Classification of Sets that Force a Group

Michael Moen
Carthage College
mmoen@carthage. edu

May 13, 2016

Abstract

In standard group theory, a group is formed from a set and a binary operation, then properties of the group that results are studied. However, there are some underlying structures in the sets that form groups. By considering the sets and determining what can be made from them it is possible to get information about the group that can be formed with the set.

1 Introduction

There has been lots of work in the field of classifying various types of groups. However, this leads to the question of what really gives the group any observed algebraic structures. This points to some innate structure stemming directly from the sets used to form the groups and the operation used for composition. If the set plays the largest role in what the group would look like it could be possible to classify sets based on what sort of groups they generate.

2 Definitions and Development

Definition 1. An operation is **associative** on a set G, if $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$.

Definition 2. An element e is called an **identity** if $a \circ e = e \circ a = a$ for all elements $a \in G$.

Definition 3. Elements a and b are considered **inverses** if $a \circ b = b \circ a = e$

Definition 4. An operation is **commutative** if $a \circ b = b \circ a$ for all elements $a, b \in G$.

Definition 5. A **group** is a set G with a binary operation $\circ$ that has the following properties:
• The operation is associative;

• There exists an identity element e;
• For each element $a \in G$, there is an element $b \in G$ that is its inverse.

Definition 6. A **Cayley table** is visual representation of a group that shows all the products of any two elements in the group.

Definition 7. The **Latin Square Property** is the property of a Cayley table such that each row and column has no repeating entries, and every element shows up once in each row and column.

Theorem 8. *(Latin Square Property) Let $(G,\circ)$ be a group. Then G satisfies the Latin square property. This means that for all $a, b \in G$, there exists a unique $g \in G$ such that $a \circ g = b$. Likewise there exists a unique $h \in G$ such that $h \circ a = b$*

Proof. Assume that $g = a^{-1} \circ b$. Then composing a on the left of both sides of the equation it is seen that, $a \circ g = a \circ (a^{-1} \circ b)$. Using the associative property of groups it is shown that, $a \circ g = (a \circ a^{-1}) \circ b$. Replacing the composition of inverses with the identity yields, $a \circ g = e \circ b$. Thus it is seen that $a \circ g = b$.

Assume that $a \circ g = b = a \circ g'$ for some $g, g' \in G$. Then it is seen that by the property of identities $g = e \circ g$. Replacing the identity with a set of inverses yields $g = (a^{-1} \circ a) \circ g$. Using the associative property again $g = a^{-1} \circ (a \circ g)$. Replacing with the assumption it is seen that $g = a^{-1} \circ b$. Using replacement with the assumption again produces $g = a^{-1} \circ (a \circ g')$. The associative property gives $g = (a^{-1} \circ a) \circ g'$. Then replacing the inverses with the identity yields $g = e \circ g' = g'$. Thus, $g = g'$, and uniqueness has been proven. The same argument can be made for h. □

Corollary 9. *If G is a finite group, its Cayley table is a Latin Square.*

The fact that a Cayley table is a Latin square means that for any finite group the Cayley table for that group will have every element of the group in every row and column. This follows from every element in each row and column being unique. This is shown below, with the Cayley table for the group Z_4.

Example 10. The set of integers under addition modulo 4 is called Z_4. This is the Cayley table for Z_4

Z_4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Having each element in each row and column be unique is important because then partially filled in Cayley tables can be filled in like a Sudoku puzzle where it is possible to eliminate possibilities based on what the other elements of the row and column are. This is shown in Example 11.

Example 11. Consider the set $\{2, 3, 6, 12\}$ under some form of multiplication. To start filling in the table standard multiplication is used. From standard multiplication it is known that $2 * 3 = 6$ and $2 * 6 = 12$. This is all that can be used to start the table since the rest of the products are not in the set, and there is no defined modular operation to reduce them. Since standard multiplication is abelian, it is possible to fill in both $2 * 3$ and $3 * 2$, likewise for $2 * 6$.

	2	3	6	12
2		6	12	
3	6			
6	12			
12				

Noticing that all elements besides 12 are already composed with something else, and none of them have the property of being an identity, the element 12 is forced to be the identity in order for this to form a group.

