb{Z}$; that is, $j \equiv 0 \mod 2$. So e and a^2 commute with every $a^i b$; that is, ρ_0 and ρ_2 commute with every flip μ_j, δ_j. Finally,

$$(a^i b)(a^j b) = (a^j b)(a^i b) \implies a^{i-j} = a^{j-i}b \implies e = a^{2j-2i}.$$

Similarly to above, this happens if and only if $j \equiv i \mod 2$; that is, they are both even (and $a^i b, a^j b$ are both μ_j's), or they are both odd (and $a^i b, a^j b$ are both δ_j's). As we have seen, two μ_j's commute with each other and two δ_j's commute with each other, but not a μ_j and a δ_j.

I'd also like to talk about Cayley's Theorem. First, a few minutes on Cayley, found at https://mathshistory.st-andrews.ac.uk/Biographies/Cayley/ .

Cayley's Theorem is one of the early theorems in group theory. If G is a finite group and $|G| = n$, then G is isomorphic to a subgroup of S_n. For example, C_4 and V have 4 elements and are isomorphic to subgroups of S_4, which have 24 elements, and D_4 has 8 elements, and is isomorphic to a subgroup of S_8, which has $8! = 40320$ elements.

The idea is very simple. Look at the rows of the multiplication table as permutations of the elements themselves. Consider C_4, with the elements $\{e, a, a^2, a^3\}$ renamed as x_1, x_2, x_3, x_4

C_4	x_1	x_2	x_3	x_4
x_1	x_1	x_2	x_3	x_4
x_2	x_2	x_3	x_4	x_1
x_3	x_3	x_4	x_1	x_2
x_4	x_4	x_1	x_2	x_3

Look at the first row as the permutation $\binom{1234}{1234}$, the second row as $\binom{1234}{2341}$, the third row as $\binom{1234}{3412}$, and the fourth row as $\binom{1234}{4123}$. These happen to be ρ_0, ρ_1, ρ_2, ρ_3 from D_4, which form a cyclic group of order 4 with generator ρ_i. So a map which takes x_i to the permutation from the i-th row is an isomorphism.

We can do the same thing with V, again naming the elements x_1, x_2, x_3, x_4:

V	x_1	x_2	x_3	x_4
x_1	x_1	x_2	x_3	x_4
x_2	x_2	x_1	x_4	x_3
x_3	x_3	x_4	x_1	x_2
x_4	x_4	x_3	x_2	x_1

Now the permutations are (1)(2)(3)(4), (12)(34), (13)(24), (14)(23), and these are also elements of D_4: $\rho_1, \mu_1, \rho_2, \mu_2$, and these we've seen, form a group, isomorphic to ... D_4.

This is the pattern in general.

I should warn you that the notation may become a bit complicated at times, but it makes sense. We are only doing what the mathematical definitions require us to do.

Let $G = \{g_1, \ldots, g_n\}$ be a group with identity $g_1 = e$. We know that $g_i g_j \in G$, so $g_i g_j = g_k$ for some k. We define the permutation $\pi_i \in S_n$ by:

$$g_i g_j = g_{\pi_i(j)}.$$

We've already seen these permutations: this is the permutation you get from the i-th row of the multiplication table.

For example, in the cyclic group of order 4, with elements g_1, g_2, g_3, g_4, we had that $g_1 g_j = g_j$ (because g_1 is the identity) and $g_2 g_j = g_{j+1}$ (with $g_5 = g_1$), so $\pi_1(j) = j$ and $\pi_2(j) = j + 1$, and $\pi_2(4) = 1$; that is,

$$\pi_1 = \binom{1234}{1234} = (1)(2)(3)(4), \quad \pi_2 = \binom{1234}{2341} = (1234).$$

Finally, let

$$H_G = \{\pi_1, \pi_2, \ldots, \pi_n\} \subset S_n$$

be the set of all permutations that appear in this way

CAYLEY'S THEOREM The group G is isomorphic to H_G.

PROOF. Define the isomorphism Φ by

$$\Phi(g_i) = \pi_i.$$

By definition, Φ is onto. Is it injective? Well,

$$\pi_i = \pi_j \implies \pi_i(k) = \pi_j(k) \implies g_{\pi_i(k)} = g_{\pi_j(k)} \iff g_i g_k = g_j g_k \iff g_i = g_j.$$

So, yes, it's injective. The crucial question is: does it preserve the operation? Suppose $g_i g_j = g_k$, so that $\pi_i(j) = k$. What is $\Phi(g_i g_j)$? For any m,

$$\Phi(g_i g_j)(m) = \pi_k(m) \implies g_k g_m = g_{\pi_k(m)}.$$

But

$$g_k g_m = (g_i g_j) g_m = g_i(g_j g_m) = g_i(g_{\pi_j(m)}) = g_{\pi_i(\pi_j(m))},$$

So

$$g_{\pi_i(\pi_j(m))} = g_{\pi_k(m)} \implies \pi_i(\pi_j(m)) = \pi_k(m),$$

for all m, so $\pi_i \pi_j = \pi_k$. In other words,

$$\Phi(g_i g_j) = \Phi(g_k) = \pi_k = \pi_i \pi_j = \Phi(g_i)\Phi(g_j)$$

and we are done, except that we haven't proved that H_G is a group.

But, look, we've seen that it's closed under multiplication. If $g_1 = e$, then $e * g_j = g_j$, so $\pi_1(j) = j$; that is, π_1 is the identity permutation, so H_G contains the identity. If $\pi_i \in H_G$ and $g_i^{-1} = g_\ell$, then $g_i g_\ell = g_1 = e$ and so $\pi_i \pi_\ell = \pi_1$; in other words, $(\pi_i)^{-1} = \pi_\ell$. Since $H_G \subset S_n$, associativity is automatic. □

September 18, 2020, in class

No slides.