Chapter 9
Normal Subgroups and Factor Groups

The set of cosets of a subgroup H has no group structure. We are now interested in a criterion on H to give the set of its cosets a group structure. In this chapter, we introduce the concept of normal subgroups and we form a group of cosets, say factor group. A factor group is a way of creating a group from another group. This new group often retains some of the properties of the original group.

9.1 Normal Subgroups

There is one kind of subgroup that is especially interesting. If G is a group and H is a subgroup of G, it is not always true that $aH = Ha$ for all $a \in G$. There are certain situations where this does hold, however, and these cases turn out to be of critical importance in the theory of groups. It was Galois, who first recognized that such subgroups were worthy of special attention.

Definition 9.1 Let G be a group and N be a subgroup of G. We say that N is a *normal subgroup* of G, or that N is *normal* in G, if we have $aNa^{-1} \subseteq N$, for all $a \in G$.

Equivalently, a subgroup N of G is normal if $axa^{-1} \in N$, for all $a \in G$ and $x \in N$. Note that, also, we can say $a^{-1}xa^{-1} \in N$, for all $a \in G$ and $x \in N$.

Example 9.2 Clearly, the trivial subgroups G and $\{e\}$ of a group G are normal subgroups.

Example 9.3 If G is an abelian group, then all its subgroups are normal.

Example 9.4 The center of a group G forms a normal subgroup of G.

B. Davvaz, *A First Course in Group Theory*,
https://doi.org/10.1007/978-981-16-6365-9_9

Example 9.5 Consider the dihedral group D_n generated by R and S with $R^n = Id$, $S^2 = Id$, and $SRS = R^{-1}$. If N is the subgroup of rotational symmetries, then N is normal in D_n.

We denote it $N \trianglelefteq G$, or $N \triangleleft G$ when we want to emphasize that N is a proper subgroup of G. The condition for a subgroup to be normal can be stated in many slightly different ways.

Definition 9.6 Let G be a group and X be a non-empty subset of G. The set

$$N_G(X) = \{a \in G \mid aXa^{-1} = X\}$$

is called the *normalizer* of X in G.

Theorem 9.7 *If G is a group and X is a non-empty subset of G, then $N_G(X)$ is a subgroup of G. In particular, if H is a subgroup of G, then $H \trianglelefteq N_G(H)$.*

Proof It is straightforward. ■

Theorem 9.8 *Let N be a subgroup of a group G. The following conditions are equivalent:*

(1) N is a normal subgroup of G;
(2) $aNa^{-1} = N$, for all $a \in G$;
(3) $aN = Na$, for all $a \in G$;
(4) Every left coset of N in G is also a right coset of N in G.

Proof $(1 \Rightarrow 2)$: Let N be a normal subgroup of G. Then, for each $a \in G$, we have $aNa^{-1} \subseteq N$. If $a \in G$, then $a^{-1} \in G$, and so $a^{-1}N(a^{-1})^{-1} = a^{-1}Na \subseteq N$. This yields that $N \subseteq aNa^{-1}$. Thus, we conclude that $aNa^{-1} = N$.

$(2 \Rightarrow 3)$: Let $a \in G$ be arbitrary. Since $aNa^{-1} = N$, it follows that $aNa^{-1}a = Na$, or equivalently $aN = Na$.

$(3 \Rightarrow 4)$: It is straightforward.

$(4 \Rightarrow 1)$: Suppose that every left coset of N in G is a right coset of N in G. Thus, for $a \in G$, aN being a left coset, must be a right coset. Let $aN = Nb$, for some $b \in G$. Since $a \in aN$, it follows that $a \in Nb$. Hence, we get $Na \subseteq NNb \subseteq Nb$. This shows that $Na = Nb$, and so $aN = Na$. Consequently, $aNa^{-1} = N$, and this implies that N is a normal subgroup of G. ■

Theorem 9.9 *For each positive integer n, A_n is a normal subgroup of S_n.*

Proof Assume that $\alpha \in S_n$ is a product of k transpositions, say $\alpha = \tau_1 \dots \tau_k$. Then, we have $\alpha^{-1} = \tau_k^{-1} \dots \tau_1^{-1}$. Now, if $\sigma \in A_n$, then σ is even, say a product of $2m$ transpositions. Consequently, $\alpha\sigma\alpha^{-1}$ is a product of $k + 2m + k = 2(k + m)$ transpositions, and so $\alpha\sigma\alpha^{-1}$ is even. ■

Theorem 9.10 *$SL_n(\mathbb{F})$ is a normal subgroup of $GL_n(\mathbb{F})$.*

Proof For every $A \in GL_n(\mathbb{F})$ and $B \in SL_n(\mathbb{F})$, we have

$$\det(ABA^{-1}) = det(A)\det(B)\det(A^{-1}) = \det(B) = 1.$$

This shows that $ABA^{-1} \in SL_2(\mathbb{F})$, and so $SL_n(\mathbb{F}) \trianglelefteq GL_n(\mathbb{F})$. ■

Lemma 9.11 *Let G be a group and $N \trianglelefteq G$. If $N \leq H \leq G$, then $N \trianglelefteq H$.*

Proof It is clear. ■

Theorem 9.12 *Let H and N be subgroups of a group G. If $N \trianglelefteq G$, then $HN = NH \leq G$.*

Proof By Theorem 8.32, it is enough to show that $HN = NH$. Let $x \in HN$ be an arbitrary element. Then, there exist $h \in H$ and $n \in N$ such that $x = hn$. Since $N \trianglelefteq G$, it follows that $hnh^{-1} \in N$. Hence, we conclude that $hn \in Nh \subseteq NH$, or equivalently, $x \in NH$. This shows that $HN \subseteq NH$. Analogously, we observe that $NH \subseteq HN$. Therefore, we get $HN = NH$. ■

Theorem 9.13 *Let H and N be normal subgroups of a group G. Then,*

(1) $H \cap N$ is a normal subgroup of G;
(2) HN is a normal subgroup of G.

