Proof. If we look back in Chapter 1, we see that to prove Lemma 2.4.3 we must verify the following three conditions: For all $a, b, c \in G$,

1. $a \equiv a \bmod H$.
2. $a \equiv b \bmod H$ implies $b \equiv a \bmod H$.
3. $a \equiv b \bmod H$, $b \equiv c \bmod H$ implies $a \equiv c \bmod H$.

Let's go through each of these in turn.

1. To show that $a \equiv a \bmod H$ we must prove, using the very definition of congruence mod H, that $aa^{-1} \in H$. Since H is a subgroup of G, $e \in H$, and since $aa^{-1} = e$, $aa^{-1} \in H$, which is what we were required to demonstrate.

2. Suppose that $a \equiv b \bmod H$, that is, suppose $ab^{-1} \in H$; we want to get from this $b \equiv a \bmod H$, or, equivalently, $ba^{-1} \in H$. Since $ab^{-1} \in H$, which is a subgroup of G, $(ab^{-1})^{-1} \in H$; but, by Lemma 2.3.1, $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$, and so $ba^{-1} \in H$ and $b \equiv a \bmod H$.

3. Finally we require that $a \equiv b \bmod H$ and $b \equiv c \bmod H$ forces $a \equiv c \bmod H$. The first congruence translates into $ab^{-1} \in H$, the second into $bc^{-1} \in H$; using that H is a subgroup of G, $(ab^{-1})(bc^{-1}) \in H$. However, $ac^{-1} = aec^{-1} = a(b^{-1}b)c^{-1} = (ab^{-1})(bc^{-1})$; hence $ac^{-1} \in H$, from which it follows that $a \equiv c \bmod H$.

This establishes that congruence mod H is a bona fide equivalence relation as defined in Chapter 1, and all results about equivalence relations have become available to us to be used in examining this particular relation.

A word about the notation we used. If G were the group of integers under addition, and $H = H_n$ were the subgroup consisting of all multiples of n, then in G, the relation $a \equiv b \bmod H$, that is, $ab^{-1} \in H$, under the additive notation, reads "$a - b$ is a multiple of n." This is the usual number theoretic congruence mod n. In other words, the relation we defined using an arbitrary group and subgroup is the natural generalization of a familiar relation in a familiar group.

DEFINITION If H is a subgroup of G, $a \in G$, then $Ha = \{ha \mid h \in H\}$. Ha is called a *right coset* of H in G.

LEMMA 2.4.4 *For all* $a \in G$,

$$Ha = \{x \in G \mid a \equiv x \bmod H\}.$$

Proof. Let $[a] = \{x \in G \mid a \equiv x \bmod H\}$. We first show that $Ha \subset [a]$. For, if $h \in H$, then $a(ha)^{-1} = a(a^{-1}h^{-1}) = h^{-1} \in H$ since H is a subgroup of G. By the definition of congruence mod H this implies that $ha \in [a]$ for every $h \in H$, and so $Ha \subset [a]$.

Suppose, now, that $x \in [a]$. Thus $ax^{-1} \in H$, so $(ax^{-1})^{-1} = xa^{-1}$ is also in H. That is, $xa^{-1} = h$ for some $h \in H$. Multiplying both sides by a from the right we come up with $x = ha$, and so $x \in Ha$. Thus $[a] \subset Ha$. Having proved the two inclusions $[a] \subset Ha$ and $Ha \subset [a]$, we can conclude that $[a] = Ha$, which is the assertion of the lemma.

In the terminology of Chapter 1, $[a]$, and thus Ha, is the equivalence class of a in G. By Theorem 1.1.1 these equivalence classes yield a decomposition of G into disjoint subsets. *Thus any two right cosets of H in G either are identical or have no element in common.*

We now claim that between any two right cosets Ha and Hb of H in G there exists a one-to-one correspondence, namely, with any element $ha \in Ha$, where $h \in H$, associate the element $hb \in Hb$. Clearly this mapping is onto Hb. We aver that it is a one-to-one correspondence, for if $h_1b = h_2b$, with $h_1, h_2 \in H$, then by the cancellation law in G, $h_1 = h_2$ and so $h_1a = h_2a$. This proves

LEMMA 2.4.5 *There is a one-to-one correspondence between any two right cosets of H in G.*

