Math 417 – Ninth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 14, 2020

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

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

$$\rho_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (132), \quad \mu_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (1)(23),$$

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

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 $a^2 b$.

If you look at the table for S_3, you'll see that ab should be μ_2 and $a^2 b$ 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 $a^i b = a^j b$, then you can multiply on the right by b (always assume associativity).

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

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

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

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

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

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

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

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

I'll put this entry in now (in red)

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. I'll do it slowly at first.

We need to find ba^2, bab and ba^2b as elements of the group.

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

This information now becomes

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 $a^i b$.

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

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

$$a^i b * e = a^i b$$

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

$$a^i b * a^2 = a^i(ba)a = a^i(a^2 b)a =$$

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

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

The succinct version of this is

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

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 $ba = a^2 b$. 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	$a^2 b$
e	e	a	a^2	b	ab	$a^2 b$
a	a	a^2	e	ab	$a^2 b$	b
a^2	a^2	e	a	$a^2 b$	b	ab
b	b	?	?	e	?	?
ab	ab	?	?	?	?	?
$a^2 b$	$a^2 b$	?	?	?	?	?

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 $a^i b *_H a^j$ 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 $a^i b *_H a^j = a^{i+1} b a^{j-1}$ and, eventually, $a^{i+j} b$. Similarly, $a^i b *_H a^j b = a^{i+j} b^2 = a^{i+j}$. This gives us

H	e	a	a^2	b	ab	$a^2 b$
e	e	a	a^2	b	ab	$a^2 b$
a	a	a^2	e	ab	$a^2 b$	b
a^2	a^2	e	a	$a^2 b$	b	ab
b	b	ab	$a^2 b$	e	a	a^2
ab	ab	$a^2 b$	b	a	a^2	e
$a^2 b$	$a^2 b$	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 $\langle ab \rangle$:

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

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 $a^j b^k$, 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:

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

Let us define a function Φ from H to $((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}), \oplus)$ by $\Phi(a^j b^k) = ([k]_2, [j]_3)$.
Then because $a^3 = e$ and $b^2 = e$, the group operation above tells us that

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

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 $|H| \mid |G|$.