Proof (1) Let $a \in G$ and $x \in H \cap N$ be arbitrary. Since $H \trianglelefteq G$, it follows that $axa^{-1} \in H$. Since $N \trianglelefteq G$, it follows that $axa^{-1} \in N$. Consequently, we have $axa^{-1} \in H \cap N$.

(2) By Theorem 9.12, HN is a subgroup of G. Now, let $a \in G$ and $hn \in HN$ be arbitrary. Then, we get $ahna^{-1} = (aha^{-1})(ana^{-1}) \in HN$, using the normality of both H and N. ■

Theorem 9.14 *Let G be a group, not necessarily finite, and let N be a subgroup of G such that the index $[G : N] = 2$. Then, N is a normal subgroup of G.*

Proof Since $[G : N] = 2$, it follows that N has two left cosets and two right cosets. One of them is always N itself. Take $a \notin N$. Then, aN is the other left coset, Na is the other right coset, and $N \cup aN = N \cup Na = G$. But these are disjoint unions, so $aN = Na$, and therefore $aNa^{-1} = N$. This equation holds for any a in the coset aN. The equation clearly holds for any element of the coset N. Hence, the equation holds for all elements of G, and we conclude that N is normal. ■

In the following example, we present three groups K, H and G such that $K \trianglelefteq H$ and $H \trianglelefteq G$, but K is not normal in G.

Example 9.15 Let $D_4 = \langle R, S\rangle$ be the dihedral group of order 8. Since $[\langle R^2, S\rangle : \langle S\rangle] = 2$, it follows that $\langle S\rangle \trianglelefteq \langle R^2, S\rangle$. Since $[D_4 : \langle R^2, S\rangle] = 2$, it follows that $\langle R^2, S\rangle \trianglelefteq D_4$. But $\langle S\rangle$ is not a normal subgroup of D_4.

Theorem 9.16 *If p is the smallest prime number that divides the order of a finite group G, then every subgroup of G with the index p is a normal subgroup.*

Proof Let N be a subgroup of a finite group G of order n such that $[G : N] = p$. First we claim that if $a \notin N$, then $a^i \notin N$, for all $1 \leq i \leq p-1$. Indeed, if this statement is not true, then there is $1 < k \leq p-1$ such that $a^k \in N$. Suppose that j is the least positive integer such that $a^j \in N$, i.e., for $1 \leq t \leq j-1$, $a^t \notin N$. Let $o(a) = m$. Since $m|n$, $1 < j < p$ and p is the smallest prime factor of n, we conclude that $j \nmid m$. Hence, there exist integers q and r such that $m = qj + r$ and $0 < r < j$. Now, we can write

$$e = a^m = a^{qj+r} = \left(a^j\right)^q a^r.$$

This implies that $x^r = \left(a^j\right)^{-q}$. Since $a^j \in N$, it follows that $a^r \in N$, and it is a contradiction. Therefore, we proved that our claim holds.

In order to prove the theorem, assume that N is not a normal subgroup of G. So, there exist $a \in G$ and $x \in N$ such that $axa^{-1} \notin N$. Obviously, $a \notin N$, and so by the above discussion, we deduce that $a^i \notin N$, for every $1 \leq i \leq p-1$. On the other hand, if $a^i N = a^j N$, then there is $y \in N$ such that $a^i = a^j y$, or equivalently $a^{i-j} = y$, and it is a contradiction. Consequently, $N, aN, \ldots, a^{p-1}N$ are disjoint left cosets of N in G. On the other hand, assume that $axa^{-1} = b$. Since $b \notin N$, in a similar way, it follows that $N, bN, \ldots, b^{p-1}N$ are disjoint left cosets of N in G, too. Thus, the following two families of left cosets

$$\{N,\ aN,\ \ldots,\ a^{p-1}N\} \text{ and } \{N,\ bN,\ \ldots,\ b^{p-1}N\}$$

are equal. So, $aN = b^r N$, for some $1 \leq r \leq p-1$. This means that $a = b^r z$, for some $z \in N$. Now, we obtain

$$a = b^r z = \left(axa^{-1}\right)^r z = ax^r a^{-1} z.$$

Hence, we have $e = x^r a^{-1} z$, or equivalently $a = zx^r$. Since x and z belong to N, it follows that $a \in N$, a contradiction. Therefore, we conclude that N is a normal subgroup of G. ■

Theorem 9.17 *Let G be a group and H and K be normal subgroups of G. If $|H \cap K| = 1$, then $hk = kh$, for all $h \in H$ and $k \in K$.*