Lemma 2.4.5 is of most interest when H is a finite group, for then it merely states that any two right cosets of H have the same number of elements. How many elements does a right coset of H have? Well, note that $H = He$ is itself a right coset of H, so any right coset of H in G has $o(H)$ elements. Suppose now that G is a finite group, and let k be the number of distinct right cosets of H in G. By Lemmas 2.4.4 and 2.4.5 any two distinct right cosets of H in G have no element in common, and each has $o(H)$ elements. Since any $a \in G$ is in the unique right coset Ha, the right cosets fill out G. Thus if k represents the number of distinct right cosets of H in G we must have that $ko(H) = o(G)$. We have proved the famous theorem due to Lagrange, namely,

THEOREM 2.4.1 *If G is a finite group and H is a subgroup of G, then $o(H)$ is a divisor of $o(G)$.*

DEFINITION If H is a subgroup of G, the *index of H in G* is the number of distinct right cosets of H in G.

We shall denote it by $i_G(H)$. In case G is a finite group, $i_G(H) = o(G)/o(H)$, as became clear in the proof of Lagrange's theorem. It is quite possible for an infinite group G to have a subgroup $H \neq G$ which is of finite index in G.

It might be difficult, at this point, for the student to see the extreme importance of this result. As the subject is penetrated more deeply one will become more and more aware of its basic character. Because the theorem is of such stature it merits a little closer scrutiny, a little more analysis, and so we give, below, a slightly different way of looking at its proof. In truth, the procedure outlined below is no different from the one already given. The introduction of the congruence mod H smooths out the listing of elements used below, and obviates the need for checking that the new elements introduced at each stage did not appear before.

So suppose again that G is a finite group and that H is a subgroup of G. Let $h_1, h_2, \ldots, h_r$ be a complete list of the elements of H, $r = o(H)$. If $H = G$, there is nothing to prove. Suppose, then, that $H \neq G$; thus there is an $a \in G$, $a \notin H$. List all the elements so far in two rows as

$$\begin{gathered} h_1, h_2, \ldots, h_r, \\ h_1a, h_2a, \ldots, h_ra. \end{gathered}$$

We claim that all the entries in the second line are different from each other and are different from the entries in the first line. If any two in the second line were equal, then $h_ia = h_ja$ with $i \neq j$, but by the cancellation law this would lead to $h_i = h_j$, a contradiction. If an entry in the second line were equal to one in the first line, then $h_ia = h_j$, resulting in $a = h_i^{-1}h_j \in H$ since H is a subgroup of G; this violates $a \notin H$.

Thus we have, so far, listed $2o(H)$ elements; if these elements account for all the elements of G, we are done. If not, there is a $b \in G$ which did not occur in these two lines. Consider the new list

$$\begin{gathered} h_1, h_2, \ldots, h_r, \\ h_1a, h_2a, \ldots, h_ra, \\ h_1b, h_2b, \ldots, h_rb. \end{gathered}$$

As before (we are now waving our hands) we could show that no two entries in the third line are equal to each other, and that no entry in the third line occurs in the first or second line. Thus we have listed $3o(H)$ elements. Continuing in this way, every new element introduced, in fact, produces $o(H)$ new elements. Since G is a finite group, we must eventually exhaust all the elements of G. But if we ended up using k lines to list all the elements of the group, we would have written down $ko(H)$ distinct elements, and so $ko(H) = o(G)$.

It is essential to point out that the converse to Lagrange's theorem is false—a group G need not have a subgroup of order m if m is a divisor of $o(G)$. For instance, a group of order 12 exists which has no subgroup of order 6. The reader might try to find an example of this phenomenon; the place to look is in S_4, the symmetric group of degree 4 which has a subgroup of order 12, which will fulfill our requirement.

Lagrange's theorem has some very important corollaries. Before we present these we make one definition.

DEFINITION If G is a group and $a \in G$, the *order* (or *period*) of a is the least positive integer m such that $a^m = e$.

If no such integer exists we say that a is of infinite order. We use the notation $o(a)$ for the order of a. Recall our other notation: for two integers u, v, $u \mid v$ reads "u is a divisor of v."

