

## Finding Subgroups Within Groups

LaGrange's Theorem guarantees that if  $S$  is a subgroup of a finite group  $G$  then  $o(S)$  is a divisor of  $o(G)$ . A group of order 12 can only have subgroups whose orders are 1, 2, 3, 4, 6, or 12. The converse of LaGrange's Theorem is false unfortunately. To be specific "If  $G$  is a finite group and  $n$  is a divisor of  $o(G)$  then  $G$  contains a subgroup of order  $n$ " is not true. Therefore, we can not be sure that a group of order 12 has any subgroups of order 6. This chapter will be devoted to discovering partial converses to LaGrange's Theorem. A huge amount of research time has been expended searching for situations that guarantee subgroups of certain orders within finite groups. The highlight of the chapter will be the classic Sylow Theorems.

The first result we need, was an exercise in a previous chapter. It is needed to establish the first result of significance to the theme of this chapter.

**Theorem:** If any element of a group  $G$  is self invertible then the group must be abelian.

**Proof:** Let  $a$  and  $b$  be elements of  $G$ . By the given  $a^2 = e$  and  $b^2 = e$ . By closure,  $ab \in G$ .  $\therefore (ab)^2 = e$

$$\begin{aligned}\therefore abab &= e \\ a^2bab &= a \\ bab &= a \\ bab^2 &= ab \\ ba &= ab\end{aligned}$$

Since  $a$  and  $b$  were arbitrary,  $G$  is abelian.

**QED**

In the body of the proof of the next theorem, we establish for the first time the existence of a subgroup of a certain order within a finite group.

**Theorem:** The only nonabelian group of order 6 is  $D_3$ .

**Proof:** Let  $G$  be a nonabelian group of order 6. Each element in  $G$  has order 1, 2, 3 or 6. The only element of order 1 is  $e$ . If  $G$  possesses an element of order 6 then  $G$  must be abelian. Hence  $G$  has no elements of order 6. If all of the elements of  $G$  (except  $e$ ) have order 2 then  $G$  must be abelian by our previous theorem. Hence  $G$  must possess at least one element of order 3. Let that element be called  $b$ . Hence  $G$  possesses a subgroup of order 3  $\{e, b, b^2\}$ .

Let  $a$  be an element of  $G$  that is not in the subgroup  $\{e, b, b^2\}$ . Hence  $G$  contains the subset  $\{e, a, b, b^2\}$ . Consider  $ab$ . Is this element also in the subset named previously?

If  $ab = e$  then  $a = b^2 \longrightarrow \longleftarrow$   
 If  $ab = a$  then  $b = e \longrightarrow \longleftarrow$   
 If  $ab = b$  then  $a = e \longrightarrow \longleftarrow$   
 If  $ab = b^2$  then  $a = b \longrightarrow \longleftarrow$   
 $\therefore ab \notin \{e, a, b, b^2\}$

Hence  $G$  contains the subset of distinct elements  $\{e, a, b, b^2, ab\}$ . Consider  $ab^2$ . Is this element in the subset of  $G$  we have constructed so far?

If  $ab^2 = e$  then  $a = b \longrightarrow \longleftarrow$   
 If  $ab^2 = a$  then  $b^2 = e \longrightarrow \longleftarrow$   
 If  $ab^2 = b$  then  $ab = e \longrightarrow \longleftarrow$   
 If  $ab^2 = b^2$  then  $a = e \longrightarrow \longleftarrow$   
 If  $ab^2 = ab$  then  $b = e \longrightarrow \longleftarrow$   
 $\therefore ab^2 \notin \{e, a, b, b^2, ab\}$   
 $\therefore G$  contains precisely the distinct elements  $e, a, b, b^2, ab$  and  $ab^2$ .

Consider  $ba$ .

If  $ba = e$  then  $a = b^2 \longrightarrow \longleftarrow$   
 If  $ba = a$  then  $b = e \longrightarrow \longleftarrow$   
 If  $ba = b$  then  $a = e \longrightarrow \longleftarrow$   
 If  $ba = b^2$  then  $a = b \longrightarrow \longleftarrow$

Suppose  $ba = ab$ . This would imply that the group is abelian. (Try all products of two elements in the order  $x \cdot y$  and the order  $y \cdot x$ .)

$\therefore ba \neq e, a, b, b^2$  or  $ab$   
 $\therefore ba = ab^2$

Consider  $a^2$ .