Proof Suppose that $h \in H$ and $k \in K$ are arbitrary. We consider the element $hkh^{-1}k^{-1}$. On the one hand, since $H \trianglelefteq G$, it follows that $h(kh^{-1}k^{-1}) \in H$, and on the other hand, since $K \trianglelefteq G$, it follows that $(hkh^{-1})k^{-1}) \in K$. So, we obtain $hkh^{-1}k^{-1} \in H \cap K = \{e\}$. This implies that $hkh^{-1}k^{-1} = e$, or equivalently, $hk = kh$. ■

Exercises

1. Let G be a group in which, for some integer $n > 1$, $(ab)^n = a^n b^n$ for all $a, b \in G$. Show that the subset $H = \{x^{n-1} \mid x \in G\}$ is a normal subgroup of G.
2. Find all normal subgroups of S_3.
3. If N is a normal subgroup of G with $|N| = 2$, prove that $N \leq Z(G)$.
4. Let N be a normal subgroup of S_4.
   (a) If N contains a transposition, prove that $N = S_4$;
   (b) If N contains a cycle of length 3, prove that $N = A_4$;
   (c) If N contains a cycle of length 4, prove that $N = S_4$;
   (d) Find all the normal subgroups of S_4.
5. Show that if a finite group G has exactly one subgroup N of a given order, then N is a normal subgroup of G.
6. If G is a group and N is a normal subgroup of G, show that $C_G(H) \trianglelefteq G$.
7. Prove that if N is a normal subgroup of the group G, then $Z(N)$ is a normal subgroup of G. Show by an example that $Z(N)$ need not be contained in $Z(G)$.
8. Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$, then $H \leq Z(G)$.
9. If A is an abelian group with $A \trianglelefteq G$ and B is any subgroup of G, prove that $A \cap B \trianglelefteq AB$.
10. Show that if H and N are subgroups of a group G, and N is normal in G, then $H \cap N$ is normal in H. Show by an example that $H \cap N$ need not be normal in G.
11. Let N be a normal subgroup of a finite group G. If N is cyclic, prove every subgroup of N is also normal in G.
12. Let G be the set of all triples of the form $(a_1, a_2, 1)$ or $(a_1, a_2, -1)$, where a_1 and a_2 are integers. Define a binary operation on G by the rule

$$(a_1, a_2, 1)(b_1, b_2, c) = (a_1 + b_2, a_1 + b_2, c),$$
$$(a_1, a_2, -1)(b_1, b_2, c) = (a_1 + b_2, a_2 + b_1, -c),$$

   where $c = \pm 1$. Prove that
   (a) G is a group;
   (b) $H = \langle (1, 0, 1),\ (0, 1, 1) \rangle$ is a normal subgroup of G;
   (c) $K = \langle (1, 0, 1) \rangle$ is a normal subgroup of H;
   (d) Is K a normal subgroup of H?
13. If N is a normal subgroup such that $[G : N] = n$, show that $x^n \in N$, for all $x \in G$.
14. Let H be a proper subgroup of G such that for all $x, y \in G \setminus H$, $xy \in H$. Prove that H is a normal subgroup of G.

9.2 Factor Groups

A factor group is a way of creating a group from another group. This new group often retains some of the properties of the original group.

Theorem 9.18 *Let G be a group and N be a normal subgroup of G. The set $G/N = \{aN \mid a \in G\}$ is a group under the binary operation $(aN)(bN) = abN$, for all aN and bN in G/N.*

Proof Our first task is to show that the operation is well defined. In order to do this, suppose that $aN = cN$ and $bN = dN$, for some a, b, c and d in G. Then, we conclude $c \in aN$ and $d \in bN$. Hence, there exist $n_1, n_2 \in N$ such that $c = an_1$ and $d = bn_2$. Now, we have

$$(ab)^{-1}cd = b^{-1}a^{-1}cd = b^{-1}a^{-1}an_1bn_2 = b^{-1}n_1bn_2.$$

Since $N \trianglelefteq G$ it follows that $b^{-1}n_1b \in N$. Therefore, we deduce that $(ab)^{-1}cd \in N$. This forces that $abN = cdN$.

Computing $aN(bNcN) = aN(bc)N = a(bc)N$, and similarly, we have $(aNbN)cN = (ab)NcN = (ab)cN$. So, associativity in G/N follows from associativity in G. Since $aNeN = aeN = aN = eaN = eNaN$, it follows that $eN = N$ is the identity element in G/N. Finally, $a^{-1}NaN = (a^{-1}a)N = N = (aa^{-1})N = aNa^{-1}N$ shows that $a^{-1}N$ is the inverse of aN. This proves that G/N is a group. ■

The group G/N which was defined in Theorem 9.18 is called the *factor group* of G by N.

Theorem 9.19 *If G is a finite group and $N \trianglelefteq G$, then $|G/N| = |G|/|N|$.*

Proof The proof follows from Lagrange's Theorem. ■

A factor group is also called the *quotient group* of G by N. Further, if the binary operation in G is addition, then each coset of N in G is denoted by $a + N$ and the binary operation in G/N is also denoted additively, i.e., we write $(a + N) + (b + N) = (a + b) + N$.