	2	3	6	12
2		6	12	2
3	6			3
6	12			6
12	2	3	6	12

Filling in the composition of the identity with each element, it becomes apparent that from the Latin Square property $2 * 2$ must be 3, and $3 * 6 = 6 * 3$ must be 2. It is important to note that since the Latin Square property holds for both columns and rows, the operation continues to be abelian in order to satisfy this constraint.

	2	3	6	12
2	3	6	12	2
3	6		2	3
6	12	2		6
12	2	3	6	12

After filling in those elements it is seen that $3 * 3 = 12$, and $6 * 6 = 3$.

	2	3	6	12
2	3	6	12	2
3	6	12	2	3
6	12	2	3	6
12	2	3	6	12

Thus it has been shown that the Latin square property can be used to fill in a partial Cayley table, and induce multiplication on a set.

The next thing that needs to be developed is the method of generating sets. Starting from an empty set the first thing to do is put an element in the set. Since it is one lone element it does not matter what the element is, so let it be called p. Expanding this set to be order two can be done in two different ways. The first way is letting the second element be the composition of the first element with itself or p^2. The second way is adding another element that is relatively prime to the first, lets call it q. This shows that there are two sets of order two that need to be evaluated. Expanding to the sets of order three happens in the same manner and all the possibilities are shown below.

Order Two	Order Three
$\{p, p^2\}$	$\{p, p^2, p^3\}$
$\{p, p^2\}$	$\{p, p^2, p^4\}$
$\{p, p^2\}$	$\{p, p^2, q\}$
$\{p, q\}$	$\{p, q, p^2\}$
$\{p, q\}$	$\{p, q, pq\}$
$\{p, q\}$	$\{p, q, q^2\}$
$\{p, q\}$	$\{p, q, r\}$

In the first set, the generation of the third element comes from composing p with p^2 to get p^3. In set two, the generation of the set comes from composing p^2 with itself to get p^4. In the third set the third element is a new element q, that is relatively prime to p. In the fourth set, the third element is generated by composing p with itself to get p^2. The fifth set is generated by composing p with q to get pq. Set six is developed from composing q with itself to get q^2. The seventh set comes from adding another element that is relatively prime to both p and q. All of the sets of order three are listed above, however, there are some repeats due to symmetry. The sets $\{p, p^2, q\}$, $\{p, q, p^2\}$ are the same set in different order, and $\{p, q, q^2\}$ is symmetric to them due to the fact that q and p are interchangeable. This means that only one of them needs to be considered, and that set will be $\{p, p^2, q\}$. A list of all sets up to order five is listed in the table in Appendix A.

3 Results

3.1 Sets of Order Two and Three

Now that the sets of been constructed the next thing to do is to check all the sets of orders two and three to see if they form a full Cayley table. The set of order one is redundant because if it is going to be a group it will be the identity and it is rather uninteresting to look at since it is trivial. Considering the sets of order two yields the following Cayley tables.

	p	p^2
p	p^2	p
p^2	p	p^2

	p	q
p		
q		

It can be seen that of the two sets of order two only one set forces a group table to be formed. The set $\{p, p^2\}$ forces a group with p^2 being the identity. The set $\{p, q\}$ does not force a set due to not enough information to start the table. This shows that any set only filled with elements that are coprime is not going to force a group due to there being not enough starting information.
Considering the sets of order three next:

	p	p^2	p^3
p	p^2	p^3	p
p^2	p^3	p	p^2
p^3	p	p^2	p^3

	p	q	pq
p	q	pq	p
q	pq	p	q
pq	p	q	pq

The sets $\{p, p^2, p^3\}$ and $\{p, q, pq\}$ both force groups with p^3 and pq as the identity respectively.

	p	p^2	p^4
p	p^2		p
p^2		p^4	p^2
p^4	p	p^2	p^4

	p	q	r
p			
q			
r			

The sets $\{p, p^2, p^4\}$ and $\{p, q, r\}$ do not force groups. The set $\{p, p^2, p^4\}$ does not work because to complete the first row the $p * p^2$ element has to be p^4, but to complete the column it has to be p. This dichotomy is the main way a set fails to force a group. The set $\{p, q, r\}$ like its predecessor $\{p, q\}$ fails to be a group due to lack of starting information.