COROLLARY 1 *If G is a finite group and $a \in G$, then $o(a) \mid o(G)$.*

Proof. With Lagrange's theorem already in hand, it seems most natural to prove the corollary by exhibiting a subgroup of G whose order is $o(a)$. The element a itself furnishes us with this subgroup by considering the cyclic subgroup, (a), of G generated by a; (a) consists of $e, a, a^2, \ldots$. How many elements are there in (a)? We assert that this number is the order of a. Clearly, since $a^{o(a)} = e$, this subgroup has at most $o(a)$ elements. If it should actually have fewer than this number of elements, then $a^i = a^j$ for some integers $0 \leq i < j < o(a)$. Then $a^{j-i} = e$, yet $0 < j - i < o(a)$ which would contradict the very meaning of $o(a)$. Thus the cyclic subgroup generated by a has $o(a)$ elements, whence, by Lagrange's theorem, $o(a) \mid o(G)$.

COROLLARY 2 *If G is a finite group and $a \in G$, then $a^{o(G)} = e$.*

Proof. By Corollary 1, $o(a) \mid o(G)$; thus $o(G) = mo(a)$. Therefore, $a^{o(G)} = a^{mo(a)} = (a^{o(a)})^m = e^m = e$.

A particular case of Corollary 2 is of great interest in number theory. The Euler ϕ-function, $\phi(n)$, is defined for all integers n by the following: $\phi(1) = 1$; for $n > 1$, $\phi(n) =$ number of positive integers less than n and relatively prime to n. Thus, for instance, $\phi(8) = 4$ since only 1, 3, 5, 7 are the numbers less than 8 which are relatively prime to 8. In Problem 15(b) at the end of Section 2.3 the reader was asked to prove that the numbers less than n and relatively prime to n formed a group under multiplication mod n. This group has order $\phi(n)$. If we apply Corollary 2 to this group we obtain

COROLLARY 3 (EULER) *If n is a positive integer and a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \bmod n$.*

In order to apply Corollary 2 one should replace a by its remainder on division by n. If n should be a prime number p, then $\phi(p) = p - 1$. If a is an integer relatively prime to p, then by Corollary 3, $a^{p-1} \equiv 1 \bmod p$, whence $a^p \equiv a \bmod p$. If, on the other hand, a is not relatively prime to p, since p is a prime number, we must have that $p \mid a$, so that $a \equiv 0 \bmod p$; hence $0 \equiv a^p \equiv a \bmod p$ here also. Thus

COROLLARY 4 (FERMAT) *If p is a prime number and a is any integer, then $a^p \equiv a \bmod p$.*

COROLLARY 5 *If G is a finite group whose order is a prime number p, then G is a cyclic group.*

Proof. First we claim that G has no nontrivial subgroups H; for $o(H)$ must divide $o(G) = p$ leaving only two possibilities, namely, $o(H) = 1$ or $o(H) = p$. The first of these implies $H = (e)$, whereas the second implies that $H = G$. Suppose now that $a \neq e \in G$, and let $H = (a)$. H is a subgroup of G, $H \neq (e)$ since $a \neq e \in H$. Thus $H = G$. This says that G is cyclic and that every element in G is a power of a.

This section is of great importance in all that comes later, not only for its results but also because the spirit of the proofs occurring here are genuinely group-theoretic. The student can expect to encounter other arguments having a similar flavor. It would be wise to assimilate the material and approach thoroughly, now, rather than a few theorems later when it will be too late.

2.5 A Counting Principle

As we have defined earlier, if H is a subgroup of G and $a \in G$, then Ha consists of all elements in G of the form ha where $h \in H$. Let us generalize this notion. If H, K are two subgroups of G, let

$$HK = \{x \in G \mid x = hk, h \in H, k \in K\}.$$

Let's pause and look at an example; in S_3 let $H = \{e, \phi\}$, $K = \{e, \phi\psi\}$. Since $\phi^2 = (\phi\psi)^2 = e$, both H and K are subgroups. What can we say about HK? Just using the definition of HK we can see that HK consists of the elements $e, \phi, \phi\psi, \phi^2\psi = \psi$. Since HK consists of four elements and 4 is not a divisor of 6, the order of S_3 by Lagrange's theorem HK could not be a subgroup of S_3. (Of course, we could verify this directly but it does not hurt to keep recalling Lagrange's theorem.) We might try to find out why HK is not a subgroup. Note that $KH = \{e, \phi, \phi\psi, \phi\psi\phi = \psi^{-1}\} \neq HK$. This is precisely why HK fails to be a subgroup, as we see in the next lemma.