Example 9.20 Let $G = \mathbb{Z}_{18}$ and $N = \langle 6 \rangle$. Then, $G/N = \{0 + N,\ 1 + N,\ 2 + N,\ 3 + N,\ 4 + N,\ 5 + N\}$.

Example 9.21 Let U_{25} be the group of units in $\mathbb{Z}_{25}$ under multiplication modulo 25. We have $|U_{25}| = \varphi(25) = 20$. If N is the subgroup generated by 7, then $N = \langle 7 \rangle = \{1,\ 7,\ 18,\ 24\}$. Since U_{25} is abelian, it follows that every subgroup including N is normal. Since $[U_{25} : N] = |U_{25}|/N = 5$, it follows that there exist 5 left cosets of N in U_{25}. We write them out

$$N = \{1,\ 7,\ 18,\ 24\},$$
$$2N = \{2,\ 11,\ 14,\ 23\},$$
$$3N = \{3,\ 4,\ 21,\ 22\},$$
$$6N = \{6,\ 8,\ 17,\ 19\},$$
$$9N = \{9,\ 13,\ 12,\ 16\}.$$

There are many ways to name these left cosets, because we can take any number of the left coset to stand in for the whole set. For example, $2N = 11N = 14N = 23N$. Then, the Cayley table for U_{25}/N is:

H	H	$2H$	$3H$	$6H$	$9H$
H	H	$2H$	$3H$	$6H$	$9H$
$2H$	$2H$	$3H$	$6H$	$9H$	H
$3H$	$3H$	$6H$	$9H$	H	$2H$
$6H$	$6H$	$9H$	H	$2H$	$3H$
$9H$	$9H$	H	$2H$	$3H$	$6H$

Example 9.22 Let G be a group such that $(ab)^p = a^p b^p$ for all $a, b \in G$, where p is a prime number. Let

$$N = \{x \in G \mid x^{p^m} = e \text{ for some } m \text{ depending on } x\}.$$

Then, N is a normal subgroup of G. If $\overline{G} = G/N$ and if $\overline{x} \in \overline{G}$ is such that $\overline{x}^p = \overline{e}$, then $\overline{x} = \overline{e}$.

Theorem 9.23 *If G is a group and $N \trianglelefteq G$, then any subgroup of G/N is in the form of H/N such that $N \trianglelefteq H \leq G$.*

Proof Suppose that $\mathcal{S}$ is a subgroup of G/N. Define $H = \{x \in G \mid xN \in \mathcal{S}\}$. First, we show that H is a subgroup of G. Since $\mathcal{S} \leq G/N$, it follows that $N \in \mathcal{S}$. This means that $e \in H$, and so H is non-empty. Now, let $a, b \in H$. Then, $aN, bN \in \mathcal{S}$. Since $\mathcal{S}$ is a subgroup, it follows that $aN(bN)^{-1} = aNb^{-1}N = ab^{-1}N \in \mathcal{S}$. This implies that $ab^{-1} \in H$, and hence H is a subgroup of G. So, by Lemma 9.11, we conclude that $N \trianglelefteq H$. Now, suppose that $A \in H/N$. Then, $A = aN$, for some $a \in H$, and so $A = aN \in \mathcal{S}$. Consequently, we obtain $H/N \subseteq \mathcal{S}$. On the other hand, if $A \in \mathcal{S}$, then $A = aN$, for some $a \in H$, and hence $A \in H/N$. Therefore, we get $\mathcal{S} = H/N$, in which $N \trianglelefteq H \leq G$. ■

Theorem 9.24 *Let G be a group and $N \trianglelefteq G$. Then, $H/N \trianglelefteq G/N$ if and only if $N \trianglelefteq H \trianglelefteq G$.*

Proof If $N \trianglelefteq H \trianglelefteq G$, then for every $aN \in G/N$ and $hN \in H/N$ we have $a^{-1}NhNaN = a^{-1}ha \in H$, which implies that $(aN)^{-1}hNaN \in H/N$. This shows that $H/N \trianglelefteq G/N$.

Conversely, if $H/N \trianglelefteq G/N$, then by Theorem 9.23, we obtain $N \trianglelefteq H \leq G$. Now, for every $a \in G$ and $h \in H$, we have $(aN)^{-1}hNaN \in H/N$, or equivalently $a^{-1}haN \in H/N$. Hence, there exists $h' \in H$ such that $a^{-1}haN = h'N$, which

implies that $h'^{-1}a^{-1}ha \in N$. Since N is a subgroup of H, it follows that $h'^{-1}a^{-1}ha \in H$. Therefore, we conclude that $a^{-1}ha \in H$. This completes the proof. ■