The last set of order three is $\{p, p^2, q\}$. This set is interesting because it has two possibilities for an identity.

	p	p^2	q
p	p^2	p	
p^2	p	p^2	q
q		q	

	p	p^2	q
p	p^2		p
p^2			p^2
q	p	p^2	q

If p^2 is chosen as the identity it can be seen that there will be an inconsistency in columns and rows again since the $p * q$ element has to be q to finish the row, but there is already a q in the column so it can not work out. However, if q is chosen to be the identity then it is seen that there are no conflicts and the table can be filled in as shown below.

	p	p^2	q
p	p^2	q	p
p^2	q	p	p^2
q	p	p^2	q

This is the first example of a set conditionally forcing a group. These sets are the most interesting because it points to a relationship between what is chosen as an identity and the other elements of the set.

That is the classification of all the sets of order three. The sets that force groups are, $\{p, p^2, p^3\}$ and $\{p, q, pq\}$. The sets that do not force groups are, $\{p, p^2, p^4\}$ and $\{p, q, r\}$. The last set, $\{p, p^2, q\}$ can force a group depending on what element is chosen as the identity.

3.2 The Sets of Order Four

Generating the sets of order four occurs in the same manner as the sets of order three. Using the sets of order three as the basis, generating all possible combinations of new elements, and discarding those that are symmetric to a previously generated set yields the following sixteen sets:

$$\{p, p^2, p^3, p^4\}, \{p, p^2, p^3, p^5\}, \{p, p^2, p^3, p^6\}, \{p, p^2, p^3, q\},$$

$$\{p, p^2, p^4, p^5\}, \{p, p^2, p^4, p^6\}, \{p, p^2, p^4, p^8\}, \{p, p^2, p^4, q\},$$

$$\{p, p^2, q, pq\}, \{p, p^2, q, p^2q\}, \{p, p^2, q, q^2\}, \{p, p^2, q, r\},$$

$$\{p, q, pq, p^2q^2\}, \{p, q, pq, p^2q\}, \{p, q, pq, r\}, \{p, q, r, s\}.$$

The sets of order four that generate a Cayley table are

$$\{p, p^2, p^3, p^4\}, \{p, pq, pq, p^2q^2\}.$$

Their tables are shown below.

	p	p^2	p^3	p^4
p	p^2	p^3	p^4	p
p^2	p^3	p^4	p	p^2
p^3	p^4	p	p^2	p^3
p^4	p	p^2	p^3	p^4

	p	q	pq	p^2q^2
p	p^2q^2	pq	q	p
q	pq	p^2q^2	p	q
pq	q	p	p^2q^2	pq
p^2q^2	p	q	pq	p^2q^2

The sets of order four that generate a Cayley table are both extensions of the sets that generated a table of order three.
The sets of order four that do not work are
$\{p, p^2, p^3, p^5\}$, $\{p, p^2, p^3, p^6\}$, $\{p, p^2, p^4, p^5\}$, $\{p, p^2, p^4, p^6\}$, $\{p, p^2, p^4, p^8\}$, $\{p, p^2, q, p^2q\}$, $\{p, p^2, q, q^2\}$, $\{p, q, pq, p^2q\}$, $\{p, q, r, s\}$.

	p	p^2	p^3	p^5
p	p^2	p^3		p
p^2	p^3		p^5	p^2
p^3		p^5		p^3
p^5	p	p^2	p^3	p^5

	p	p^2	p^3	p^6
p	p^2	p^3		p
p^2	p^3			p^2
p^3			p^6	p^3
p^6	p	p^2	p^3	p^6

	p	p^2	p^4	p^5
p	p^2		p^5	p
p^2		p^4		p^2
p^4	p^5			p^4
p^5	p	p^2	p^4	p^5

	p	p^2	p^4	p^6
p	p^2			p
p^2		p^4	p^6	p^2
p^4		p^6		p^4
p^6	p	p^2	p^4	p^6

	p	p^2	p^4	p^8
p	p^2	p^8		p
p^2	p^8	p^4	p	p^2
p^4		p	p^8	p^4
p^8	p	p^2	p^4	p^8

	p	p^2	q	q^2
p	p^2			p
p^2			p	p^2
q		p	q^2	q
q^2	p	p^2	q	q^2

	p	p^2	q	p^2q
p	p^2	q		p
p^2	q	p	p^2q	p^2
q		p^2q		q
p^2q	p	p^2	q	p^2q

	p	q	r	s
p				
q				
r				
s				

The sets of order four that work if the right identity is chosen are $\{p, p^2, p^3, q\}$, $\{p, p^2, p^4, q\}$. The Cayley tables for these sets are shown below.

