Proof: If $aH \cap bH = \phi$ for two left cosets aH and bH, there is nothing to prove.

Let $aH \cap bH \neq \phi$. So let $p \in aH \cap bH$. Then $\exists\ h_1, h_2 \in H$ such that $p = ah_1$ and $p = bh_2$

So $p = ah_1 = bh_2 \Rightarrow a = bh_2h_1^{-1}$ and $b = ah_1h_2^{-1}$

Let $x \in aH \Rightarrow x = ah_3,\ h_3 \in H$

$$= (bh_2h_1^{-1})h_3 = b(h_2h_1^{-1}h_3) = bh_4$$

where $h_4 = h_2h_1^{-1}h_3 \in H$, as H is a subgroup

So, $x \in bH$. So, $aH \subset bH$

Similarly, $bH \subset aH$. So, $aH = bH$

Theorem 4.4 Let G be a group and H be a subgroup of G. Let $a, b \in G$. Then $aH = bH$ if and only if $a^{-1}b \in H$.

Proof: Let $aH = bH$. Then $ah_1 = bh_2$ for some $h_1, h_2 \in H$

So, $a^{-1}b = h_1h_2^{-1} \in H$, as H is a subgroup.

Conversely, let $a^{-1}b \in H$. Then $a^{-1}b = h$ for some $h \in H$

So, $b = ah \Rightarrow b \in aH$. But $b \in bH$

So, $b \in aH \cap bH$. So $aH \cap bH \neq \phi$. So, $aH = bH$ by Theorem 4.3.

Theorem 4.5 Let H be a subgroup of a group G and $a, b \in G$

Then $b \in aH$ if and only $a^{-1}b \in H$

Proof: Let $b \in aH \Rightarrow b = ah$, for some $h \in H$, So, $a^{-1}b = h \in H$

Conversely, let $a^{-1}b \in H$. Then $a^{-1}b = h_1$ for some $h_1 \in H$.

So, $b = ah_1$. So $b \in aH$.

Note: So, we see that if H be a subgroup of a group G, the following conditions are equivalent: For $a, b \in G$

(i) $b \in aH$ (ii) $a^{-1}b \in H$ (iii) $aH = bH$.

Theorem 4.6 Let H be a subgroup of a group G. The relation R defined by "$(a, b) \in R$ or aRb if and only if $a^{-1}b \in H$" for $a, b \in G$ is an equivalence relation on G.

Proof: For every $a \in H$, aRa holds as $a^{-1}a = e \in H$ (e is the identity element in G and H is a subgroup). So R is reflexive.

For $a, b \in G$, $aRb \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H$ (Since H is a subgroup)
$\Rightarrow b^{-1}a \in H \Rightarrow bRa$

So, R is symmetric.

For $a, b, c \in G$, aRb and $bRc \Rightarrow a^{-1}b \in H$ and $b^{-1}c \in H$
$\Rightarrow (a^{-1}b)(b^{-1}c) \in H$ (Since H is a subgroup)
$\Rightarrow a^{-1}c \in H \Rightarrow aRc$

So, R is transitive. Since R is reflexive, symmetric and transitive, it is an equivalence relation on G.

Remark 1: For each theorem corresponding to left cosets, there is a similar theorem related to right cosets.

Remark 2: So, G is partitioned by R into equivalence classes and each class is a left coset of H, because, for $a \in G$,

$$cl(a) = \{x \in G : aRx\} = \{x \in G : a^{-1}x \in H\} = \{x \in G : x \in aH\} = aH$$

Theorem 4.7 Any two left cosets of a subgroup H in a group G have the same cardinality, i.e., $\exists$ a bijective mapping between any two left cosets.

Proof: Let aH and bH be two left cosets of H in G. Let us define a mapping $f: aH \to bH$ by $f(ah) = bh$ for every $ah \in aH$

Let ah_1 and ah_2 be in H and $f(ah_1) = f(ah_2) \Rightarrow bh_1 = bh_2$
$\Rightarrow h_1 = h_2$ (left cancellation law)
$\Rightarrow ah_1 = ah_2$. So, f is injective

Let $bh \in bH$. Then $f(ah) = bh$. So, f is surjective.

So, f is bijective. So, aH and bH have the same cardinality

Note: For a finite group G, aH and bH have the same number of elements.
So, in a finite group G, $o(H) = o(aH) = o(bH)$ as $H = eH$ is also a left coset of H. (e is the identity element in G)

Theorem 4.8 Let H be a subgroup of a group G. Then the cardinality of the set of all left cosets of H in G and the set of all right cosets of H in G are same.