Exercises

1. If G is an abelian group and N is a subgroup of G, show that G/N is abelian.
2. If G is a cyclic group and N is a subgroup of G, show that G/N is cyclic.
3. What is the order of the factor group $\mathbb{Z}_{60}/\langle 15\rangle$?
4. Let G be a group with $G/Z(G)$ abelian, and let $m \in \mathbb{N}$ be odd. Prove that $G^m := \{x^m \mid x \in G\}$ is a normal subgroup of G.
5. Prove or disprove: If N is a normal subgroup of G such that N and G/N are abelian, then G is abelian.
6. Prove or disprove: If N and G/N are cyclic, then G is cyclic.
7. Suppose that N is a normal subgroup of a finite group G. If G/N has an element of order n, show that G has an element of order n. Show, by example, that the assumption that G is finite is necessary.
8. Let N be a normal subgroup of a group G and let a belong to G. If the element aN has order 3 in the group G/N and $|N| = 10$, what are the possibilities for the order of a?
9. Suppose that N is a normal subgroup of a group G. If $|N| = 4$ and aN has order 3 in G/N, find a subgroup of order 12 in G.
10. If N is a normal subgroup of a group G such that N and G/N are finitely generated, prove that so is G.
11. Let $UT_2(\mathbb{F})$ be the group of invertible upper triangular matrices with entries in $\mathbb{F}$, that is matrices of the form

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix},$$

where $a, b, c \in \mathbb{F}$ and $ac \neq 0$. Let N consists of matrices of the form

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix},$$

where $x \in \mathbb{F}$.

(a) Show that N is an abelian subgroup of $UT_2(\mathbb{F})$;
(b) Prove that N is normal in $UT_2(\mathbb{F})$;
(c) Show that $UT_2(\mathbb{F})/N$ is abelian;
(d) Is $UT_2(\mathbb{F})$ normal in $GL_2(\mathbb{F})$.

12. Let G be a group and let $K \leq H \leq G$ with $K \trianglelefteq G$. Prove that

$$N_G\left(\frac{H}{K}\right) = \frac{N_G(H)}{K}.$$

9.3 Cauchy's Theorem and Class Equation

Cauchy's Theorem gives some converse to Lagrange's Theorem.

Theorem 9.25 (Cauchy's Theorem for Abelian Groups) *Let G be a finite abelian group and p be a prime that divides the order of G. Then, G has an element of order p.*

Proof We establish this theorem by mathematical induction on $|G|$. In other words, we assume that the statement is true for all abelian groups having fewer elements than G, and we use this assumption to show that the statement holds for G as well. To start the induction we note that the statement is vacuously true for group having a single element. So, let $|G| > 1$. If G has no trivial subgroups, then G must be cyclic of prime order, and this prime must be p. Hence, there is $a \in G$ such that $G = \langle a \rangle$. This yields that $|G| = o(a) = p$, and we are finished.

Now, we assume that G has a non-trivial subgroup N. We consider two cases:

Case 1: Let $p \big| |N|$. In this case, by our induction hypothesis, since N is abelian and $|N| < |G|$, it follows that there exists a non-identity element $x \in N \subset G$ such that $o(x) = p$, and we are done.

Case 2: Let $p \nmid |N|$. Since G is abelian, it follows that N is a normal subgroup of G. Hence, we may construct the factor group G/N. Moreover, G/N is abelian. Since $|G/N| = |G|/|N|$ and $p \nmid |N|$, it follows that $p \big| |G/N| < |G|$. Hence, by our induction assumption, there is a left coset $xN \in G/N$ such that $o(xN) = p$. Then, we obtain $(xN)^p = x^p N = N$. This implies that $x^p \in N$ and $x \notin N$, consequently $\left(x^p\right)^{|N|} = x^{p|N|} = e$. Take $y = x^{|N|}$, then $y^p = e$. At the end, we must show that $y \neq e$. Indeed, if $y = e$, then $x^{|N|} = e$, and so $(xN)^{|N|} = N$. On the other hand, since $(xN)^p = N$ and $p \nmid |N|$, we conclude that $xN = N$, or equivalently $x \in N$, it is a contradiction. Consequently, $y \neq e$ and $y^p = e$. Therefore, y is the desired element of order p. ■

Theorem 9.26 *If G is a finite abelian group and a positive integer m divides $|G|$, then G contains a subgroup of order m.*

Proof We proceed by mathematical induction over $|G|$. If $|G| = 1$, then m must be 1. In this case G is its own subgroup of order m. To apply induction, let $|G| > 1$ and assume that the statement is true for every abelian group of order less than $|G|$. We can suppose that $m > 1$, because for $m = 1$, $\{e\}$ is the subgroup of G of order 1. Let p be a prime number such that $p|m$. We conclude that $p \big| |G|$. Then, by Cauchy's Theorem, there is $a \in G$ such that $o(a) = p$. Let $N = \langle a \rangle$ be the cyclic

group generated by a. Then, we have $|N| = p$. Now, G/N is an abelian group such that $|G/N| = |G|/|N| < |G|$. Since $p|m$, it follows that $m = kp$, for some positive integer k. Moreover, we have $k\big||G/N|$. Hence, by our induction assumption and Theorem 9.23, G/N has a subgroup H/N of order k, where H is a subgroup of G containing N. Consequently, we obtain $|H| = |H/N| \cdot |N| = kp = m$. This completes the proof. ■

Let $a, b \in G$. We recall that b is a conjugate of a in G if $b = xax^{-1}$, for some $x \in G$, and in this case, we write $a \sim_{Conj} b$. In Theorem 3.53, we showed that the conjugacy relation is an equivalence relation. For each $a \in G$, let $C(a) = \{b \in G \mid a \sim_{Conj} b\}$, the equivalence class of $a \in G$ under $\sim_{Conj}$ relation, and it is usually called the *conjugate class* of $a \in G$.