	p	p^2	p^3	q
p	p^2	p^3	q	p
p^2	p^3	q	p	p^2
p^3	q	p	p^2	p^3
q	p	p^2	p^3	q

	p	p^2	p^3	q
p	p^2	p^3	p	
p^2	p^3	q	p^2	p
p^3	p	p^2	p^3	q
q		p	q	

	p	p^2	p^4	q
p	p^2	q		p
p^2	q	p^4	p	p^2
p^4		p	p^2	p^4
q	p	p^2	p^4	q

	p	p^2	p^4	q
p	p^2	q	p	p^4
p^2	q	p^4	p^2	p
p^4	p	p^2	p^4	q
q	p^4	p	q	p^2

The last sets of order four do not fit into the preexisting set structures that were developed for order three. Starting with the set $\{p, p^2, q, r\}$. If q or r is chosen to be the identity the result is shown in the table below.

	p	p^2	q	r
p	p^2	q	r	p
p^2	q	r	p	p^2
q	r	p	p^2	q
r	p	p^2	q	r

However if p^2 is chosen as the identity something interesting occurs.

	p	p^2	q	r
p	p^2	p	r	q
p^2	p	p^2	q	r
q	r	q		
r	q	r		

This set produces a table that works no matter what elements are chosen to finish it off. The table works with both p and p^2 going in either of the two remaining positions. The set $\{p, p^2, q, pq\}$ generates similar tables to the set $\{p, p^2, q, r\}$, as shown below.

	p	p^2	q	pq
p	p^2	q	pq	p
p^2	q	pq	p	p^2
q	pq	p	p^2	q
pq	p	p^2	q	pq

	p	p^2	q	pq
p	p^2	p	pq	q
p^2	p	p^2	q	pq
q	pq	q		
pq	q	pq		

The last set of order four is $\{p, q, pq, r\}$. Choosing pq as the identity the following table is generated.

	p	q	pq	r
p	r	pq	p	q
q	pq	r	q	p
pq	p	q	pq	r
r	q	p	r	pq

However if r is chosen as the identity, a different result appears.

	p	q	pq	r
p		pq		p
q	pq			q
pq				pq
r	p	q	pq	r

At this point another choice needs to be made in order to keep filling in the table. Choosing whether $p \circ p = r$ or $p \circ p = q$. Both choices are shown below.

	p	q	pq	r
p	r	pq	q	p
q	pq			q
pq	q			pq
r	p	q	pq	r

	p	q	pq	r
p	q	pq	r	p
q	pq	r	p	q
pq	r	p	q	pq
r	p	q	pq	r

When $p \circ p = r$, there is a square in the middle that can be filled in two different ways. This is due to the fact that $q \circ q$ can be equal to both p and r and still force a complete table.

4 Discussion

From this study it is possible to conclude that there is some amount of structure in the elements. Some of this structure can be attributed to the fact that a commutative operation was used to start the process. It is also important to note that associativity is a property that needs to be checked to verify it is a group. All of the tables generated up to order five are associative. It is possible that associativity might not continue to be present as the size of the sets get larger. There are sets of order five that appear in the table in appendix A. Since all the sets were generated by hand there is a possibility that some are missing still. Some work has been done looking into the order five sets and the trends seem to continue but an exhaustive study has not been completed yet.

5 Future Work

There are two big things that could be achieved to further this study. The first is to figure out a way to count or generate how many sets there should be of each order. Some attempts at writing a program to do this have been made, but there is issues with comparing symmetric sets. This would allow for an easier time looking at higher order sets. The second thing that could be done is to prove that each table has to be associative or disprove it. This would either remove the hassle of checking each element for associativity or show that it really is necessary.

References

[1] Joseph A. Gallian , *Contemporary Abstract Algebra*, Cengage Learning, 2010.

