Chapter 8
Cosets of Subgroups and Lagrange's Theorem

In group theory, the result known as Lagrange's theorem states that for a finite group G the order of any subgroup divides the order of G. Lagrange's theorem is one of the central theorems of group theory. In order to prove this theorem we introduce the notion of cosets of a subgroup.

8.1 Cosets and Their Properties

To understand Lagrange's theorem, one has to look at cosets of a subgroup. This notion was invented by Galois in 1830, although the term was coined by G.A. Miller in 1910.

Definition 8.1 Let G be a group and H be a subgroup of G. For any $a \in G$, the set $aH = \{ah \mid h \in H\}$ is called the *left coset of H in G containing a*. Analogously, $Ha = \{ha \mid h \in H\}$ is called the *right coset of H in G containing a*.

In other words, a coset is what we get when we take a subgroup and shift it (either on the left or on the right). The best way to think about cosets is that they are shifted subgroups, or translated subgroups. Note that a lies in both aH and Ha, since $a = ae = ea$. If the left and right cosets coincide or if it is clear from the context to which type of coset that we are referring to, we will use the word coset without specifying left or right. In additive notation, we get $a + H$ (which usually implies that we deal with a commutative group where we do not need to distinguish left and right cosets). Any element of a coset is called a representative of that coset.

Example 8.2 Let $G = \mathbb{Z}$, the additive group of integers, and $H = \langle m \rangle = m\mathbb{Z}$, the subgroup generated by m, for some $m \in \mathbb{Z}$. The set of left cosets is $\{H,\ 1 + H,\ 2 + H,\ \ldots,\ m - 1 + H\}$. Since $a + H = H + a$, left cosets coincide with right cosets.

B. Davvaz, *A First Course in Group Theory*,
https://doi.org/10.1007/978-981-16-6365-9_8

Example 8.3 Let $G = S_3$, the symmetric group of an equilateral triangle. Take the subgroup $H = \{id,\ (1\ 3)\}$. Then, the left cosets are

$$\begin{aligned}(1\ 2)H &= \{(1\ 2),\ (1\ 2)(1\ 3)\} = \{(1\ 2),\ (1\ 2\ 3)\} = (1\ 2\ 3)H,\\ (1\ 3)H &= \{(1\ 3),\ (1\ 3)(1\ 3)\} = \{(1\ 3),\ id\} = H,\\ (2\ 3)H &= \{(2\ 3),\ (2\ 3)(1\ 3)\} = \{(2\ 3),\ (1\ 3\ 2)\} = (1\ 3\ 2)H.\end{aligned}$$

Example 8.4 If $G = GL_2(\mathbb{R})$ and $H = SL_2(\mathbb{R})$, then for any matrix $A \in G$, the coset AH is the set of all 2×2 matrices with the same determinant as A. Thus, the coset $\begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix} H$ is the set of all 2×2 matrices of determinant 3.

Theorem 8.5 (Properties of Cosets) *Let G be a group and H be a subgroup of G. Then,*

(1) $a \in aH$;
(2) $aH = H$ if and only if $a \in H$;
(3) $(ab)H = a(bH)$ and $H(ab) = (Ha)b$;
(4) $aH = bH$ if and only if $a \in bH$;
(5) $aH = bH$ or $aH \cap bH = \emptyset$;
(6) $aH = bH$ if and only if $a^{-1}b \in H$;
(7) $|aH| = |bH|$;
(8) aH is a subgroup of G if and only if $a \in H$.

Proof (1) We have $a = ae \in \{ah \mid h \in H\} = aH$.

(2) Suppose that $aH = H$. Then, $a = ae \in aH = H$. Conversely, let $a \in H$. We show that $aH \subseteq H$ and $H \subseteq aH$. The first inclusion follows immediately from the closure of H. In order to show that $H \subseteq aH$, assume that $h \in H$ is an arbitrary element. Since $a \in H$ and $h \in H$, it follows that $a^{-1}h \in H$. Consequently, we get $h = eh = (aa^{-1})h = a(a^{-1}h) \in H$.

(3) This follows directly from $(ab)h = a(bh)$ and $h(ab) = (ha)b$, for all $h \in H$.

(4) If $aH = bH$, then $a = ae \in aH = bH$. Conversely, if $a \in bH$, then there exists $h \in H$ such that $a = bh$. So, we deduce that $aH = (bh)H = b(hH) = bH$.

(5) This property follows directly from (4). Because if $aH \cap bH \neq \emptyset$, then there exists $c \in aH \cap bH$. This implies that $cH = aH$ and $cH = bH$, and so $aH = bH$.

(6) We observe that $aH = bH$ if and only if $H = a^{-1}bH$. Now, the result follows from (2).