Our attention now narrow to the case in which G is a finite group. Let G be a finite group, and suppose that $C(a_1), C(a_2), \ldots, C(a_m)$ are the totally of all conjugate classes of G. For each $a \in G$, let $c_a = |C(a)|$. Since conjugacy classes are disjoint and their union is G, we obtain

$$|G| = \sum_{i=1}^{m} c_{a_i}.$$

Theorem 9.27 *If G is a finite group, then*

$$c_a = \frac{|G|}{|C_G(a)|},$$

in other words, the number of elements conjugate to a in G is the index of the centralizer of a in G.

Proof Let $C_G(a)$ has k distinct left cosets, say $x_1C_G(a), x_2C_G(a), \ldots, x_kC_G(a)$. Then, we know that $k = [G : C_G(a)]$. We claim that for every $i \neq j$, $x_iax_i^{-1}$ and $x_jax_j^{-1}$ are distinct conjugate of a. Indeed, if $x_iax_i^{-1} = x_jax_j^{-1}$, for some $i \neq j$, then we conclude that

$$\begin{aligned} x_j^{-1}x_iax_i^{-1}x_j = a &\Rightarrow (x_j^{-1}x_i)a(x_j^{-1}x_i)^{-1} = a \Rightarrow (x_j^{-1}x_i)a = a(x_j^{-1}x_i) \\ &\Rightarrow x_j^{-1}x_i \in C_G(a) \Rightarrow x_iC_G(a) = x_jC_G(a) \Rightarrow i = j. \end{aligned}$$

Now, we show that $x_1ax_1^{-1}, \ldots, x_kax_k^{-1}$ are all distinct conjugate of a. Let $b = xax^{-1}$, for some $x \in G$. Since

$$G = \bigcup_{i=1}^{k} x_iC_G(a),$$

it follows that $x = x_iy$, for some $y \in C_G(a)$ and positive integer i. Then, we can write

$$xax^{-1} = (x_i y)a(x_i y)^{-1} = x_i yay^{-1}x_i^{-1} = x_i ax_i^{-1}.$$

Consequently, any conjugate b of a is equal to one of the $x_i ax_i^{-1}$. Therefore, a has exactly k conjugate. This yields that $C(a)$ contains exactly k elements. ■

Corollary 9.28 *If G is a finite group, then*

$$|G| = \sum_a \frac{|G|}{|C_G(a)|},$$

where this sum runs over one element a in each conjugate class.

Proof Since $|G| = \sum c_a$, using Theorem 9.27, the result immediately follows. ■

Lemma 9.29 *Let G be a group. Then, $a \in Z(G)$ if and only if $C_G(a) = G$.*

Proof It is straightforward. ■

In Lemma 9.29, if G is finite, then $|C_G(a)| = |G|$ is equivalent to $C_G(a) = G$.

Corollary 9.30 *Let G be a finite group, then*

$$|G| = |Z(G)| + \sum_a \frac{|G|}{|C_G(a)|},$$

where the sum runs over elements a, taken one from each of those distinct conjugate classes which contains more than one element.

Proof By Lemma 9.29, $a \in Z(G)$ if and only if $c_a = 1$. Since there are $|Z(G)|$ number of conjugate classes each having only one element, the corollary follows. ■

The equation in Corollary 9.30 is usually referred to as the class equation of G.

Theorem 9.31 (Cauchy's Theorem) *Let G be a finite group and $p \big| |G|$. Then, G has an element of order p.*

Proof We do the proof by mathematical induction. The statement is vacuously true for groups of order 1. We assume the statement holds for all groups having fewer elements than G, and then we prove the statement is true for G. We consider the following two cases:

Case 1: There exists a proper subgroup H of G such that $p \big| |H|$. Then, by our induction assumption there exists an element a of order p in H, and so it is also in G.

Case 2: p is not divisor of the order of any proper subgroup of G. If $G \neq Z(G)$, then there exists $a \notin Z(G)$. Hence, we obtain $C_G(a) \neq G$. Since $C_G(a)$ is a subgroup of G, by our assumption, we conclude that $p \nmid |C_G(a)|$. We write down the class equation:

$$|G| = |Z(G)| + \sum_{C_G(a)\neq G} \frac{|G|}{|C_G(a)|}.$$

Since $p\big||G|$ and $p \nmid |C_G(a)|$, it follows that

$$p\Big|\frac{|G|}{|C_G(a)|}.$$

Thus, we obtain

$$p\Big|\sum_{C_G(a)\neq G} \frac{|G|}{|C_G(a)|}.$$

Since also we have $p\big||G|$, it follows that

$$p\Big|\Big(|G| - \sum_{C_G(a)\neq G} \frac{|G|}{|C_G(a)|}\Big),$$

and consequently, $p\big||Z(G)|$. But we assumed that p is not divisor of the order of any proper subgroup of G, so we conclude that $Z(G)$ can not be a proper subgroup of G. This means that $Z(G) = G$, i.e., G is abelian. Now, by Cauchy Theorem for abelian groups, the result follows. ■