A Appendix

Order	Set	Order	Set	Order	Set
1	$\{p\}$	5	$\{p, p^2, p^3, p^4, p^5\}$	5	$\{p, p^2, p^4, q, pq\}$
2	$\{p, p^2\}$	5	$\{p, p^2, p^3, p^4, p^6\}$	5	$\{p, p^2, p^4, q, p^2q\}$
2	$\{p, q\}$	5	$\{p, p^2, p^3, p^4, p^7\}$	5	$\{p, p^2, p^4, q, p^4q\}$
3	$\{p, p^2, p^3\}$	5	$\{p, p^2, p^3, p^4, p^8\}$	5	$\{p, p^2, p^4, q, q^2\}$
3	$\{p, p^2, p^4\}$	5	$\{p, p^2, p^3, p^4, q\}$	5	$\{p, p^2, p^4, q, r\}$
3	$\{p, p^2, q\}$	5	$\{p, p^2, p^3, p^5, p^6\}$	5	$\{p, p^2, q, pq, p^3q\}$
3	$\{p, q, pq\}$	5	$\{p, p^2, p^3, p^5, p^7\}$	5	$\{p, p^2, q, pq, p^2q\}$
3	$\{p, q, r\}$	5	$\{p, p^2, p^3, p^5, p^8\}$	5	$\{p, p^2, q, pq, pq^2\}$
4	$\{p, p^2, p^3, p^4\}$	5	$\{p, p^2, p^3, p^5, p^{10}\}$	5	$\{p, p^2, q, pq, p^2q^2\}$
4	$\{p, p^2, p^3, p^5\}$	5	$\{p, p^2, p^3, p^5, q\}$	5	$\{p, p^2, q, q^2, pq\}$
4	$\{p, p^2, p^3, p^6\}$	5	$\{p, p^2, p^4, p^6, p^8\}$	5	$\{p, p^2, q, pq, r\}$
4	$\{p, p^2, p^3, q\}$	5	$\{p, p^2, p^4, p^6, p^{10}\}$	5	$\{p, p^2, q, p^2q, p^4q\}$
4	$\{p, p^2, p^4, p^5\}$	5	$\{p, p^2, p^4, p^6, p^{12}\}$	5	$\{p, p^2, q, p^2q, p^3q\}$
4	$\{p, p^2, p^4, p^6\}$	5	$\{p, p^2, p^4, p^6, q\}$	5	$\{p, p^2, q, p^2q, p^4q^2\}$
4	$\{p, p^2, p^4, p^8\}$	5	$\{p, p^2, p^4, p^8, p^{10}\}$	5	$\{p, p^2, q, q^2, p^2q\}$
4	$\{p, p^2, p^4, q\}$	5	$\{p, p^2, p^4, p^8, p^{12}\}$	5	$\{p, p^2, q, p^2q, p^3\}$
4	$\{p, p^2, q, pq\}$	5	$\{p, p^2, p^4, p^8, p^{16}\}$	5	$\{p, p^2, q, p^2q, p^4\}$
4	$\{p, p^2, q, p^2q\}$	5	$\{p, p^2, p^4, p^8, q\}$	5	$\{p, p^2, q, p^2q, r\}$
4	$\{p, p^2, q, q^2\}$	5	$\{p, p^2, p^4, p^5, p^6\}$	5	$\{p, p^2, p^3, q, q^2\}$
4	$\{p, p^2, q, r\}$	5	$\{p, p^2, p^4, p^5, p^7\}$	5	$\{p, p^2, p^4, q, q^2\}$
4	$\{p, q, pq, p^2q^2\}$	5	$\{p, p^2, p^4, p^5, p^9\}$	5	$\{p, p^2, q, q^2, r\}$
4	$\{p, q, pq, r\}$	5	$\{p, p^2, p^4, p^5, p^{10}\}$	5	$\{p, p^2, q, r, pr\}$
4	$\{p, q, r, s\}$	5	$\{p, p^2, p^4, p^5, q\}$	5	$\{p, p^2, q, r, qr\}$
5	$\{p, p^2, q, r, p^2r\}$	5	$\{p, p^2, p^3, q, r\}$	5	$\{p, p^2, p^4, q, r\}$
5	$\{p, p^2, q, r, s\}$	5	$\{p, q, pq, p^2q^2, p^3q^3\}$	5	$\{p, q, pq, p^2q^2, p^4q^4\}$
5	$\{p, q, pq, p^2q^2, p^3q^2\}$	5	$\{p, q, pq, p^2q, p^2q^2\}$	5	$\{p, q, pq, p^2q^2, r\}$
5	$\{p, q, r, s, p^2\}$	5	$\{p, q, r, s, pq\}$	5	$\{p, q, r, s, t\}$