

Discovering a Common Property of All Groups: (Motivating Cayley's Theorem)

Daylene, Brian, and Shaochen

Introduction:

One of the first things we did when we encountered groups was make group-operation (multiplication, addition, etc...) tables. Here is such a table for a 4-element group.

	e_1	e_2	e_3	e_4
e_1	e_1	e_2	e_3	e_4
e_2	e_2	e_1	e_4	e_3
e_3	e_3	e_4	e_1	e_2
e_4	e_4	e_3	e_2	e_1

Table 1: A Group-operation Table

(Note to GAP Workshop Participants: The group above is $Z_2 \oplus Z_2$, but this is being suppressed since $Z_2 \oplus Z_2$ is not encountered in Gallian until after Cayley's Theorem. It is also $U(12)$, but this is also being suppressed.)

Exercise 1: We can see from the table that e_1 is the identity element of this group. What other properties of this group can you find from the table above?

Remember that one of the properties of group-operation tables that we've talked about is that every element of the group appears exactly once in each row and column of the table, so each row is a distinct arrangement of the elements of the group. With our new understanding of permutations, we can rephrase this in the following way:

*Every row of a group-operation table is **distinct** permutation of the elements in that group.*

We'll investigate this table from that perspective. Here's the array form of the permutation given by each of the rows along with a simpler version that just records the index of the group element. Notice that we are using only the body of the table, disregarding the row headings.

The e_1^{th} row gives $\begin{bmatrix} e_1 & e_2 & e_3 & e_4 \\ e_1 & e_2 & e_3 & e_4 \end{bmatrix}$ which can be restated as $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}$ or $()$.

The e_2^{th} row gives $\begin{bmatrix} e_1 & e_2 & e_3 & e_4 \\ e_2 & e_1 & e_4 & e_3 \end{bmatrix}$ which can be restated as $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$ or $(12)(34)$.

The e_3^{th} row gives $\begin{bmatrix} e_1 & e_2 & e_3 & e_4 \\ e_3 & e_4 & e_1 & e_2 \end{bmatrix}$ which can be restated as $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}$ or $(13)(24)$.

The e_4^{th} row gives $\begin{bmatrix} e_1 & e_2 & e_3 & e_4 \\ e_4 & e_3 & e_2 & e_1 \end{bmatrix}$ which can be restated as $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$ or $(14)(23)$.

Since each row is associated to a particular element of the group and each row is a distinct permutation of the elements of the group, we can create a correspondence between the elements of our group and these four permutations as shown below.

e_1	$()$
e_2	$(12)(34)$
e_3	$(13)(24)$
e_4	$(14)(23)$

Table 2: The Correspondence between Group Elements and Permutations

Now that we have these four permutations, we should investigate them further in GAP. First, enter them as a list. (Don't forget that GAP requires commas in cycle notation.)

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

Next, we'll test whether or not this collection of permutations forms a group.

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

So, now we know that the four permutations form a group generated by the elements $(12)(34)$ and $(13)(24)$. Since these are permutations on four symbols, this is a subgroup of S_4 . Let's examine its structure.

```
gap> Display(MultiplicationTable(G));
[ [ 1, 2, 3, 4],
  [ 2, 1, 4, 3],
  [ 3, 4, 1, 2],
  [ 4, 3, 2, 1] ]
```

	e_1	e_2	e_3	e_4
e_1	e_1	e_2	e_3	e_4
e_2	e_2	e_1	e_4	e_3
e_3	e_3	e_4	e_1	e_2
e_4	e_4	e_3	e_2	e_1

Table 1

Each integer in the GAP multiplication table above refers to the position of a permutation in our original GAP list s . GAP's multiplication table is identical in structure to the group-operation table that started this investigation. This means that our original group and the group G formed by the four permutations must be isomorphic.

Since the group of permutations, G , is a subgroup of S_4 , we can conclude that our original group is isomorphic to a subgroup of S_4 . Therefore, even though the original group appeared to have nothing whatsoever to do with permutations, it is isomorphic to a group of permutations!