(7) In order to show that $|aH| = |bH|$, it is enough to define a one to one function from aH onto bH. For this, we define $f : aH \to bH$ by $f(ah) = bH$. Obviously, f is onto. Moreover, from the cancellation law, f is one to one. This shows that f is a one to one correspondence.

(8) Assume that aH is a subgroup of G. Then, it contains the identity e. So, we get $aH \cap eH \neq \emptyset$. Then, from (5) we have $aH = eH = H$. Now, from (2), we conclude that $a \in H$. Conversely, if $a \in H$, then again by (2), we obtain $aH = H$. ■

Remark 8.6 In Theorem 8.5, analogous results hold for right cosets.

Theorem 8.7 *If H and K are two subgroups of a group G, then for any $a, b \in G$ either $aH \cap bK = \emptyset$ or $aH \cap bK = c(H \cap K)$, for some $c \in G$.*

Proof Suppose that $aH \cap bK \neq \emptyset$, and let $c \in aH \cap bK$. Since $c \in cH$ and $c \in cK$, it follows that $c \in aH \cap cH$ and $c \in bK \cap cK$. Consequently, we obtain $aH = cH$ and $bK = cK$, and so $aH \cap bK = cH \cap cK$. Moreover, it is not difficult to see that $c(H \cap K) \subseteq cH \cap cK$. On the other hand, if $x \in cH \cap cK$, then $x = ch = ck$, for some $h \in H$ and $k \in K$. This implies that $h = c^{-1}x = k \in H \cap K$. So, $x \in c(H \cap K)$. Therefore, we conclude that $aH \cap bK = cH \cap cK = c(H \cap K)$. ■

Theorem 8.8 *Let G be a group and H be a subgroup of G. If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.*

Proof Consider the mapping $f : \mathcal{R} \to \mathcal{L}$ defined by $f(Ha) = a^{-1}H$. First, we need to show that f is well defined. Namely, if we take two different representations of the same right coset we must show our mapping sends them to the same image. Suppose that $Ha = Hb$. Then, we know that $Hab^{-1} = H$ or $ab^{-1} \in H$. Let $ab^{-1} = h$, where $h \in H$. Then, $a^{-1}h = b^{-1}$ and so $a^{-1}hH = b^{-1}H$, or equivalently $a^{-1}H = b^{-1}H$. Consequently, we have $f(Ha) = f(Hb)$ as desired. Therefore, f is well defined.

Now, assume that $f(Ha) = f(Hb)$. Then, $a^{-1}H = b^{-1}H$. This yields that $ba^{-1}H = H$, or equivalently $ba^{-1} \in H$. If $ba^{-1} = h$, where $h \in H$, then $b = ha$. Consequently, $Hb = Hha$ and so $Ha = Hb$. Thus, f is one to one. In addition, if $aH \in \mathcal{L}$ is an arbitrary element, then $f(Ha^{-1}) = (a^{-1})^{-1}H = aH$. This shows that f is onto. Therefore, f is a one to one correspondence between $\mathcal{L}$ and $\mathcal{R}$. ■

Exercises

1. List the left and right cosets of the subgroup $\{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ in A_4.
2. If G is a group and $\{H_i \mid i \in I\}$ is a family of subgroups of G, show that $\Big(\bigcap_{i\in I} H_i\Big)a = \bigcap_{i\in I} H_i a$.
3. Suppose that $G = Q_8$ and let $H = \langle -1 \rangle$ and $K = \langle I \rangle$ be subgroups of G. Find
   (a) the left cosets of H and K in G;
   (b) the right cosets of H and K in G.
4. Suppose that H and K are subgroups of G and there are elements a and b in G such that $aH \subseteq bK$. Prove that $H \subseteq K$.
5. Let G be a group and $a \in G$. If $o(a) = 30$, how many cosets of $\langle a^4 \rangle$ in $\langle a \rangle$ are there? List them.
6. Give an example of a group G having a subgroup H and two elements a, b such that $Ha = Hb$ but $aH \neq bH$.
7. Find an example of a subgroup H of a group G and elements a and b in G such that $aH \neq Hb$ and $aH \cap Hb \neq \emptyset$.

8. Suppose that H and K are subgroups of a group G with $H \leq K$. Show that for each $a \in G$, either $aH \subseteq K$ or $aH \cap K = \emptyset$.

8.2 Geometric Examples of Cosets

When a group is defined in terms of vectors and matrices, we can often get a picture of the group and its cosets.

