

Some Elementary Group Theory

In the chapter "**Binary Operations**", we demonstrated that if a binary operation possesses an identity then it is unique. In other words, no binary operation could possess two different identities. An analogous result pertains to inverses of elements of a group.

Theorem: Let G be a group. Let $x \in G$. The inverse of x is unique.

Proof: Suppose not. Suppose y is an inverse of x and z is an inverse of x where $y \neq z$.

$$\therefore xy = e \text{ and } xz = e$$

$$\therefore xy = xz$$

$$\therefore y = z \text{ [LHC]}$$

→ ←

QED

As a result of this theorem, whenever we use the symbol x^{-1} we are referencing a unique element in G . Suppose $x^{-1} = q$. By the definition of x^{-1} , $x \cdot q = e$ and $q \cdot x = e$. However, the definition of q^{-1} would demand an element of G that satisfies precisely the same equations. We therefore deduce: If $x^{-1} = q$ then $q^{-1} = x$. This is the heart of the following theorem.

Theorem: Let G be a group. Let $x \in G$. $(x^{-1})^{-1} = x$

Proof: Let $x^{-1} = q$.

$$\therefore (x^{-1})^{-1} = q^{-1}$$

$$\text{By our discussion above, } q^{-1} = x$$

$$\therefore (x^{-1})^{-1} = x$$

QED

We know, from our earlier explorations of specific groups, that some elements are self-invertible. There are two ways to regard a self-invertible element. If z is a self-invertible element in a specific group then $z^{-1} = z$. However, a different way to view the same fact is to note that $z \cdot z = e$. Notice that in every group the identity element e is self-invertible. We call the identity element of any group the "trivial" self-invertible element. If $x \neq e$ and $x^{-1} = x$, then we call x a "non-trivial" self-invertible element. Not all groups have a non-trivial self-invertible element. Consider Z_5 . $[0]^{-1} = [0]$ and is therefore self-invertible. However, $[0]$ is the identity of Z_5 . Therefore, $[0]$ is the trivial self-invertible element. None of the other elements of Z_5 is self-invertible.

$$\begin{aligned}
[1]^{-1} &= [4] \\
[2]^{-1} &= [3] \\
[3]^{-1} &= [2] \\
[4]^{-1} &= [1]
\end{aligned}$$

We see that Z_5 possesses no non-trivial self-invertible element.

Suppose a group G is finite and $o(G)$ is an even number. Let's take each element that is self-invertible and pair it with its inverse. Let's take all such pairs and put them in a set. This set would be an even order subset of G . The remaining elements in G (the elements that are not invertible) must also constitute a set with an even number of elements. e is self-invertible. If e is deleted from the remaining elements, there is an odd number of elements left. Therefore, G contains at least one non-trivial self-invertible element. We have proven:

Theorem: If G is a finite group and $o(G) = 2n$ for some integer $n \geq 1$, G contains at least one non-trivial self-invertible element.

What about finite groups with odd order? When we study subgroups in a later chapter, we will be able to prove that odd order finite groups never contain a non-trivial self-invertible element.

Let's explore another interesting fact about inverses:

Theorem: Let G be a group. Let $a \in G$ and $b \in G$.

$$(ab)^{-1} = b^{-1}a^{-1}$$

Proof: Let's consider what the symbol $(ab)^{-1}$ means. It denotes an element x such that $x \cdot (ab) = e$ and $(ab) \cdot x = e$. Consider the element $b^{-1}a^{-1}$.

$$\begin{aligned}
(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}(ab)) \text{ [Associativity]} \\
&= b^{-1}((a^{-1}a)b) \text{ [Associativity]} \\
&= b^{-1}(eb) \\
&= b^{-1} \cdot b \\
&= e
\end{aligned}$$

$$\begin{aligned}
\text{Similarly: } (ab)(b^{-1}a^{-1}) &= a(b(b^{-1}a^{-1})) \\
&= a((bb^{-1}) \cdot a^{-1}) \\
&= a(ea^{-1}) \\
&= aa^{-1} \\
&= e
\end{aligned}$$

Therefore, by the definition of an inverse,

$$(ab)^{-1} = b^{-1}a^{-1}$$

QED

The preceding theorem can be extended to any number of elements. For example:

$$(xyzw)^{-1} = w^{-1}z^{-1}y^{-1}x^{-1}.$$

You probably have already encountered the effect of this theorem in Linear Algebra. The set of all $n \times n$ matrices is not a group since the singular matrices have no inverses. However, the set of all nonsingular $n \times n$ matrices is a group. The identity element is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. You may recall that for nonsingular $n \times n$ matrices A and B , $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.

