17  Lagrange’s Theorem

A very important corollary to the fact that the left cosets of a subgroup partition a group is Lagrange’s Theorem. This theorem gives a relationship between the order of a finite group $G$ and the order of any subgroup of $G$ (in particular, if $|G| < \infty$ and $H \subseteq G$ is a subgroup, then $|H| \mid |G|$).

**Theorem 17.1 (Lagrange’s Theorem)**

Let $G$ be a finite group, and let $H$ be a subgroup of $G$. Then the order of $H$ divides the order of $G$.

**Proof.**

By Theorem 16.1, the right cosets of $H$ form a partition of $G$. Thus, each element of $G$ belongs to at least one right coset of $H$ in $G$, and no element can belong to two distinct right cosets of $H$ in $G$. Therefore every element of $G$ belongs to exactly one right coset of $H$. Moreover, each right coset of $H$ contains $|H|$ elements (Lemma 16.2). Therefore, $|G| = n|H|$, where $n$ is the number of right cosets of $H$ in $G$. Hence, $|H| \mid |G|$. This ends a proof of the theorem. ■

**Example 17.1**

If $|G| = 14$ then the only possible orders for a subgroup are $1, 2, 7,$ and $14$. ■

**Definition 17.1**

The number of different right cosets of $H$ in $G$ is called the **index** of $H$ in $G$ and is denoted by $[G : H]$.

It follows from the above definition and the proof of Lagrange’s theorem that


**Example 17.2**

Since $|S_3| = 3! = 6$ and $|(12)| = |< (12) >| = 2$ then $[S_3, < (12) >] = \frac{6}{2} = 3$. ■
The rest of this section is devoted to consequences of Lagrange’s theorem; we begin with the order of an element.

**Corollary 17.1**
If \( G \) is a finite group and \( a \in G \) then \( o(a) \mid |G| \).

**Proof.**
Since \(<a>\) is a subgroup of \( G \), then \(|<a>|\mid |G|\). By Theorem 14.7, \( o(a) = |<a>| \). Hence, \( o(a) \mid |G| \). □

**Corollary 17.2**
If \( G \) is a finite group and \( a \in G \) then \( a^{|G|} = e \).

**Proof.**
By the previous corollary, \( o(a) \mid |G| \). Thus, \(|G| = k \cdot o(a)\) for some positive integer \( k \). Hence, \( a^{|G|} = a^{k \cdot o(a)} = (a^{o(a)})^k = e^k = e \). □

**Corollary 17.3** *(Euler’s Theorem)*
If \( a \) and \( n \) are positive integers such that \( gcd(a, n) = 1 \) then \( a^{\phi(n)} \equiv 1 \pmod{n} \).

**Proof.**
By Theorem 13.4, \(|U_n| = \phi(n)\). By the previous corollary, \([a]^{[U_n]} = [a]^{\phi(n)} = [1]\). Since \([a]^{\phi(n)} = [a^{\phi(n)}] = [1]\) then \( a^{\phi(n)} \equiv 1 \pmod{n} \). □

**Corollary 17.4** *(Fermat’s Little Theorem)*
If \( p \) is a prime number and \( p \not|a\) then

1. \( a^{p-1} \equiv 1 \pmod{p} \)
2. \( a^p \equiv a \pmod{p} \) for all \( a \in \mathbb{N} \).

**Proof.**
1. Since \( p \) is prime then \( \phi(p) = p - 1 \) by Theorem 13.5. Since \( p \not|a\) then \( gcd(a, p) = 1 \). By Euler’s theorem we have \( a^{p-1} \equiv 1 \pmod{p} \).
2. From part (i), we have \( a^{p-1} - 1 = pt \) for some integer \( t \). Thus, \( a^p - a = pt' \) where \( t' = ta \in \mathbb{Z} \). Hence, \( a^p \equiv a \pmod{p} \). □

The above theorem suggests a test of primality for \( p \). Take a number \( n \) such that \( p \not|n \) and raise it to the \((p - 1)\)st power and find its remainder when divided by \( p \). If the remainder is not \( 1 \) then we can conclude that \( p \) is not a prime number.
Corollary 17.5
If \(|G| = p\), where \(p\) is prime then the only subgroups of \(G\) are \(\{e\}\) and \(G\).