Your Turn:

Exercise 2: Repeat this process with the group whose table is given below.

	e_1	e_2	e_3	e_4	e_5	e_6
e_1	e_1	e_2	e_3	e_4	e_5	e_6
e_2	e_2	e_3	e_1	e_5	e_6	e_4
e_3	e_3	e_1	e_2	e_6	e_4	e_5
e_4	e_4	e_5	e_6	e_1	e_2	e_3
e_5	e_5	e_6	e_4	e_2	e_3	e_1
e_6	e_6	e_4	e_5	e_3	e_1	e_2

Table 3: Another Group-operation Table

Find the permutation that corresponds to each row of the group-operation table.
 [Hint: The second row corresponds to $(321)(654)$.]

Create a correspondence between the group elements and the permutations you've found.

Enter these permutations as a list into GAP and check if they form a group or not.

If they do form a group, have GAP make its multiplication table and compare it to Table 3.

Make a conjecture about this new group and the six permutations you've found.

What does your conjecture imply about this group and S_6 ?

Exercise 3: Repeat this process for D_4 using the table below.

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

Table 4: Group-operation Table for D_4

Make a conjecture about D_4 and S_8 .

Moving Towards a Proof:

At this point, you probably have a conjecture about any finite group, G , of order n and the symmetric group S_n . Now, we have to try to prove it.

First, we'll return to the introductory example and think a bit deeper about what a group-operation table is telling us. Recall that the e_i^{th} row of our group-operation table is just the result of multiplying each element of the group by the element e_i . Therefore, the permutation we were associating with each element of our group is induced by left-multiplication by that element. However, that's just a function from the group back to itself (as any permutation ought to be).

e_1	()	Left-multiplication by e_1	$f_1(x) = e_1 * x$
e_2	(12)(34)	Left-multiplication by e_2	$f_2(x) = e_2 * x$
e_3	(13)(24)	Left-multiplication by e_3	$f_3(x) = e_3 * x$
e_4	(14)(23)	Left-multiplication by e_4	$f_4(x) = e_4 * x$

Table 5: From Group Elements to Permutations to Functions

Now let us investigate this left-multiplication thought using GAP.

Let D_4 be our original group.

```
gap> d4 := DihedralGroup(IsPermGroup, 8);
```

Define functions by left-multiplication by each element of the original group and check if they are permutations. (i.e. if they are bijective functions.)

```
gap> a := Elements(d4);
```

```
gap> h1 := x-> a[1]*x;
```

```
gap> f1 := MappingByFunction(d4, d4, h1);
```

```
gap> IsBijective(f1);
```

```
⋮
```

Repeat for other elements of the group.

We can also find all permutations induced by left-multiplication by each element of the original group using GAP command **List**.

```
gap> w := List(a, i -> MappingByFunction(d4, d4, x -> i*x));
```

```
gap> List(w, IsBijective);
```

Check if the set of above permutations form a group or not.

```
gap> Gprime := AsGroup([f1, f2, f3, f4, f5, f6, f7, f8]);
```

or

```
gap> Gprime := AsGroup(w);
```

Is this new permutation group isomorphic to our original group?

```
gap> IsomorphismGroups(d4, Gprime);
```

What is your conjecture about D_4 and this permutation group?

Can we generalize this result to an arbitrary group?

Conclusion:

Notice that each row of any group-operation table is a permutation of the set of elements of the group. It is not surprising that at least every finite group G is isomorphic to a subgroup of the group S_G of all permutations of G . In fact the same is true for infinite groups. Cayley's theorem states that every group is isomorphic to a group of permutations. Now we are going to prove the Cayley's theorem.

Cayley's Theorem: Every group is isomorphic to a group of permutations.

Proof:

Let G be a group with identity e .

We must find a group G' of permutations that is isomorphic to G . Notice that the G' in our example consists of permutations induced by left-multiplication by each element of the group G . That is how we are going to construct G' .