Definition: Let G be a group. Let $x \in G$. The symbol x^n is defined to be:

$$\underbrace{x \cdot x \cdot x \cdot \dots \cdot x}_{n \text{ factors}}.$$

For example:

$$\text{in } Q_8, i^3 = i \cdot i \cdot i = -1 \cdot i = -i.$$

$$\text{In } Z_5, [2]^4 = [2] + [2] + [2] + [2] = [3].$$

$$\text{Finally, in } S_3, (123)^3 = (123)(123)(123) = (132)(123) = e.$$

We also define the symbol x^{-n} to be symbolic for $(x^{-1})^n$ or $\underbrace{x^{-1} \cdot x^{-1} \cdot x^{-1} \cdot \dots \cdot x^{-1}}_{n \text{ factors}}$.

We have already defined the order of a finite group to mean the number of elements in that group. We now define the order of a group element.

Definition: Let G be a group. Let $x \in G$. The order of x ($o(x)$) is defined to be the smallest positive integer n such that $x^n = e$. If no such n exists, we will say that x has infinite order.

Examples:

1. In D_4 : $o(a) = 2$
 $o(b^3) = 4$
2. In S_3 : $o((12)) = 2$
 $o((123)) = 3$
3. In the group of all non-zero real numbers under multiplication :
 $o(-1) = 2$
3 has infinite order
4. In K_8 : every element has order 2
5. In Q_8 : $o(i) = 4$
 $o(-1) = 2$

$$6. \text{ In } \mathbb{Z}_{12} : \quad \begin{aligned} o(2) &= 6 \\ o(3) &= 4 \end{aligned}$$

Notice that in all of our finite group examples no element had infinite order.

Theorem: If G is a finite group and $x \in G$ then x has finite order.

Proof: Construct the set $S = \{e, x, x^2, x^3, \dots\}$. By closure, all elements in this set are elements of G . Since G is finite, there must be duplication of results in S . $\therefore \exists$ positive integers p and q such that $x^p = x^q$ where $p < q$.

Let's rewrite the elements of S :

$$e, x, x^2, x^3, \dots, x_{\eta}^p, \dots, x_{\eta}^q, \dots$$

$$x^p = x^q$$

$$\Rightarrow x^{-1} \cdot x^p = x^{-1} x^q$$

$$\Rightarrow x^{p-1} = x^{q-1}$$

$$e, x, x^2, x^3, \dots, x_{\eta}^{p-1}, x_{\eta}^p, \dots, x_{\eta}^{q-1}, x_{\eta}^q, \dots$$

If we continue this process of multiplying by x^{-1} p times, we will arrive at the equation: $e = x^{q-p}$

$\therefore x$ has finite order.

QED

Let's consider an interesting and fun exercise that illustrates many of the theorems concerning groups that we have studied. Suppose the following incomplete table represents a group:

?	f	g	h	i	j
f					
g			h		
h					g
i			f		
j					

Let's try to fill in the entire table. The given result $g \cdot h = h$ allows us to deduce that g is the identity. The chart's entries expand to:

<i>?</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>
<i>f</i>		<i>f</i>			
<i>g</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>
<i>h</i>		<i>h</i>			<i>g</i>
<i>i</i>		<i>i</i>	<i>f</i>		
<i>j</i>		<i>j</i>			

The result $h \cdot j = g$ implies that $h = j^{-1}$ (remember that g is the identity). By a previous theorem, we can deduce that $j = h^{-1}$ and the chart becomes:

<i>?</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>
<i>f</i>		<i>f</i>			
<i>g</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>
<i>h</i>		<i>h</i>			<i>g</i>
<i>i</i>		<i>i</i>	<i>f</i>		
<i>j</i>		<i>j</i>	<i>g</i>		

We are now ready to capitalize on RHC and LHC. Consider the entry for $i \cdot j$. Because row and column duplication is impossible, this result can't be i, f, j , or g . By default, the result must be h and the chart becomes:

<i>?</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>
<i>f</i>		<i>f</i>			
<i>g</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>
<i>h</i>		<i>h</i>			<i>g</i>
<i>i</i>		<i>i</i>	<i>f</i>		<i>h</i>
<i>j</i>		<i>j</i>	<i>g</i>		

Note now that $f \cdot j$ can only be i . In fact, a domino effect now takes place that allows every position to be filled in. The entire chart is:

?	f	g	h	i	j
f	h	f	j	g	i
g	f	g	h	i	j
h	j	h	i	f	g
i	g	i	f	j	h
j	i	j	g	h	f

Actually, the chart you just completed is an isomorphic copy of \mathbb{Z}_5 . Try this decode:

$$\begin{aligned} g &= [0] \\ j &= [1] \\ f &= [2] \\ i &= [3] \\ h &= [4]. \end{aligned}$$

Interestingly, as we shall see, there are numerous other decodes possible. In fact, we will learn that the only group of order 5 is \mathbb{Z}_5 .