Example 8.9 Let $G = \mathbb{R}^2 = \{xi + yj \mid x, y \in \mathbb{R}\}$, the additive group of vectors in a plane, where $i = (1, 0)$ and $j = (0, 1)$. Suppose that $H = \{xi \mid x \in \mathbb{R}\}$ and $v = ai + bj$ is a vector in G. Then, the left coset of H in G containing v is

$$v + H = \{(a + x)i + bj \mid x \in \mathbb{R}\}.$$

This is the line parallel to H that passes through the endpoint of v. The left cosets of H in G, in general, are the lines parallel to H. Two parallel lines are either equal or disjoint, so any two left cosets of H in G are equal or disjoint. In Fig. 8.1, the cosets H in G containing v and v' are equal while those of u, v, and w are disjoint.

Example 8.10 Let $\mathbb{C}^*$ be the group of non-zero complex numbers (see Example 3.36), and let $H = \{a + bi \mid a^2 + b^2 = 1,\ a, b \in \mathbb{R}\}$ be the subgroup of $\mathbb{C}^*$, which is defined in Example 3.66. First, notice that geometrically H is a circle of radius 1 with center $(0, 0)$. Let $4 + 3i$ be an element of $\mathbb{C}^*$. We want to study the coset of H in $\mathbb{C}^*$ containing $4 + 3i$. Of course, $\mathbb{C}^*$ is abelian, so there is no distinction between the left and the right cosets, and they are the same. The coset of H in $\mathbb{C}^*$ containing $4 + 3i$ is of the form $(4 + 3i)H$, and it is a circle with center $(0, 0)$ too. However, $4 + 3i$ scales the equation so that 1 becomes $4^2 + 3^2 = 25$. In order to see this,

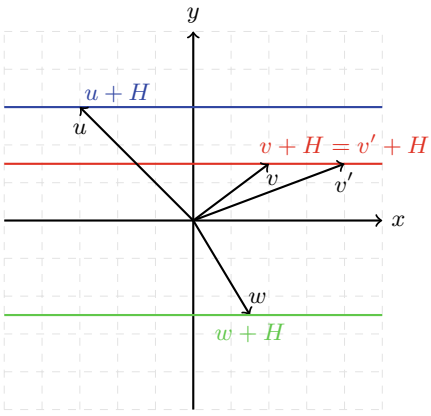

Fig. 8.1 The cosets of $v + H$ in $\mathbb{R}^2$

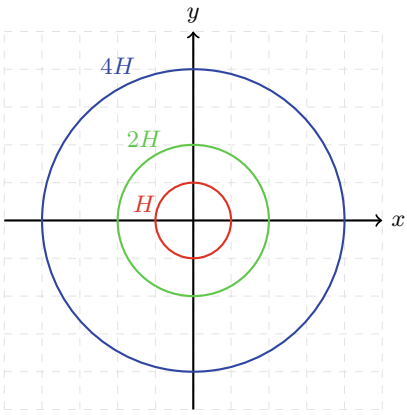

Fig. 8.2 H and its cosets $2H$ and $4H$ in $\mathbb{C}^*$

we have $(4+3i)(a+bi) = (4a-3b)+(3a+4b)i$. So, the multiplication $4+3i$ sends the point $(a,b) \in H$ to the point $(4a-3b,\ 3a+4b)$. Now, this gives us the equation

$$\begin{aligned}(4a-3b)^2+(3a+4b)^2 &= 16a^2+9b^2-24ab+9a^2+16b^2-24ab\\ &= 25a^2+25b^2 = 25(a^2+b^2) = 25.\end{aligned}$$

Now, we consider the general case. If $z \in \mathbb{C}^*$ be an arbitrary number, we can write $z = re^{i\theta}$, where r is the absolute value of z and θ is the argument of z. Consider $e^{i\theta}H$. Multiplying any complex number by $e^{i\theta}$ simply rotates anticlockwise through angle θ about the origin. Hence, we deduce that $e^{i\theta}H = H$. So, we obtain $zH = rH$. What does multiplying by r do? It scales the circle H by a factor of r. Two different positive real numbers $r \neq r'$ give different cosets $rH \neq r'H$, since the first has radius r and the second has radius r'. For illustration, see Fig. 8.2. Therefore, the cosets of H in $\mathbb{C}^*$ are the circles centered at the origin of positive radius.