Exercises

1. In this exercise, we obtain a simple proof of Cauchy's Theorem. Let G be a finite group of order n and p be a prime number such that $p|n$. Consider the set

$$S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1a_2 \ldots a_p = e\}.$$

   (a) Compute $|S|$, the number of elements in S;
   (b) Define a relation ρ on S by saying two p-tuples are related if one is a cycle permutation of the other. For example, $(a_1, a_2, \ldots, a_p)\rho(a_2, a_3, \ldots, a_p, a_1)$. Show that ρ is an equivalence relation.
   (c) If all component of a p-tuple are equal, show that its equivalence class contains only one element; otherwise, if two components of a p-tuple are distinct, there are p elements in the equivalence class;
   (d) Let r denote the number of solutions to the equation $x^p = e$. Then, r equals the number of equivalence classes with only one element. Let s denote the number of equivalence classes with p elements. Show that $r + sp = n^{p-1}$;

(e) Deduce Cauchy's Theorem from the above, namely, G has kp solutions to the equation $x^p = e$.

2. If all non-identity elements of a group G have the same order, show that this order is a prime p and $|G|$ is a power of p.
3. Prove that any normal subgroup of order $2p$, where p is a prime number, has a normal subgroup of order p.
4. If G is an abelian group of order $p_1 p_2 \dots p_k$, where $p_1, p_2, \dots, p_k$ are distinct primes, prove that G is cyclic.

9.4 Worked-Out Problems

Problem 9.32 Let H be a cyclic subgroup of a group G and let $H \trianglelefteq G$. If N is a subgroup of H, prove that $N \trianglelefteq G$.

Solution Suppose that $H = \langle x \rangle$ is a normal subgroup of G and let $a \in G$ is arbitrary. Since H is normal, it follows that $axa^{-1} \in H$. Hence, we have $axa^{-1} = x^k$, for some integer k. If N is a subgroup of H, then N is cyclic and generated by x^n, for some integer n. Now, we obtain $ax^n a^{-1} = (axa^{-1})^n = x^{kn} = (x^n)^k \in N$. This completes the proof. ■

Problem 9.33 Let N be a normal subgroup of a finite group G. If $|N|$ and $[G : N]$ are relatively prime, prove that any element $a \in G$ satisfying $a^{|N|} = e$ must belong to N.

Solution Suppose that $a \in G$ such that $a^{|N|} = e$. Since $([G : N], |N|) = 1$, it follows that there exist integers m and n such that $m[G : N] + n|N| = 1$. Then, we deduce that

$$a = a^{m[G:N]+n|N|} = a^{m[G:N]} a^{n|N|} = a^{m[G:N]} \left(a^{|N|}\right)^n = a^{m[G:N]}.$$

Now, we consider aN as an element of G/N. Then, we have $(aN)^{|G/N|} = a^{|G/N|}N = N$, the identity element of G/N. This yields that $a^{|G/N|} \in N$, and consequently, $a = \left(a^{[G:N]}\right)^m \in N$. ■

Problem 9.34 Let G be a group and $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, prove that G is abelian.

Solution To start, every elements in the factor group $G/Z(G)$ is a left coset $aZ(G)$ with $a \in G$. Since $G/Z(G)$ is cyclic, it follows that $G/Z(G) = \langle xZ(G) \rangle$, for some $x \in G$. Now, let a and b be elements of G so that $aZ(G)$ and $bZ(G)$ belong to $G/Z(G)$. It follows that there exist integers i and j such that $aZ(G) = \left(xZ(G)\right)^i = x^i Z(G)$ and $bZ(G) = \left(xZ(G)\right)^j = x^j Z(G)$. Hence, $a = x^i z_1$ and $b = x^j z_2$, for some $z_1, z_2 \in Z(G)$. Then, by the definition of center and laws of exponents, we have

$$ab = (x^i z_1)(x^j z_2) = x^i x^j z_1 z_2 = x^j x^i z_2 z_1 = (x^j z_2)(x^i z_1) = ba.$$

Now, we conclude that G is abelian. ■

Problem 9.35 If G is a group of order p^n, where p is a prime number, prove that $Z(G) \neq \{e\}$.

Solution Suppose that $|Z(G)| = m$. By the class equation, we have

$$|G| = m + \sum_a \frac{|G|}{|C_G(a)|},$$

where sum runs over element a, taken one from each of conjugate class which has more than one element. Now, for each $a \notin Z((G)$, we have $|C_G(a)|\big||G|$. This implies that $|C_G(a)| = p^{k_a}$, for some integer $1 \leq k_a < n$. Hence, we obtain

$$p\Big|\Big(p^n - \sum_a \frac{p^n}{p^{k_a}}\Big) = m.$$

Since $e \in Z(G)$, it follows that m is non-zero. Hence, m is a positive integer divisible by the prime number p, and so we conclude that $m > 1$. This shows that $Z(G) \neq \{e\}$. ■

Problem 9.36 Let G be a group of order p^n, where p is a prime number. Prove that every subgroup of order p^{n-1} of G is normal.

Solution Suppose that H is a subgroup of G and $|H| = p^{n-1}$. We establish the proof by mathematical induction. If $n = 1$, then $|G| = p$ and $H = \{e\} \trianglelefteq G$. Suppose that $n > 1$ and the statement is true for every group of order p^m, where $1 \leq m < n$. We know that $H \trianglelefteq N_G(H)$. We consider the following two cases:

Case 1: $N_G(H) \neq H$. In this case, $|N_G(H)| = p^n$, and so $N_G(H) = G$. This means that $H \trianglelefteq G$.