**Proof.**
Suppose the contrary, that is \(G\) has a subgroup \(H\) such that \(H \neq \{e\}\) and \(H \neq G\). By Theorem 17.1, \(|H||G|\) with \(1 < |H| < p\). This contradicts the fact that \(p\) is prime. ■

Corollary 17.6
If \(G\) is a group of prime order then it is cyclic. That is, \(G = < a >\) where \(a\) is any nonidentity element of \(G\).

**Proof.**
Let \(a \in G\) with \(a \neq e\). Then \(< a > \neq \{e\}\). By the previous corollary, \(G = < a >\). ■

Example 17.3
The previous corollary tells that groups of prime order are always cyclic. What about groups of prime-squared order? The group

\[\mathbb{Z}_2 \times \mathbb{Z}_2 = \{([0], [0]), ([0], [1]), ([1], [0]), ([1], [1])\}\]

has order \(4 = 2^2\). Since each element has order 2 then by Theorem 14.7, \(\mathbb{Z}_2 \times \mathbb{Z}_2\) is not cyclic. ■

Example 17.4
Lagrange’s Theorem greatly simplifies the problem of determining all the subgroups of a finite group. For example, consider the group \((\mathbb{Z}_6, \oplus)\). Aside from \(\{[0]\}\) and \(\mathbb{Z}_6\) any subgroup of \(\mathbb{Z}_6\) must have order 2 or 3. There is only one subgroup of order 2, \(< [3] >\). Also, there is only one subgroup of order 3, \(< [2] >\). A subgroup lattice shows the subgroups of \(\mathbb{Z}_6 = < [1] >\) and the inclusion relation between them.

![Subgroup Lattice](image-url)
The Converse of Lagrange’s Theorem
The converse of Lagrange’s theorem is not true in general. That is, if $n$ is a divisor of $G$ then it does not necessarily follow that $G$ has a subgroup of order $n$.

Example 17.5
The set of all even permutations

\[ A_4 = \{(1), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\} \]

is a subgroup of $S_4$ (and therefore a group itself) of order 12 (See Theorem 7.9). Note that $A_4$ has three elements of order 2, namely,

\[ \{(12)(34), (13)(24), (14)(23)\} \]

and 8 elements of order 3,

\[ (123), (132), (124), (142), (134), (143), (234), (243) \}

We will show that $A_4$ has no subgroup of order 6.

Let $H$ be a subgroup of $A_4$ of order 6. Then $(1) \in H$. Since $A_4$ contains only 3 elements of order 2 then $H$ must contain at least one element of order 3 of the form $(abc)$. Then by closure, $(acb) = (abc)(abc) \in H$. If $H$ also contains an element, say of the form $(ab)(cd)$ (or of the form $(abd)$), then by closure $(abc)(ab)(cd) = (acd) \in H$ and $(acb)(ab)(cd) = (bcd)$. Thus, $(bcd)^{-1} = (bdc) \in H$. In either case, $H$ has more than six elements. Thus, $A_4$ has no subgroup of order 6.

The converse of Lagrange’s theorem is valid for cyclic groups. To prove this result we need the following two theorems.

Theorem 17.2
Let $G$ be a finite cyclic group of order $n$ and generator $a$. That is, $G = \{e, a, a^2, \ldots, a^{n-1}\}$

Every subgroup of $G$ is cyclic. That is, a subgroup of a cyclic group is also cyclic.
Proof.
Let $H$ be a subgroup of $G$. Then elements of $H$ are of the form $a^k$ with $1 \leq k < n$. Let $t$ be the smallest positive integer such that $a^t \in H$. We shall prove that $H = \langle a^t \rangle$. Indeed, let $a^m \in H$. By the Division Algorithm there exist unique integers $q$ and $r$ such that $m = tq + r$ where $0 \leq r < t$. It follows that $a^m = (a^t)^q a^r$ or $a^r = a^m (a^t)^{-q}$. But $a^m \in H$ and $a^t \in H$ then by closure $a^r \in H$. Since $t$ is the smallest positive integer such that $a^t \in H$ then we must have $r = 0$. Hence, $a^m = (a^t)^q$ or $a^m \in \langle a^t \rangle$. Clearly, $\langle a^t \rangle \subseteq H$ since $a^t \in H$ and $H$ is a group.

