Recall that Lagrange’s Theorem and its Corollary puts restrictions on the order of subgroups and elements of a group.

We can use these restrictions to completely classify finite groups whose orders are prime.  

**Theorem 8.7.** For a positive prime integer $p$, every group of order $p$ is isomorphic to $\mathbb{Z}_p$.

**Proof.** Let $G$ be a group of order $p$.

Since $p \geq 2$, there is non-identity element $a$ in $G$.

The cyclic subgroup $\langle a \rangle$ has order $|a|$ that is greater than 1 and divides $p$, the order of $G$ (by Lagrange’s Theorem).

Since $p$ is prime and $|a| > 1$, the order $|a|$ must be $p$.

Thus $G = \langle a \rangle$, so that $G$ is a cyclic group of order $p$.

Any cyclic group of order $p$ is isomorphic to $\mathbb{Z}_p$ (by Theorem 7.19 Ed.3). $\square$

We can use Lagrange’s Theorem and its Corollary to classify some finite groups whose orders are not prime.

**Theorem 8.8.** Every group $G$ of order 4 is isomorphic to either $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

**Proof.** Let $G$ be a group of order 4.


Then $\langle a \rangle$ has order 4 and must be all of $G$.

Thus $G$ is isomorphic to $\mathbb{Z}_4$ (by Theorem 7.19 Ed.3).

Case 2. Suppose $G$ has no element of order 4.

Let $e, a, b, c$ be the four elements of $G$.

The only element of $G$ has order 1 is the identity element $e$.

Since no element of $G$ has order 4, then the orders of $a, b, c$ must each be 2 by Lagrange’s Theorem.

Thus we have the following partial binary operation table for $G$.

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td></td>
<td>e</td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>e</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We fill in the table using previous theory that states that each element of the group appears exactly once in each row and in each column, and applications of the cancelation law.

For instance, the product $ba$ can not be $e$ or $a$, so it is either $ba = b$ (which implies that $a = e$, a contradiction), or $ba = c$, the only option left.

Using similar arguments we complete the binary operation table for $G$.

<table>
<thead>
<tr>
<th>·</th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>e</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>e</td>
</tr>
</tbody>
</table>

The function $f : G \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ given by

$$f(e) = (0, 0), \ f(a) = (1, 0), \ f(b) = (0, 1), \ f(c) = (1, 1)$$

is an isomorphism, whence $G$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

\[\square\]

**Theorem 8.9.** Every group of order 6 is isomorphic to $\mathbb{Z}_6$ or $S_3$.

The proof of this is a lengthy exercise in constructing the table for a group of order 6 when it is not cyclic, and showing that the table is that of $S_3$.

The groups of order 2 through 7 are

$\mathbb{Z}_2, \ \mathbb{Z}_3, \ \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2, \ \mathbb{Z}_5, \ \mathbb{Z}_6$ or $S_3 \cong D_3$, and $\mathbb{Z}_7$.

To classify finite groups of composite order beyond 7 requires developing more tools, the next of which is normal subgroups.

We know for a subgroup $K$ of a group $G$ that the right cosets of $K$ in $G$ form a partition of $G$.

We determine when we can place a group structure on the set of right cosets of $K$ in $G$.

At issue is the problem of whether $a \equiv b \pmod{K}$ and $c \equiv d \pmod{K}$ implies $ac \equiv bd \pmod{K}$ or not.

In the right coset notation, we are asking if $Ka = Kb$ and $Kc = Kd$ implies $Kac = Kbd$.

**Exploration.** For a subgroup $K$ of a group $G$, we consider for $a, c \in G$ the “product” of right cosets

$$(Ka)(Kc) = Kac.$$

For $b, d \in G$ we have

$$(Kb)(Kd) = Kbd.$$

If $a \equiv b \pmod{K}$ and $c \equiv d \pmod{K}$, does $Kac = Kbd$?

This is the question of whether this “product” is well-defined.
With $Ka = Kb$ and $Kc = Kd$ we have $r = ab^{-1} \in K$ and $s = cd^{-1} \in K$.

We know that $Kac = Kbd$ if and only if $ac \equiv bd \pmod{K}$ if and only if $(ac)(bd)^{-1} \in K$.

Here we have

$$(ac)(bd)^{-1} = acd^{-1}b^{-1} = asb^{-1}.\]

We do not know at this point if $asb^{-1}$ is in $K$ or not.

Notice that $as$ is the product of $a$ and an element $s \in K$.

That is, the product $as$ belongs to the left coset $aK$ of $K$ in $G$.

If we knew that $as = ta$ for some $t \in K$, then $asb^{-1} = tab^{-1} = tr \in K$ because $t, r \in K$ and $K$ is a subgroup.

This would happen if we knew that $Ka = aK$ for all $a \in G$, from which it follows that the product $(Ka)(Kb) = Kab$ is well-defined on the set of right cosets of $K$ in $G$.

**Definition.** A subgroup $N$ of a group $G$ is said to be normal if $Na = aN$ for all $a \in G$.

**Warning:** the condition $Na = aN$ does not say that $na = an$ for all $n \in N$.

Rather it says that for each $n \in N$ there exist $m \in N$ such that $na = am$.

Only in one very special case does $Na = aN$ imply $na = an$ for all $n \in G$, and that is when $G$ is abelian.

**Examples.** (a) Every subgroup of an abelian group is normal.

(b) Is the subgroup $K = \{(1), (123), (132)\}$ of the nonabelian group $S_3$ normal?

The six elements of $S_6$ are $(1)$, $(12)$, $(13)$, $(23)$, $(123)$, and $(132)$.

We check for the equality of the left and right cosets of $K$ in $S_3$.

$$
K(1) = \{(1), (123), (132)\} \quad \quad (1)K = \{(1), (123), (132)\},
K(12) = \{(12), (13), (23)\} \quad \quad (12)K = \{(12), (23), (13)\},
K(13) = \{(13), (23), (12)\} \quad \quad (13)K = \{(13), (12), (23)\},
K(23) = \{(23), (12), (13)\} \quad \quad (23)K = \{(23), (13), (12)\},
K(123) = \{(123), (132), (1)\} \quad \quad (123)K = \{(123), (1), (132)\},
K(132) = \{(132), (1), (123)\} \quad \quad (132)K = \{(132), (1), (123)\}.
$$

Since $Ka = aK$ for all $a \in S_3$, the subgroup $K$ is normal.

(c) Recall that the center of a group $G$ is the subgroup

$$Z(G) = \{c \in G : gc = cg \text{ for all } g \in G\}.$$

For any $a \in G$, we have that $ca = ac$ for all $c \in Z(G)$, so that $Z(G)a = aZ(G)$ for all $a \in G$, whence $Z(G)$ is normal.

(d) Is the subgroup $K = \{(1), (23)\}$ normal in $S_3$?

Well $K(12) = \{(12), (132)\}$ and $(12)K = \{(12), (123)\}$ are not the same, so $K$ is not normal.