Case 2: $N_G(H) = H$. Since $Z(G) \subseteq N_G(H)$, it follows that $Z(G) \subseteq H$. Since $p\big||Z(G)|$, by Cauchy's Theorem it follows that there exists $a \in Z(G)$ such that $o(a) = p$. Take $K = \langle a \rangle$, then K is a normal subgroup of order p in G. Now, we have $|H/K| = p^{n-2}$, so by our induction assumption, we conclude that $H/K \trianglelefteq G/K$, because $|G/K| = p^{n-1}$. Therefore, H is a normal subgroup of G. ■

Problem 9.37 If G is a group of order p^2, prove that G is abelian.

Solution As a group G is abelian if and only if $Z(G) = G$, our aim is to show that $Z(G) = G$. Since $|G| = p^2$, by Lagrange's Theorem, $|Z(G)|\big|p^2$. This implies that $|Z(G)| = 1$, p or p^2. By Problem 9.35, we conclude that $|Z(G)| \neq 1$. Assume that $|Z(G)| = p$. Take $a \in G$ such that $a \notin Z(G)$. Then, $C_G(a)$ is a subgroup of G and $Z(G)$ is a subset of $C_G(a)$. Since $a \notin Z(G)$ and $a \in C_G(a)$, it follows that $Z(G) \neq C_G(a)$. Hence, we have $p = |Z(G)| < |C_G(a)|$. Then, we conclude that

$|C_G(a)| = p^2$ or $C_G(a) = G$. This means that all of elements of G commute with a, and so $a \in Z(G)$, a contradiction. Thus, $|Z(G)| = p$ is not an actual possibility. Therefore, $|Z(G)| = p^2$, and so $G = Z(G)$. ■

9.5 Supplementary Exercises

1. (a) Let N be a normal subgroup of a group G, with G/N abelian. Does it follow that $G = HN$ for some abelian subgroup H of G? Give a proof or a counterexample.
   (b) Answer the same question, with both occurrences of "abelian" replaced by "cyclic".
2. Suppose that $K \trianglelefteq G$ with $|K| = m$. Let $x \in G$ and n be a positive integer such that $(m, n) = 1$. Prove that
   (a) If $o(x) = n$, then $o(xK) = n$;
   (b) If $o(xK) = n$, then there is an element $y \in G$ such that $o(y) = n$ and $xK = yK$.
3. Let N be a normal subgroup of a group G. If $x, y \in G$ such that $xy \in N$, show that $yx \in N$.
4. Let H be a subgroup of index 2 in a finite group G. If the order of H is odd and every element of $G \setminus H$ is of order 2, prove that H is abelian.
5. Suppose that G is a finite abelian group such that each element of G has order 1 or 3. If H is a subgroup of G, show that each element of G/H has order 1 or 3. Use induction on $|G|$ to show that $|G| = 3^k$, for some positive integer k.
6. For which values of n is it true that the dihedral group D_n has a pair of proper normal subgroups H and K for which $D_n = HK$ and $H \cap K$ is singleton.
7. If $K \leq H \leq G$ and $N \trianglelefteq G$, show that the equations $HN = KN$ and $H \cap N = K \cap N$ imply that $H = K$.
8. Let G be a finite group, H be a subgroup of G, and $N \trianglelefteq G$. If $|H|$ and $[G : N]$ are relatively prime, prove that H is a subgroup of N.
9. Let G be a finite group and $N \trianglelefteq G$. If $|N|$ and $[G : N]$ are relatively prime, prove that N is the unique subgroup of G of order N.
10. Let G be a group and H be the intersection of all subgroups of G that have finite index in G. Show that H is normal in G.
11. Let G be a group and H be a subgroup of G with finite index. Show that there is a normal subgroup N of G for which $N \leq H \leq G$ where N also has finite index in G.
12. Prove that the torsion subgroup T of an abelian group G is a normal subgroup of G, and that G/T is torsion free.
13. Let N be a normal subgroup of G of index n. Show that if $a \in G$, then $a^n \in N$. Give an example to show that this may be false when N is not normal.
14. If $|G| = pq$, where p and q are not necessarily distinct primes, prove $|Z(G)| = 1$ or G is abelian.

15. If H and K are subgroups of finite index in a group G, and $[G : H]$ and $[G : K]$ are relatively prime, prove that $G = HK$.
16. If G is a non-abelian group of order p^3, where p is a prime number, show that $|Z(G)| = p$.
    Hint: Use Problem 9.34.
17. Let G be a finite group and p be the smallest prime number such that $p \big| |G|$. If $N \trianglelefteq G$ and $|N| = p$, prove that $N \leq Z(G)$.
18. If H is a subgroup of finite index in a group G, prove that H contains a subgroup N which is of finite index and normal in G.
19. The set X is called a *normal subset* of G if G is the normalizer of X. Let X be a finite normal subset of a group G such that for some positive integer n, $x^n = e$, for all $x \in X$. Prove that every element of the group $H = \langle X \rangle$ may be written as a product of not more than $(n-1)|X|$ elements of X. In particular, H is a finite group.