Example 8.11 Let $G = \{(a,b) \mid a, b \in \mathbb{R} \text{ and } a > 0\}$ be the group defined in Example 3.42 with the following binary operation:

$$(a,b) \star (c,d) = (ac, bc+d),$$

for all $(a,b),\ (c,d) \in G$. Suppose that

$$\begin{aligned}H &= \{(1,y) \mid y \in \mathbb{R}\},\\ K &= \{(x,0) \mid x \in \mathbb{R} \text{ and } x > 0\}.\end{aligned}$$

It is easy to check that H and K are subgroups of G. These subgroups are indicated in Fig. 8.3. Now, let $(a,b) \in G$. What are the left and right cosets of H in G containing (a,b)? We observe that

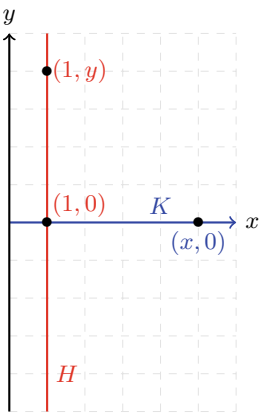

Fig. 8.3 Subgroups H and K

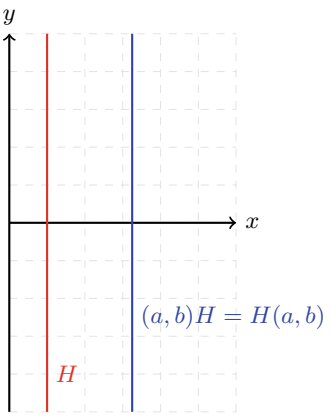

Fig. 8.4 Left and right cosets of H in G containing (a, b)

$$(a, b)(1, y) = (a, b + y) \text{ and } (1, y)(a, b) = (a, ay + b),$$

for all $(1, y) \in H$. Clearly, the numbers $b + y$ and $ay + b$ run over $\mathbb{R}$. This yields that the left and the right cosets of H in G containing (a, b) are the same. In other words, we have

$$(a, b)H = H(a, b) = \{(a, z) \mid z \in \mathbb{R}\},$$

and this is the vertical line parallel to H passing through the point (a, b), see Fig. 8.4. Now, we determine the right coset of K in G containing (a, b). We have

$$(x, 0)(a, b) = (xa, b),$$

for all $(x, 0) \in K$. Since $x > 0$, it follows that (xa, b) runs through all points of the form (z, b) with $z > 0$. Consequently, we can write

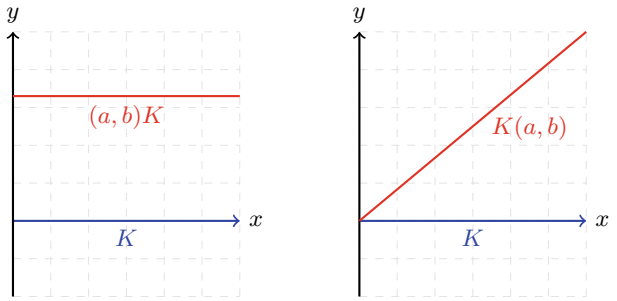

Fig. 8.5 Left and right cosets of K in G containing (a, b)

$$K(a, b) = \{(z, b) \mid z \in \mathbb{R} \text{ and } z > 0\}.$$

In view of this, the right coset of K in G containing (a, b) is determined by b alone and it is independent of the choice of a. So, it is horizontal line through (a, b). See the left hand picture in Fig. 8.5. Finally, we try to find the left coset of K in G containing (a, b). We have

$$(a, b)(x, 0) = (ax, bx),$$

for all $(x, 0) \in K$. If we take $ax = r$, then $bx = br/a$. So, we can write

$$(a, b)K = \left\{(r, s) \mid r, s \in \mathbb{R},\ r > 0,\ \text{and } s = \frac{b}{a}r\right\}.$$

This is a half line out of the origin with slope b/a. See the right hand picture in Fig. 8.5. We observe that the left and right cosets of K in G containing (a, b) are not the same if $b \neq 0$.

Example 8.12 We know that $G = \mathbb{R}^3$ forms a group under the following binary operation:

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2).$$

If we consider the subset

$$H = \{(x, y, z) \mid 2x + 7y - 3z = 0\},$$

then we observe that H is a subgroup of G. In geometrical terms, H is a plane through the origin in a three-dimensional space. The left coset $(a, b, c) + H$ is, in general terms, nothing more than the plane P passing through the point (a, b, c) and parallel to H in $\mathbb{R}^3$. For illustration, in Fig. 8.6 we consider $(a, b, c) = (0, 2, 0)$.