Let's return to our study of exponential notation. It is an easy consequence of our definition of an exponent that $a^n \cdot a^m = a^{n+m}$ for any element a in any group G .

$$a^n \cdot a^m = \underbrace{(a \cdot a \cdot \dots \cdot a)}_{n \text{ factors}} \cdot \underbrace{(a \cdot a \cdot \dots \cdot a)}_{m \text{ factors}} = \underbrace{a \cdot a \cdot \dots \cdot a}_{n+m \text{ factors}}.$$

We will say that an element x is a cyclic generator of a group G iff every element a in G can be written in the form x^j for some positive integer j . If this is the case, we say that G is a cyclic group. As our first example, let's consider whether or not D_3 is a cyclic group. If so, e can't be a cyclic generator since $e^n = e$ for all n . Is a a cyclic generator? $a^1 = a$, $a^2 = e$, $a^3 = a$, $a^4 = e$, and so on. The various powers of a only generate e and a (and not the whole group). The powers of b only generate e, b, b^2 as is the case for b^2 . The powers of ab only generate e and ab while the powers of ab^2 can create only e and ab^2 . D_3 is not cyclic.

Let's now consider \mathbb{Z}_6 :

$$\begin{aligned} [1]^1 &= [1] \\ [1]^2 &= [1] + [1] = [2] \\ [1]^3 &= [3] \\ [1]^4 &= [4] \\ [1]^5 &= [5] \\ [1]^6 &= [0] \end{aligned}$$

This exhausts the elements of \mathbb{Z}_6 . $\therefore \mathbb{Z}_6$ is cyclic and $[1]$ is a cyclic generator. $[5]$ is also a cyclic generator! However, $[0]$, $[2]$, $[3]$, and $[4]$ are not cyclic generators of \mathbb{Z}_6 .

- We now know:
1. Not all groups are cyclic
 2. When a group is cyclic, it may have more than one cyclic generator.

Let's explore further. Let G be a finite group of order n with cyclic generator x . Every element in G is a power of x . In particular, e is a power of x . Suppose $o(x) = j$.

$$\begin{aligned} \text{Consider : } \quad x^{j+1} &= x^j \cdot x = e \cdot x = x \\ x^{j+2} &= x^j \cdot x^2 = x^2 \\ &\vdots \\ &\vdots \\ &\vdots \\ x^{j+(j-1)} &= x^j \cdot x^{j-1} = e \cdot x^{j-1} = x^{j-1} \end{aligned}$$

Continuing in like manner (consider x^{j+j} yourself), we see that the only elements generated by x are $\{e, x, x^2, \dots, x^{j-1}\}$ which is a set with at most j elements. If $j < n$, x can't be a cyclic generator for G . Suppose $j > n$. By closure, all of the elements in the set $\{e, x, x^2, \dots, x^{j-1}\}$ are in G . Since j is assumed to be larger than n , there has to be duplication of entries in this set. Suppose $x^s = x^t$ where both s and t are less than or equal to $j - 1$ and $s < t$. As we have seen previously, x^{t-s} must equal e . However, $t - s$ is also less than $j - 1$ contradicting the fact that the order of x is j . We can now deduce that $o(x)$ can't be larger than n or smaller than n . $\therefore o(x) = n$

Consider the set $\{e, x, x^2, \dots, x^{n-1}\}$. Using the same techniques used in the last paragraph, it is easy to prove that this set has n distinct elements (no duplication).

$$\therefore G = \{e, x, x^2, \dots, x^{n-1}\}$$

A table for G would be:

G	e	x	x^2	\dots	x^{n-1}
e	e	x	x^2		x^{n-1}
x	x	x^2	x^3		e
x^2	x^2	x^3	x^4		x
\vdots					
x^{n-1}	x^{n-1}	e	x		x^{n-2}

Compare this table to the one for \mathbb{Z}_n :

\mathbb{Z}_n	[0]	[1]	[2]	\dots	[$n-1$]
[0]	[0]	[1]	[2]		[$n-1$]
[1]	[1]	[2]	[3]		[0]
[2]	[2]	[3]	[4]		[1]
\vdots					
[$n-1$]	[$n-1$]	[0]	[1]		[$n-2$]

They are isomorphic copies of each other! Therefore, except for isomorphic copies, the only finite cyclic groups are the groups $\mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3$, etc. This family of groups can now be called the cyclic groups.

Finally, let's use our theory to discover how many different (non-isomorphic) groups there are of order 4. Let $G = \{e, a, b, c\}$. By previous theorem, there exists at least one element of G that is a non-trivial self-invertible element. Without loss of generality (wolog), we can assign that role to b (a, b and c at this point are indistinguishable).

Therefore a table for G begins:

G	e	a	b	c
e	e	a	b	c
a	a			
b	b		e	
c	c			

What are the inverses of a and c ? There are only 2 possibilities. Either they are inverses of each other or they are both self-invertible. This results in 2 possible tables:

G_1	e	a	b	c
e	e	a	b	c
a	a			e
b	b		e	
c	c	e		

G_2	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

LHC and RHC allows us to complete both tables with no further information:

G_1	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

G_2	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Look at your group cards. G_1 is clearly an isomorphic copy of Z_4 . G_2 is clearly an isomorphic copy of K_4 . Therefore, the only groups (except for isomorphic copies) of order 4 are Z_4 and K_4 .