Proof: Let $\mathcal{L} = \{aH : a \in G\}$ be the set of all left cosets of H in G. and $\mathcal{R} = \{Ha : a \in G\}$ be the set of all right cosets of H in G.

Define $f : \mathcal{L} \to \mathcal{R}$ by $f(aH) = Ha^{-1}$, for $aH \in \mathcal{L}$

We first show that f is well defined. Let $aH = bH$. Then by Theorem 4.4, $a^{-1}b \in H$. This implies $(a^{-1}b)^{-1} \in H$ or $b^{-1}a \in H$ or $b^{-1}(a^{-1})^{-1} \in H$. This implies $Ha^{-1} = Hb^{-1}$ (by the corresponding theorem of right cosets, that $Ha = Hb$ if and only if $ba^{-1} \in H$). Thus $f(aH) = f(bH)$. So f is well defined.

Now, let $f(aH) = f(bH) \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow b^{-1}(a^{-1})^{-1} \in H$

$\Rightarrow b^{-1}a \in H \Rightarrow bH = aH$ or $aH = bH$ by Theorem 4.4.

Hence, f is injective. Since, for $Ha \in \mathcal{R}$,

$Ha = H(a^{-1})^{-1}$, so, $f(a^{-1}H) = H(a^{-1})^{-1} = Ha$. So, f is surjective. So, f is a bijection. So, $\mathcal{L}$ and $\mathcal{R}$ have the same cardinality.

Definition: Let H be a subgroup of a group G. Then the number of distinct left (or right) cosets, denoted by $[G:H]$, is called the index of H in G.

By Theorem 4.4, the number of left cosets and the number of right cosets of a subgroup H of a group G are the same. So, $[G:H]$ is well defined.

If G is finite, then of course $[G:H]$ is finite. The following example is one, where G is infinite and $[G:H]$ is finite.

Example: Let n be a fixed positive integer. Consider the cyclic subgroup $(n\mathbb{Z}, +)$ of $(\mathbb{Z}, +)$. Let $k + n\mathbb{Z}$ be a left coset of $n\mathbb{Z}$ in $\mathbb{Z}$. By the division algorithm, $\exists$ integers q and r such that $k = qn + r$, $0 \le r < n$. Then $k - r = qn \in n\mathbb{Z}$ and so, $k + n\mathbb{Z} = r + n\mathbb{Z}$ by Theorem 4.4. Suppose $i + n\mathbb{Z} = j + n\mathbb{Z}$, where $0 \le i, j \le n$. Then $i - j \in n\mathbb{Z}$ by Theorem 4.4. This implies that n divides $i - j$ and so we must have $i - j = 0$ or, $i = j$ since $0 \le i, j < n$. Thus, the distinct left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are $0 + n\mathbb{Z}$, $1 + n\mathbb{Z}$, $\ldots$, $n-1 + n\mathbb{Z}$.

Theorem 4.9 (Lagrange's Theorem) Let H be a subgroup of a finite group G. Then the order of H divides the order of G. In particular, $o(G) = [G : H] \cdot o(H)$

Proof: Since G is a finite group, the number of left cosets of H in G is finite. Let $\{a_1H, a_2H, \ldots, a_rH\}$ be the set of all distinct left cosets of H in G. Then by Theorem 4.6 and remark 2 of Theorem 4.6,

$$G = \bigcup_{i=1}^{r} a_iH \quad \text{and} \quad a_iH \cap a_jH = \phi \quad \text{for all } i \ne j,\ 1 \le i, j \le r$$

Hence $[G : H] = r$ and

$$\begin{aligned} o(G) &= o(H) + o(a_1H) + \ldots + o(a_rH) \\ &= r \cdot o(H) \quad \text{as } o(H) = o(a_iH) \text{ for all } i,\ 1 \le i \le r \\ &= [G : H] \cdot o(H). \end{aligned}$$

So, the order of H divides the order of G.

Corollary 4.9.1 Let G be a group of finite order n. Then the order of any element a of G divides n and $a^n = e$, e the identity element in G.

Proof: Let $a \in G$ and $o(a) = k$. Let $H = \langle a \rangle$. Then by Theorem 3.3 $o(H) = o(a) = k$. Hence by Theorem 4.9, k divides n. Thus $\exists\ q \in \mathbb{Z}$ such that $n = kq$. Hence $a^n = a^{kq} = (a^k)^q = e^q = e$

Corollary 4.9.2 Let G be a group of prime order. Then G is cyclic.