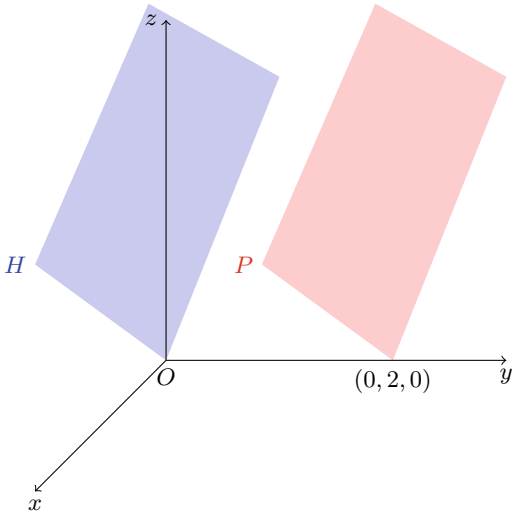

Fig. 8.6 The left coset $(0, 2, 0) + H$ is the plane P passing through the point $(0, 2, 0)$ and parallel to H

Exercises

1. In $\mathbb{R}^2$ under component addition, let $H = \{(x, 5x) \mid x \in \mathbb{R}\}$, the subgroup of all points on the line $y = 5x$. Show that the left coset $(3, 2) + H$ is the straight line passing through the point $(3, 2)$ and parallel to the line $y = 5x$.
2. Consider the additive group $\mathbb{R}$ and its subgroup $\mathbb{Z}$. Describe a coset $t + \mathbb{Z}$ geometrically. Show that the set of all cosets of $\mathbb{Z}$ in $\mathbb{R}$ is $\{t + \mathbb{Z} \mid 0 \leq t < 1\}$. What are the analogous results for $\mathbb{Z}^2 \subseteq \mathbb{R}^2$?
3. Show that the function sine assigns the same value to each element of any fixed left coset of the subgroup $\langle 2\pi \rangle$ of the additive group $\mathbb{R}$ of real numbers. Thus sine induces a well-defined function on the set of cosets; the value of the function on a coset is obtained when we choose an element x of the coset and compute $\sin x$.

8.3 Lagrange's Theorem

Let H be a subgroup of a group G, which may be of finite or infinite order. We reconsider some parts of Theorem 8.5 in a different view. We exhibit two partitions of G by defining two equivalence relations, $\equiv_L$ and $\equiv_R$ on G.

Theorem 8.13 *Let H be a subgroup of G. Let the relation $\equiv_L$ be defined on G by*

$$a \equiv_L b (\text{mod } H) \Leftrightarrow a^{-1}b \in H.$$

Also, let the relation $\equiv_R$ be defined on G by

$$a \equiv_R b (\text{mod } H) \Leftrightarrow ab^{-1} \in H.$$

Then, $\equiv_L$ and $\equiv_R$ are both equivalence relations on G.

Proof We show that $\equiv_L$ is an equivalence relation, and leave the proof for $\equiv_R$ as exercise. We must verify the following conditions, for all $a, b, c \in G$,

(1) $a \equiv_L a (\text{mod } H)$;
(2) $a \equiv_L b (\text{mod } H)$ implies $b \equiv_L a (\text{mod } H)$;
(3) $a \equiv_L b (\text{mod } H)$ and $b \equiv_L c (\text{mod } H)$ imply $a \equiv_L c (\text{mod } H)$.

Now, we prove the above items.

(1) Since H is a subgroup, it follows that $a^{-1}a = e$ and $e \in H$, which is what we were required to demonstrate.

(2) Suppose that $a \equiv_L b (\text{mod } H)$. Then $a^{-1}b \in H$. Since H is a subgroup, it follows that $(a^{-1}b)^{-1} \in H$. But $(a^{-1}b)^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a$. Hence, $b^{-1}a \in H$ and $b \equiv_L a (\text{mod } H)$.

(3) Finally, we require that $a \equiv_L b (\text{mod } H)$ and $b \equiv_L c (\text{mod } H)$ force $a \equiv_L c (\text{mod } H)$. Indeed, we have $a^{-1}b \in H$ and $b^{-1}c \in H$. Again, since H is a subgroup, we conclude that $(a^{-1}b)(b^{-1}a) = a^{-1}c \in H$, from which it follows that $a \equiv_L c (\text{mod } H)$. ■

If $[a]_L$ and $[a]_R$ are the equivalence classes containing a related to $\equiv_L$ and $\equiv_R$, respectively, then we have $[a]_L = aH$ and $[a]_R = Ha$.

The left cosets of H in G define a partition of G, i.e.,

(1) For each $a \in G$, $aH \neq \emptyset$;
(2) For any $a, b \in G$, $aH = bH$ or $aH \cap bH = \emptyset$;
(c) $G = \bigcup_{a \in G} aH$.

We can now prove the theorem of Lagrange.