**Theorem 17.3**
Let $G$ be as in the statement of Theorem 17.2. If $1 \leq k < n$ then $a^k$ generates a subgroup of order $\frac{n}{\gcd(k,n)}$.

**Proof.**
Let $d = \gcd(k,n)$. By Theorem 14.6(i), $| \langle a^k \rangle |$ is the smallest positive integer such that $a^{k|\langle a^k \rangle|} = e$. By Theorem 14.6 (ii), $n | k | \langle a^k \rangle |$. That is, $k | \langle a^k \rangle | = nq$ for some integer $q$. Hence, $\frac{k|\langle a^k \rangle|}{d} = \frac{nq}{d}$ so that $\frac{n}{d} | \frac{k|\langle a^k \rangle|}{d}$. Since $\gcd(\frac{n}{d}, \frac{k}{d}) = 1$ then by Lemma 13.1, we have $\frac{n}{d} | \langle a^k \rangle |$. On the other hand, $(a^k)^\frac{n}{d} = (a^n)^\frac{k}{d} = e$ so that $| \langle a^k \rangle | \frac{n}{d}$. Hence, by Theorem 10.2(d), $| \langle a^k \rangle | \leq \frac{n}{d}$. ■

**Theorem 17.4**
Let $G$ be a cyclic group of order $n$ and generator $a$. For each positive divisor $d$ of $n$, $G$ has exactly one subgroup of order $d$.

**Proof.**
**Existence:** Let $d$ be a positive divisor of $n$. Then there exists a positive integer $q < n$ such that $n = dq$. Thus, $q|n$ and $\gcd(n,q) = q$. By Theorem 17.3, $a^q$ generates a subgroup of $G$ of order $\frac{n}{\gcd(n,q)} = \frac{n}{q} = d$. Thus, $G$ has at least one subgroup of order $d$.

**Uniqueness:** Suppose that $G$ has two subgroups of order $d$, say $H$ and $K$. We will show that $H = K$. Let $1 \leq m < n$ be the smallest positive integer such that $a^m \in H$ and $1 \leq k < n$ be the smallest positive integer such that $a^k \in K$. As in the proof of Theorem 17.2, we establish that $H = \langle a^m \rangle$ and $K = \langle a^k \rangle$. By Theorem 17.3, $| \langle a^m \rangle | = \frac{n}{\gcd(n,m)}$ and $| \langle a^k \rangle | = \frac{n}{\gcd(n,k)}$. Thus, $\frac{n}{\gcd(n,m)} = \frac{n}{\gcd(n,k)} = d$ or $\gcd(n,m) = \gcd(n,k)$.
Now, by the Division Algorithm, \( n = mq + r \) with \( 0 \leq r < m \). Since \( a^n = e \in H \) then \( a^r = (a^m)^{-q} \in H \). From the definition of \( m \) we see that \( r = 0 \). Hence, \( n = mq \) and \( m|n \). It follows that \( gcd(n, m) = m \). A similar argument shows that \( gcd(n, k) = k \) and therefore \( m = k \). Hence, \( <a^m> = <a^k> \), i.e. \( H = K \). This ends a proof of the theorem.\( \blacksquare \)

**Remark 17.1**
The converse of Lagrange’s theorem holds also for finite Abelian groups. This topic will not be covered in this book.

**Example 17.6**
Consider the group \((\mathbb{Z}_{12}, \oplus)\). Since \(|\mathbb{Z}_{12}| = 12\) then the positive divisors of 12 are 1, 2, 3, 4, 6, and 12. The subgroup lattice below shows the different subgroups of \( \mathbb{Z}_{12} = <[1]> \).

![Subgroup Lattice](image_url)

6