LEMMA 2.5.1 *HK is a subgroup of G if and only if $HK = KH$.*

Proof. Suppose, first, that $HK = KH$; that is, if $h \in H$ and $k \in K$, then $hk = k_1h_1$ for some $k_1 \in K$, $h_1 \in H$ (it need not be that $k_1 = k$ or

$h_1 = h$!). To prove that HK is a subgroup we must verify that it is closed and every element in HK has its inverse in HK. Let's show the closure first; so suppose $x = hk \in HK$ and $y = h'k' \in HK$. Then $xy = hkh'k'$, but since $kh' \in KH = HK$, $kh' = h_2k_2$ with $h_2 \in H$, $k_2 \in K$. Hence $xy = h(h_2k_2)k' = (hh_2)(k_2k') \in HK$, and HK is closed. Also $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK$, so $x^{-1} \in HK$. Thus HK is a subgroup of G.

On the other hand, if HK is a subgroup of G, then for any $h \in H$, $k \in K$, $h^{-1}k^{-1} \in HK$ and so $kh = (h^{-1}k^{-1})^{-1} \in HK$. Thus $KH \subset HK$. Now if x is any element of HK, $x^{-1} = hk \in HK$ and so $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$, so $HK \subset KH$. Thus $HK = KH$.

An interesting special case is the situation when G is an abelian group for in that case trivially $HK = KH$. Thus as a consequence we have the

COROLLARY *If H, K are subgroups of the abelian group G, then HK is a subgroup of G.*

If H, K are subgroups of a group G, we have seen that the subset HK need not be a subgroup of G. Yet it is a perfect meaningful question to ask: How many distinct elements are there in the subset HK? If we denote this number by $o(HK)$, we prove

THEOREM 2.5.1 *If H and K are finite subgroups of G of orders $o(H)$ and $o(K)$, respectively, then*

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)}.$$

Proof. Although there is no need to pay special attention to the particular case in which $H \cap K = (e)$, looking at this case, which is devoid of some of the complexity of the general situation, is quite revealing. Here we should seek to show that $o(HK) = o(H)o(K)$. One should ask oneself: How could this fail to happen? The answer clearly must be that if we list all the elements hk, $h \in H$, $k \in K$ there should be some collapsing; that is, some element in the list must appear at least twice. Equivalently, for some $h \neq h_1 \in H$, $hk = h_1k_1$. But then $h_1^{-1}h = k_1k^{-1}$; now since $h_1 \in H$, h_1^{-1} must also be in H, thus $h_1^{-1}h \in H$. Similarly, $k_1k^{-1} \in K$. Since $h_1^{-1}h = k_1k^{-1}$, $h_1^{-1}h \in H \cap K = (e)$, so $h_1^{-1}h = e$, whence $h = h_1$, a contradiction. We have proved that no collapsing can occur, and so, here, $o(HK)$ is indeed $o(H)o(K)$.

With this experience behind us we are ready to attack the general case. As above we must ask: How often does a given element hk appear as a product in the list of HK? We assert it must appear $o(H \cap K)$ times! To see this we first remark that if $h_1 \in H \cap K$, then

$$hk = (hh_1)(h_1^{-1}k), \tag{1}$$

where $hh_1 \in H$, since $h \in H$, $h_1 \in H \cap K \subset H$ and $h_1^{-1}k \in K$ since $h_1^{-1} \in H \cap K \subset K$ and $k \in K$. Thus hk is duplicated in the product at least $o(H \cap K)$ times. However, if $hk = h'k'$, then $h^{-1}h' = k(k')^{-1} = u$, and $u \in H \cap K$, and so $h' = hu$, $k' = u^{-1}k$; thus all duplications were accounted for in (1). Consequently hk appears in the list of HK exactly $o(H \cap K)$ times. Thus the number of distinct elements in HK is the total number in the listing of HK, that is, $o(H)o(K)$ divided by the number of times a given element appears, namely, $o(H \cap K)$. This proves the theorem.