Proof: Since $o(G) \geq 2$, $\exists\ a \in G$ such that $a \neq e$, e is the identity element in G. Let $H = \langle a \rangle$ Then $H \neq \{e\}$ and $o(H)$ divides $o(G)$. But $o(G)$ is prime and so, $o(H) = o(G)$, so, $G = H$. So, G is cyclic.

Theorem 4.10 (Fermat's little theorem). Let p be a prime integer and a be an integer such that p does not divide a.

Then p divides $a^{p-1} - 1$, i.e.,

$$a^{p-1} \equiv 1 \pmod{p}$$

[Note: Let $U_n = \{\bar{a} : \mathbb{Z}_n \setminus \{\bar{0}\} : \gcd(a, n) = 1\}$ If '$\cdot$' denotes binary operation multiplication modulo n defined by

$$\bar{a} \cdot \bar{b} = \overline{ab} \text{ if } ab \leq n$$
$$= \overline{ab - n} \text{ if } ab > n$$

Then $(U_n, \cdot)$ forms a group, $\bar{1}$ is the identity element]

Proof: Let $U_p = \mathbb{Z}_p \setminus \{\bar{0}\}$. Then U_p is a group with respect to multiplication modulo p and $o(U_p) = p - 1$. Let a be an integer such that p does not divide a. Then $\bar{a}$ is a non-zero element of $\mathbb{Z}_p$ and so $\bar{a} \in U_p$. Thus, by Corollary 4.9.1 $\bar{a}^{p-1} = \bar{1}$ or $\overline{a^{p-1}} = \bar{1}$. Hence

$$a^{p-1} \equiv 1 \pmod{p}.$$

Worked out Exercises: 1. Let G be a noncyclic group of order p^2, p a prime integer. Show that the order of each nonidentity element is p

Proof: Let $a \in G$ and $a \neq e$, e is the identity element in G. Now $o(a)$ divides $o(G) = p^2$. Hence, $o(a) = 1, p$ or p^2. Since $a \neq e$, $o(a) \neq 1$. If $o(a) = p^2$, then G contains an element a such that $o(a) = o(G)$ and this implies that

G is cyclic, which contradicts the fact that G is non-cyclic.

So, $o(a) = p$.

2. Let $G = \{a, b, c, d\}$ be a group. Compute the following composition table for this group:

	a	b	c	d
a				
b				
c			b	
d		b		

Solution: From the table, $c^2 = b$, and $db = b$. Now $db = b$ implies that $d = e$, the identity element of G. Since $c^2 = b \neq d$, $o(c) \neq 2$. Hence $o(c) = 4$. Thus, G is a cyclic group generated by c. So, $G = \{e, c, c^2, c^3\}$. Since $d = e$ and $c^2 = b$, it follows that $c^3 = a$.

Hence, the composition table is

	a	b	c	d
a	b	c	d	a
b	c	d	a	b
c	d	a	b	c
d	a	b	c	d

3. Let G be a group such that $o(G) > 1$. Prove that G has only the trivial subgroups if and only $o(G)$ is prime

[A subgroup H of a group G is trivial if $H = \{e\}$ or $H = G$, e is the identity element of G]

Proof: Let $o(G) = p$, p a prime. Let H be a subgroup of G. Then $o(H)$ divides $o(G)$. This implies that $o(H) = 1$ or p. Thus, $H = \{e\}$ or $H = G$.

Conversely, suppose that G has only the trivial subgroups. Let $a \in G$ be such that $a \neq e$. Now $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a cyclic subgroup of G. and $\langle a \rangle \neq \{e\}$. So $G = \langle a \rangle$. If G is infinite, then $a^r = a^s$ for all $r, s \in \mathbb{Z}$, $r \neq s$. Hence, $\{a^{2n} : n \in \mathbb{Z}\}$ is a non-trivial subgroup of G, which is a contradiction. Thus, G is a finite cyclic group of order, say, $m > 1$.

Suppose m is not prime. Then $m = rs$ for some $r, s \in \mathbb{Z}$, $1 < r, s < m$. Since r divides $o(G)$ and G is cyclic, G has a cyclic subgroup H of order r. This contradicts the assumption that G has only the trivial subgroups. Hence $o(G)$ is prime.