Theorem 8.14 (Lagrange's Theorem) *Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.*

Proof Let us start by recalling that the left cosets of H forms a partition of G. Since G is finite, it follows that there exists a finite number of disjoint left cosets, namely $a_1H, a_2H, \ldots, a_nH$. So, we have

$$G = a_1H \cup a_2H \cup \cdots \cup a_nH \text{ and } a_iH \cap a_jH = \emptyset, \text{ for all } i \neq j.$$

Let us look at the cardinality of G. We can write

$$|G| = |a_1H \cup a_2H \cup \cdots \cup a_nH| = \sum_{i=1}^{n} |a_iH|.$$

By Theorem 8.5 (7), the cosets of H in G all have some size of H, i.e., $|a_iH| = |H|$, for all $1 \leq i \leq n$. This yields that

$$|G| = \underbrace{|H| + |H| + \cdots + |H|}_{n \text{ times}} = n|H|.$$

This shows that the order of H is a divisor of the order of G. ■

There are several corollaries of Lagrange's theorem.

Corollary 8.15 *If G is a finite group and $a \in G$, then $o(a)||G|$.*

Proof Since $\langle a \rangle$ is a subgroup of G, then the order of $\langle a \rangle$ is a divisor of order G. By Corollary 4.27, we know that $o(a) = |\langle a \rangle|$. This shows that $o(a)||G|$. ■

Corollary 8.16 *If G is a finite group and $a \in G$, then $a^{|G|} = e$.*

Proof By Corollary 8.15, we have $o(a)||G|$. Thus, there is a positive integer q such that $|G| = o(a)q$. Consequently, we have

$$a^{|G|} = a^{o(a)q} = (a^{o(a)})^q = e^q = e,$$

as desired. ■

Corollary 8.17 (Euler's Theorem) *If a and n are positive integers such that $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 (\text{mod } n)$.*

Proof Let U_n be the group of units of $\mathbb{Z}_n$ under multiplication modulo n. By Corollary 4.7, we have $|U_n| = \varphi(n)$. So, by Corollary 8.16, we have $\overline{a}^{\varphi(n)} = \overline{1}$, for all $\overline{a} \in U_n$, which in turn translates into $n|a^{\varphi(n)} - 1$, or equivalently $a^{\varphi(n)} \equiv 1 (\text{mod } n)$. ■

Remark 8.18 In Problem 1.74, we realized a proof for Fermat's little theorem. Since $\varphi(p) = p - 1$, for any prime p, we can conclude Fermat's little theorem from Euler's theorem too.

Corollary 8.19 *Every group of prime order is cyclic.*

Proof Assume that G is of prime order p, and let $a \in G$ be an element different from the identity. Then, the cyclic subgroup $\langle a \rangle$ of G generated by a has at least two elements, a and e. But by Lagrange's theorem, the order $m \geq 2$ of $\langle a \rangle$ must divide the prime p. Consequently, we must have $m = p$ and $\langle a \rangle = G$. This shows that G is cyclic. ■

Corollary 8.20 *Let G be a group and p be a prime number. If G has exactly r subgroups of order p, then it has $r(p - 1)$ elements of order p.*

Proof In each subgroup of order p, all non-identity elements have order p. In addition, an element of order p generates a subgroup of order p. By Lagrange's theorem, the intersection of distinct subgroups of order p is trivial subgroup, so their non-identity elements are disjoint from each other. Consequently, each subgroup of order p has its own $p - 1$ elements of order p, not shared by the other subgroups of order p. Therefore, the number of elements of order p is $r(p - 1)$. ■

The following natural question arises: Is the converse of Lagrange's theorem true? That is, if d is a divisor of the order of G, then does G necessarily have a subgroup of order d. The standard example of the alternating group A_4, which has order 12 but has no subgroup of order 6, shows that the converse of Lagrange's theorem is not true.

Theorem 8.21 *The group A_4 of order 12 has no subgroups of order 6.*

Proof To verify this, recall that A_4 has eight elements of order 3 and suppose that H is a subgroup of order 6. Let σ be any element of order 3 in A_4. If σ is not in H, then $A_4 = H \cup \sigma H$. But then $\sigma^2 \in H$ or $\sigma^2 \in \sigma H$. If $\sigma^2 \in H$, then so is $(\sigma^2)^2 = \sigma^4 = \sigma$, so this case is ruled out. If $\sigma^2 \in \sigma H$, then $\sigma^2 = \sigma h$, for some $h \in H$, but this also implies that $\sigma \in H$. This argument shows that any subgroup of A_4 of order 6 must contain all eight elements of A_4 of order 3, which is absurd. ■

Theorem 8.22 *If $n > 4$, then A_n has no subgroup of order $n!/4$.*

Proof If H is a subgroup of order $n!/4$, then H has only two left cosets in A_n. So, if σ is a cycle of length 3 in A_n, then the cosets H, σH, and $\sigma^2 H$ cannot be all distinct. Equality of any two of the above cosets implies either $\sigma \in H$ or $\sigma^2 \in H$. Now, $\sigma^2 \in H$ implies $\sigma = \sigma^4 \in H$. Thus, H contains all cycles of length 3. Now, since A_n is generated by cycles of length 3, it follows that $H = A_n$, a contradiction. ■

Remark 8.23 Theorem 4.31 expresses that the converse of Lagrange's theorem holds for any finite cyclic group.