Suppose H, K are subgroups of the finite group G and $o(H) > \sqrt{o(G)}$, $o(K) > \sqrt{o(G)}$. Since $HK \subset G$, $o(HK) \leq o(G)$. However,

$$o(G) \geq o(HK) = \frac{o(H)o(K)}{o(H \cap K)} > \frac{\sqrt{o(G)}\sqrt{o(G)}}{o(H \cap K)} = \frac{o(G)}{o(H \cap K)},$$

thus $o(H \cap K) > 1$. Therefore, $H \cap K \neq (e)$. We have proved the

COROLLARY *If H and K are subgroups of G and $o(H) > \sqrt{o(G)}$, $o(K) > \sqrt{o(G)}$, then $H \cap K \neq (e)$.*

We apply this corollary to a very special group. Suppose G is a finite group of order pq where p and q are prime numbers with $p > q$. We claim that G can have at most one subgroup of order p. For suppose H, K are subgroups of order p. By the corollary, $H \cap K \neq (e)$, and being a subgroup of H, which having prime order has no nontrivial subgroups, we must conclude that $H \cap K = H$, and so $H \subset H \cap K \subset K$. Similarly $K \subset H$, whence $H = K$, proving that there is at most one subgroup of order p. Later on we shall see that there is at least one subgroup of order p, which, combined with the above, will tell us there is exactly one subgroup of order p in G. From this we shall be able to determine completely the structure of G.

Problems

1. If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?)
2. Let G be a group such that the intersection of all its subgroups which are different from (e) is a subgroup different from (e). Prove that every element in G has finite order.
3. If G has no nontrivial subgroups, show that G must be finite of prime order.

4. (a) If H is a subgroup of G, and $a \in G$ let $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. Show that aHa^{-1} is a subgroup of G.
   (b) If H is finite, what is $o(aHa^{-1})$?

5. For a subgroup H of G define the left coset aH of H in G as the set of all elements of the form ah, $h \in H$. Show that there is a one-to-one correspondence between the set of left cosets of H in G and the set of right cosets of H in G.

6. Write out all the right cosets of H in G where
   (a) $G = (a)$ is a cyclic group of order 10 and $H = (a^2)$ is the subgroup of G generated by a^2.
   (b) G as in part (a), $H = (a^5)$ is the subgroup of G generated by a^5.
   (c) $G = A(S)$, $S = \{x_1, x_2, x_3\}$, and $H = \{\sigma \in G \mid x_1\sigma = x_1\}$.

7. Write out all the left cosets of H in G for H and G as in parts (a), (b), (c) of Problem 6.

8. Is every right coset of H in G a left coset of H in G in the groups of Problem 6?

9. Suppose that H is a subgroup of G such that whenever $Ha \neq Hb$ then $aH \neq bH$. Prove that $gHg^{-1} \subset H$ for all $g \in G$.

10. Let G be the group of integers under addition, H_n the subgroup consisting of all multiples of a fixed integer n in G. Determine the index of H_n in G and write out all the right cosets of H_n in G.

11. In Problem 10, what is $H_n \cap H_m$?

12. If G is a group and H, K are two subgroups of finite index in G, prove that $H \cap K$ is of finite index in G. Can you find an upper bound for the index of $H \cap K$ in G?

13. If $a \in G$, define $N(a) = \{x \in G \mid xa = ax\}$. Show that $N(a)$ is a subgroup of G. $N(a)$ is usually called the *normalizer* or *centralizer* of a in G.

14. If H is a subgroup of G, then by the centralizer $C(H)$ of H we mean the set $\{x \in G \mid xh = hx \text{ all } h \in H\}$. Prove that $C(H)$ is a subgroup of G.

15. The *center* Z of a group G is defined by $Z = \{z \in G \mid zx = xz \text{ all } x \in G\}$. Prove that Z is a subgroup of G. Can you recognize Z as $C(T)$ for some subgroup T of G?

16. If H is a subgroup of G, let $N(H) = \{a \in G \mid aHa^{-1} = H\}$ [see Problem 4(a)]. Prove that
   (a) $N(H)$ is a subgroup of G. (b) $N(H) \supset H$.

17. Give an example of a group G and a subgroup H such that $N(H) \neq C(H)$. Is there any containing relation between $N(H)$ and $C(H)$?

18. If H is a subgroup of G let
$$N = \bigcap_{x \in G} xHx^{-1}.$$
Prove that N is a subgroup of G such that $aNa^{-1} = N$ for all $a \in G$.

