Math 417 – Eleventh Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 18, 2020

The link for the Lagrange biography is
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:

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

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

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

To put this all together: for $j = 0, 1, 2, 3$,

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

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

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

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

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

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

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

All the others can be found this way too, and we get this huge table without doing any more permutation multiplications:

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.

Translated!

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:

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

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

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

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 previously 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.

Here's C_4, with the elements $\{e, a, a^2, a^3\}$ renamed as x_1, x_2, x_3, x_4 on the next page

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 $\begin{pmatrix}1234\\1234\end{pmatrix}$, the second row as $\begin{pmatrix}1234\\2341\end{pmatrix}$, the third row as $\begin{pmatrix}1234\\3412\end{pmatrix}$, and the fourth row as $\begin{pmatrix}1234\\4123\end{pmatrix}$.

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 ... V.

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,

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

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 H_G 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, $(\pi_i)^{-1} = \pi_\ell$, so H_G contains inverses.

Since $H_G \subset S_n$, associativity is automatic. □

Weekend!

(Except for Friday's class, and your emails telling me what I should talk about more.)