Theorem 8.24 *Let G be a group of order n. If G has at most one cyclic subgroup of order d where $d|n$, then G is cyclic.*

Proof For each divisor d of n, let $\theta_G(d)$ denote the number of elements of G of order d. For a given positive integer n such that $d|n$, let $\theta_G(d) \neq 0$. Then, there exists $a \in G$ of order d which generates a cyclic group $\langle a \rangle$ of order d of G. We prove that all elements of G of order d belong to $\langle a \rangle$. If $x \in G$ is an element such that $o(x) = d$ and $x \notin \langle a \rangle$, then $\langle x \rangle$ is another subgroup of order d such that $\langle a \rangle \neq \langle x \rangle$. This contradicts the hypothesis. Consequently, if $\theta_G(d) \neq 0$, then $\theta_G(d) = \varphi(d)$, for all positive integer $d|n$. In general, we can write $\theta_G(d) \leq \varphi(d)$, for all positive integer $d|n$. So, we obtain

$$n = \sum_{d|n} \theta_G(d) \leq \sum_{d|n} \varphi(d) = n.$$

This yields that $\theta_G(d) = \varphi(d)$, for all $d|n$. In particular, we have $\theta_G(n) = \varphi(n) \geq 1$. Hence, there exists at least one element of G of order n. This shows that G is cyclic. ■

Exercises

1. Show that a group with at least two elements but with no proper non-trivial subgroups must be finite and of prime order.
2. Suppose that H and K are unequal subgroups of a group G, each of order 16. Prove that $24 \leq |H \cup K| \leq 31$.
3. For a group G and a subgroup H of G, let $Ha_1 \cup Ha_2 \cup \cdots \cup Ha_n$ be a decomposition of G into disjoint right cosets of H in G. Show that $a_1^{-1}H \cup a_2^{-1}H \cup \cdots \cup a_n^{-1}H$ is a decomposition of G into left cosets of H in G.
4. Let G be a finite group and let H and K be subgroups with relatively prime order. Prove that $H \cap K = \{e\}$.
5. Show that if H and K are subgroups of a group G, and have orders 56 and 63, respectively, then the subgroup $H \cap K$ must be cyclic.
6. Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?
7. Use Fermat's little theorem to show that if $p = 4n + 3$ is prime, there is no solution to the equation $x^2 \equiv 1 (\text{mod } p)$.
8. If G is a finite group with fewer than 100 elements and G has subgroups of orders 10 and 25, what is the order of G?
9. Let G be a group and $a, b \in G$. If $a^5 = e$ and $aba^{-1} = b^2$, find $o(b)$ if $b \neq e$.
10. Does A_5 contain a subgroup of order m for each factor m of 60?
11. Let G be an abelian group of order $2n$ with n odd. Prove that G has precisely one element of order 2.
12. Let G be a finite group. Show that the following conditions are equivalent:

    (1) G is cyclic;
    (2) For each positive integer d, the number of $a \in G$ such that $a^d = e$ is less than or equal to d;
    (3) For each positive integer d, G has at most one subgroup of order d;
    (4) For each positive integer d, G has at most $\varphi(d)$ elements of order d.

13. Let G be a finite group and H be a subgroup of G. Let $l(a)$ be the smallest positive integer m such that $a^m \in H$. Prove that $l(a)|o(a)$.
14. Let n be a positive integer and let m be a factor of $2n$. Show that D_n contains a subgroup of order m.
15. Using Lagrange's theorem, show that the binomial coefficient

$$\binom{n}{m} = \frac{n!}{m!(n-m)!},$$

    for every integers m and n with $n \geq 1$ and $0 \leq m \leq n$, is an integer.
    Hint: Consider a subgroup of S_n of order $m!(n-m)!$.

8.4 Index of Subgroups

A special name and notation have been adopted for the number of left (or right) cosets of a subgroup in a group.

Definition 8.25 Let H be a subgroup of a group G. The number of distinct left (or right) cosets of H in G is the *index* of H in G. The index of H in G is denoted by $[G : H]$.

Note that if G is finite, then the index $[G : H]$ divides $|G|$.

Example 8.26 Consider Example 8.3, and let $H = \{id,\ (1\ 3)\}$ be the subgroup of S_3. Then, we observe that $[S_3 : H] = 3$.