First, we will prove that for each $x \in G$, $\lambda_x : G \rightarrow G$ defined by $\lambda_x(g) = xg$ for all $g \in G$ is a permutation of G . i.e. $\lambda_x \in S_G$ (Note that this is a left-multiplication by x)

(i) Show that λ_x is one-to-one.

$$\lambda_x(a) = \lambda_x(b) \Rightarrow xa = xb \Rightarrow x^{-1}xa = x^{-1}xb \Rightarrow a = b$$

(ii) Show that λ_x is onto.

$$\text{Let } c \in G \text{ Then } x^{-1}c \in G \text{ and } \lambda_x(x^{-1}c) = x(x^{-1}c) = c$$

Second, we will let $G' = \{\lambda_x : x \in G\}$ and prove that G' is a group.

(i) Let $\lambda_x, \lambda_y \in G'$, where $x, y \in G$

Show that $\lambda_x \circ \lambda_y \in G'$ i.e. show that $\lambda_x \circ \lambda_y = \lambda_{xy}$

$$(\lambda_x \circ \lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg) = (xy)(g) = \lambda_{xy}(g)$$

(ii) $\lambda_e(g) = eg = g \Rightarrow \lambda_e$ is an identity of G'

(iii) Let $\lambda_x \in G'$, where $x \in G$

Show that $(\lambda_x)^{-1} \in G'$ i.e. show that $(\lambda_x)^{-1} = \lambda_{x^{-1}}$

Let $\lambda_x \in G'$, where $x \in G$

$$\text{Then } (\lambda_x \circ \lambda_{x^{-1}})(g) = \lambda_x(\lambda_{x^{-1}}(g)) = \lambda_x(x^{-1}g) = x(x^{-1}g) = eg = \lambda_e(g)$$

Hence $\lambda_x \circ \lambda_{x^{-1}} = \lambda_e$

Similarly $\lambda_{x^{-1}} \circ \lambda_x = \lambda_e$

Thus the inverse of λ_x is $\lambda_{x^{-1}}$ (i.e. $(\lambda_x)^{-1} = \lambda_{x^{-1}}$)

Last, we will prove that $\phi : G \rightarrow G'$ is an isomorphism.

Define $\phi(x) = \lambda_x$

ϕ is one-to-one:

$$\phi(x) = \phi(y) \Rightarrow \lambda_x = \lambda_y \Rightarrow \lambda_x(e) = \lambda_y(e) \Rightarrow xe = ye \Rightarrow x = y$$

ϕ is onto :

Let $\lambda_x \in G'$ Then $\phi(x) = \lambda_x$

$\phi(xy) = \phi(x)\phi(y) :$

$$\phi(xy) = \lambda_{xy} = \lambda_x \circ \lambda_y = \phi(x)\phi(y)$$

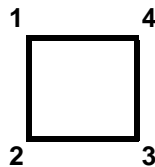
Another Approach:

```
gap> Order(SymmetricGroup(8));  
gap> Order(DihedralGroup(8));
```

Exercise 4:

We've seen that we can find a copy of D_4 inside S_8 . Comparing the sizes of D_4 and S_8 (check: how big are they?), it seems reasonable to think that we might be able to find D_4 inside some smaller S_n . Let's see if we can do just that.

Recall that D_4 is the group of symmetries of the square:



Recall also that D_4 is generated by R_{90} , a 90° counterclockwise rotation, and H , a flip across the horizontal axis of symmetry.

Write R_{90} and H in cycle notation. In GAP, use the Subgroup command to create D_4 as a subgroup of S_4 .

In GAP, use the IsomorphismGroups command to verify that this copy of D_4 is isomorphic to the one you found inside S_8 before.

Hence there's a copy of D_4 inside S_4 . In general, the construction in the proof of Cayley's Theorem isn't very efficient; it locates a group of order n inside S_n , a group of order $n!$.

Can we do better than this? That is, can we find a copy of D_4 inside S_n for some $n < 4$? Prove that your answer is correct.

Is the D_4 you found inside S_4 the only copy of D_4 that's in S_4 ? In GAP, see if you can find another subgroup of S_4 that's isomorphic to D_4 .