*19. If H is a subgroup of finite index in G, prove that there is only a finite number of distinct subgroups in G of the form aHa^{-1}.

*20. If H is of finite index in G prove that there is a subgroup N of G, contained in H, and of finite index in G such that $aNa^{-1} = N$ for all $a \in G$. Can you give an upper bound for the index of this N in G?

21. Let the mapping τ_{ab} for a, b real numbers, map the reals into the reals by the rule $\tau_{ab}:x \to ax + b$. Let $G = \{\tau_{ab} \mid a \neq 0\}$. Prove that G is a group under the composition of mappings. Find the formula for $\tau_{ab}\tau_{cd}$.

22. In Problem 21, let $H = \{\tau_{ab} \in G \mid a \text{ is rational}\}$. Show that H is a subgroup of G. List all the right cosets of H in G, and all the left cosets of H in G. From this show that every left coset of H in G is a right coset of H in G.

23. In the group G of Problem 21, let $N = \{\tau_{1b} \in G\}$. Prove
(a) N is a subgroup of G.
(b) If $a \in G$, $n \in N$, then $ana^{-1} \in N$.

*24. Let G be a finite group whose order is *not* divisible by 3. Suppose that $(ab)^3 = a^3b^3$ for all $a, b \in G$. Prove that G must be abelian.

*25. Let G be an abelian group and suppose that G has elements of orders m and n, respectively. Prove that G has an element whose order is the least common multiple of m and n.

**26. If an abelian group has subgroups of orders m and n, respectively, then show it has a subgroup whose order is the least common multiple of m and n. (Don't be discouraged if you don't get this problem with what you know about group theory up to this stage. I don't know anybody, including myself, who has done it subject to the restriction of using material developed so far in the text. But it is fun to try. I've had more correspondence about this problem than about any other point in the whole book.)

27. Prove that any subgroup of a cyclic group is itself a cyclic group.

28. How many generators does a cyclic group of order n have? ($b \in G$ is a generator if $(b) = G$.)

Let U_n denote the integers relatively prime to n under multiplication mod n. In Problem 15(b), Section 2.3, it is indicated that U_n is a group.

In the next few problems we look at the nature of U_n as a group for some specific values of n.

29. Show that U_8 is not a cyclic group.
30. Show that U_9 is a cyclic group. What are all its generators?
31. Show that U_{17} is a cyclic group. What are all its generators?
32. Show that U_{18} is a cyclic group.
33. Show that U_{20} is not a cyclic group.
34. Show that both U_{25} and U_{27} are cyclic groups.
35. Hazard a guess at what all the n such that U_n is cyclic are. (You can verify your guess by looking in any reasonable book on number theory.)
36. If $a \in G$ and $a^m = e$, prove that $o(a) \mid m$.
37. If in the group G, $a^5 = e$, $aba^{-1} = b^2$ for some $a, b \in G$, find $o(b)$.

*38. Let G be a finite abelian group in which the number of solutions in G of the equation $x^n = e$ is at most n for every positive integer n. Prove that G must be a cyclic group.

39. Let G be a group and A, B subgroups of G. If $x, y \in G$ define $x \sim y$ if $y = axb$ for some $a \in A$, $b \in B$. Prove
    (a) The relation so defined is an equivalence relation.
    (b) The equivalence class of x is $AxB = \{axb \mid a \in A,\ b \in B\}$. ($AxB$ is called a *double coset* of A and B in G.)
40. If G is a finite group, show that the number of elements in the double coset AxB is
$$\frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$
41. If G is a finite group and A is a subgroup of G such that all double cosets AxA have the same number of elements, show that $gAg^{-1} = A$ for all $g \in G$.

2.6 Normal Subgroups and Quotient Groups

Let G be the group S_3 and let H be the subgroup $\{e, \phi\}$. Since the index of H in G is 3, there are three right cosets of H in G and three left cosets of H in G. We list them:

Right Cosets	Left Cosets
$H = \{e, \phi\}$	$H = \{e, \phi\}$
$H\psi = \{\psi, \phi\psi\}$	$\psi H = \{\psi, \psi\phi = \phi\psi^2\}$
$H\psi^2 = \{\psi^2, \phi\psi^2\}$	$\psi^2 H = \{\psi^2, \psi^2\phi = \phi\psi\}$