If  $a^2 = a$  then  $a = e \longrightarrow \longleftarrow$   
 If  $a^2 = b$  then  $a^3 = ba$   
 $\therefore a^3 = ab^2$   
 $\therefore a^2 = b^2$   
 $\therefore b = b^2 \longrightarrow \longleftarrow$   
 If  $a^2 = b^2$  then  $a^3 = b \cdot ba$   
 $\therefore a^3 = bab^2$   
 $\therefore a^3 = ab^4$   
 $\therefore a^3 = ab$   
 $\therefore a^2 = b$   
 $\therefore b^2 = b \longrightarrow \longleftarrow$

$$\begin{aligned} \text{If } a^2 = ab \text{ then } a = b &\longrightarrow \longleftarrow \\ \text{If } a^2 = ab^2 \text{ then } a = b^2 &\longrightarrow \longleftarrow \\ \therefore a^2 \neq a, b, b^2, ab \text{ or } ab^2 & \\ \therefore a^2 = e & \end{aligned}$$

We now know:

1.  $G$  consists of the distinct elements  $e, a, b, b^2, ab$  and  $ab^2$
2.  $b^3 = e$
3.  $a^2 = e$
4.  $ba = ab^2$

These are the defining equations for  $D_3$ !

$$\therefore G = D_3$$

**QED**

The proof just completed establishes that  $D_3$  is isomorphic to  $S_3$ . This result was established earlier in this text by brute force. However, we have established a much stronger result. There are no nonabelian groups of order 6 that are not isomorphic to  $D_3$ .

**Corollary:** There are only two non-isomorphic groups of order 6.

**Proof:** By the Fundamental Theorem of Abelian groups, the only abelian group of order 6 is  $Z_6$  (recall that  $Z_2 \times Z_3$  is isomorphic to  $Z_6$  since 2 and 3 are relatively prime). Our previous theorem established that the only nonabelian group of order 6 is  $D_3$ .

**QED**

**Theorem:** If  $o(G) = n$  where  $G$  is an abelian group and the prime number  $p$  is a divisor of  $n$  then  $G$  contains a subgroup of order  $p$ .

**Proof:** We will execute this proof by using the strong form of induction. If  $o(G) = 2$  then  $p = 2$  and the group itself is the subgroup we seek.

Now assume:

1.  $o(G) = n$
2. The prime number  $p$  is a divisor of  $n$
3. Whenever the prime number  $p$  is a divisor of the order of a group with less than  $n$  elements, that group has a subgroup of order  $p$ .

We must prove  $G$  has a subgroup with  $p$  elements. Let  $a$  be an element of  $G$  where  $a \neq e$ . Let  $o(a) = r$ . Either  $p$  is a divisor of  $r$  or  $p$  is not a divisor of  $r$ .

### Case I -- $p$ is a divisor of $r$

If  $r = p$  then the set  $\{e, a, a^2, a^3, \dots, a^{p-1}\}$  is a subgroup of order  $p$  in  $G$ .

If  $r = kp$  where  $k \geq 2$ ,  $e = a^r = a^{k \cdot p} = (a^k)^p$ . Since  $p$  is a prime number,  $o(a^k) = 1$  or  $o(a^k) = p$ . If  $o(a^k) = 1$  then  $a^k = e$  where  $k < r$ . This is a contradiction of the fact that  $o(a) = r$ .  $\therefore o(a^k) = p$ . Let  $b = a^k$ . The set  $\{e, b, b^2, \dots, b^{p-1}\}$  is a subgroup of order  $p$  in  $G$ .

### Case II -- $p$ is not a divisor of $r$

Let  $A = \{e, a, a^2, \dots, a^{r-1}\}$ .  $A$  is a normal subgroup of  $G$  since  $G$  is abelian. Construct  $G/A$ .  $o(G) = o(A) \cdot o(G/A)$ .

Since  $p$  is a divisor of  $o(G)$  and  $p$  is not a divisor of  $o(A)$ ,  $p$  must be a divisor of  $o(G/A)$ .  $G/A$  is a group whose order is less than  $o(G)$ .  $\therefore$  there exists a subgroup with order  $p$  in  $G/A$  by our induction assumption. This subgroup must be cyclic. Let  $Ax$  be a cyclic generator of this order  $p$  subgroup of  $G/A$ .

$$\begin{aligned}\therefore (Ax)^p &= A \\ \therefore x^p &\in A \\ \therefore x^p &= a^s \text{ for some } s \leq r \\ (x^r)^p &= (x^p)^r = (a^s)^r = (a^r)^s = e \\ \therefore o(x^r) &= p \text{ or } o(x^r) = 1 \\ \text{If } o(x^r) &= 1 \text{ then } x^r = e \\ \therefore (Ax)^r &= A\end{aligned}$$

Since  $o(Ax) = p$ ,  $r$  must be a multiple of  $p$ .

$\therefore p$  is a divisor of  $r$ .  $\longrightarrow \longleftarrow$

$\therefore o(x^r) = p$

Let  $c = x^r$ .

The subset  $\{e, c, c^2, \dots, c^{p-1}\}$  is a subgroup of  $G$  of order  $p$ .

**QED**

We need the previous result to prove the more general result that now follows. Note that the premise is the same as the previous theorem except that the abelian condition is omitted.

**Cauchy's Theorem:** Let  $G$  be a finite group. If  $o(G) = n$  and the prime number  $p$  is a divisor of  $n$  then  $G$  contains a subgroup of order  $p$ .

**Proof:** We make use again of induction in its strong form. If  $o(G) = 2$  then  $G$  is abelian and our previous theorem establishes the result.

Now suppose:

1.  $o(G) = n$
2.  $p$  is a divisor of  $n$
3. This theorem hold for all groups with order less than  $n$

If  $G$  is abelian, our previous theorem establishes the result. If  $G$  is not abelian,  $o(Z) < o(G)$ .

By the class equation:

$$o(G) = o(Z) + \sum o(G/C(a))$$

If  $p$  is a divisor of  $Z$ , our induction assumption guarantees a subgroup of  $Z$  with order  $p$ . This set would also be a subgroup of  $G$  and we are done.

Assume  $p$  is not a divisor of  $o(Z)$ . Let  $a \notin Z$ . If  $p$  is a divisor of  $C(a)$  then  $C(a)$  contains a subgroup of order  $p$  by our induction assumption since  $o(C(a)) < o(G)$ . the set would also be a subgroup of  $G$  and we are done.

Assume  $p$  is not a divisor of  $C(a)$  for any  $a$  not in the center. We note that  $o(G) = o(C(a)) \cdot o(G/C(a))$ . [ $G/C(a)$  could either be the right cosets generated by  $C(a)$  or the left cosets.]

Since  $p$  is a divisor of  $o(G)$ ,  $p$  must be a divisor of  $o(C(a)) \cdot (G/C(a))$ . Since  $p$  is prime and  $p$  is not a divisor of  $o(C(a))$ ,  $p$  has to be a divisor of  $o(G/C(a))$  for every  $a \notin Z$ .

Let's return to the class equation:

$$o(G) = o(Z) + \sum o(G/C(a))$$

$$\Rightarrow o(G) - \sum o(G/C(a)) = o(Z)$$

$p$  is a divisor of every term on the left.

$\therefore p$  is a divisor of the left side of this equation.

$\therefore p$  is a divisor of  $o(Z)$ .

$Z$  is an abelian group. By our last theorem, there exists a subgroup of order  $p$  in  $Z$ . This set must also be a subgroup of  $G$ .

**QED**

Note that we have done more than prove the group has a subgroup of order  $p$ . We also have proven that the group has an element of order  $p$ .

We still have no guarantee that a group of order 24 has a subgroup of order 6 but we do know it must have subgroups of order 2 and 3. The next set of theorems are some of the most important, classic results in group theory. Their existence dates back to the late nineteenth century.

**Lemma 1:** Let  $f : G_1 \rightarrow G_2$  be a group homomorphism. Let  $N_2$  be a normal subgroup of  $G_2$ . The set  $N_1 = f^{-1}(N_2)$  consisting of all elements in  $G_1$  that are pre-images of elements in  $N_2$  is a normal subgroup of  $G_1$ .

**Proof:**

**Closure**

Let  $x \in N_1$  and  $y \in N_1$

Consider  $f(xy) = f(x) \cdot f(y)$

Since  $f(x) \in N_2$  and  $f(y) \in N_2$ ,  $f(x) \cdot f(y) \in N_2$

$\therefore xy \in N_1$

**Inverse Closure**

Let  $x \in N_1$

Consider  $f(x^{-1}) = [f(x)]^{-1}$ . Since  $f(x) \in N_2$ ,  $[f(x)]^{-1} \in N_2$

$\therefore x^{-1} \in N_1$

**NTE**

Let  $x \in N_1$  and  $g \in G$

$f(gxg^{-1}) = f(g)f(x)[f(g)]^{-1}$

Since  $f(x) \in N_2$  and  $f(g) \in G_2$ ,  $f(g)f(x)[f(g)]^{-1} \in N_2$

$\therefore gxg^{-1} \in N_1$

**QED**

Note that if  $N_2$  is only a subgroup of  $G_2$ , our first and second steps guarantee that  $f^{-1}(N_2)$  is a subgroup of  $G_1$ .

**Lemma 2:** Let  $N$  be a normal subgroup of the group  $G$ . Every subgroup of  $G/N$  has the form  $H/N$  where  $H$  is a subgroup of  $G$ .

**Proof:** Let  $f : G \rightarrow G/N$  be defined by  $f(x) = Nx$ . We have seen previously that  $f$  is a homomorphism.