Example 8.27 A left coset of $SL_2(\mathbb{F})$ in $GL_2(\mathbb{F})$ has the form $XSL_2(\mathbb{F})=\{XA \mid A \in SL_2(\mathbb{F})\}$, where $X \in GL_2(\mathbb{F})$. If $\det(X) = c$, then $\det(XA) = c$. Therefore, all matrices in $XSL_2(\mathbb{F})$ have the determinant equal to c. Conversely, let $B \in GL_2(\mathbb{F})$ such that $\det(B) = c$. Take $A = X^{-1}B$, then $B = XA$. On the other hand, $\det(A) = \det(X^{-1}B) = \det(X^{-1})\det(B) = c^{-1}c = 1$. This means that $A \in SL_2(\mathbb{F})$. So, we deduce that $B \in XSL_2(\mathbb{F})$. Consequently, we have $XSL_2(\mathbb{F}) = \{A \mid A \in GL_2(\mathbb{F})$ and $\det(A) = c\}$. Hence, each left coset of $SL_2(\mathbb{F})$ in $GL_2(\mathbb{F})$ has the above description, for some non-zero element $c \in \mathbb{F}$. This shows that $[GL_2(\mathbb{F}) : SL_2(\mathbb{F})]$ is infinite.

Theorem 8.28 *If H and K are subgroups of a group G such that $K \leq H$, then $[G : K] = [G : H][H : K]$.*

Proof Suppose that $G = \bigcup_{i \in I} a_i H$, the union of distinct left cosets of H in G, where $|I| = [G : H]$, and let $H = \bigcup_{j \in J} b_j K$, the union of distinct left cosets of K in H, where $|J| = [H : K]$. Then, we can write

$$G = \bigcup_{i \in I} a_i H = \bigcup_{i \in I} a_i \left(\bigcup_{j \in J} b_j K \right) = \bigcup_{(i,j) \in I \times J} a_i b_j K.$$

Now, we claim that $a_i b_j K$'s are distinct. Assume that $a_i b_j K = a_k b_l K$, for some $i, k \in I$ and $j, l \in J$. Since $b_j K \subseteq H$ and $b_l K \subseteq H$, it follows that $a_i H \cap a_k H \neq \emptyset$. This implies that $a_i H = a_k H$, and so $i = k$. Then, we obtain $b_j K = b_l K$, and hence $j = l$. Therefore, we deduce that $a_i b_j K$'s are distinct left cosets of K in G. This yields that $[G : K] = [G : H][H : K]$. ■

Theorem 8.29 (Poincaré Lemma) *If H and K are two subgroups of finite index in a group G such that $[G : H] = m$ and $[G : K] = n$, then $H \cap K$ is also of finite index in G and $[m, n] \leq [G : H \cap K] \leq mn$. In particular, if m and n are relatively prime, then $[G : H \cap K] = mn$. Moreover, if G is finite, then $G = HK$.*

Proof Let $a_1H, a_2H, \ldots, a_mH$ and $b_1K, b_2K, \ldots, b_nK$ be distinct left cosets of H and K in G, respectively. Now, by Theorem 8.7, for every $1 \leq i \leq m$ and $1 \leq j \leq n$ either $a_iH \cap b_jK = \emptyset$ or $a_iH \cap b_jK = c_{ij}(H \cap K)$, for some $c_{ij} \in G$. On the other hand, $x(H \cap K) = xH \cap xK$. Therefore, each left coset of $H \cap K$ is determined by intersection of a left coset of H and a left coset of K in G. Consequently, distinct number of left cosets of $H \cap K$ is at most equal to mn.

Now, by Theorem 8.28, we can write

$$[G : H \cap K] = [G : H][H : H \cap K] = m[H : H \cap K],$$
$$[G : H \cap K] = [G : K][K : H \cap K] = n[K : H \cap K],$$

and hence $m|[G : H \cap K]$ and $n|[G : H \cap K]$. Therefore, we conclude that the least common multiple of m and n divides $[G : H \cap K]$. ■

Corollary 8.30 *In Theorem 8.29, if m and n are relatively prime, then $[G : H \cap K] = mn$.*

Proof It is straightforward. ■

Theorem 8.31 *If H and K are subgroups of a group G, then*

$$[H : H \cap K] \leq [G : K].$$

Proof Suppose that $\mathcal{A}$ is the set of all disjoint left cosets of $H \cap K$ in H and $\mathcal{B}$ is the set of all disjoint left cosets of K in G. We define $f : \mathcal{A} \to \mathcal{B}$ by $f\big(h(H \cap K)\big) = hK$, for all $h \in H$. If $h(H \cap K) = h'(H \cap K)$, for some $h, h' \in H$, then $h^{-1}h' \in H \cap K \subseteq K$. This implies that $hK = h'K$. So, we conclude that f is well defined. Moreover, if $hK = h'K$, for some $h, h' \in H$, then $h^{-1}h' \in K$. Since H is a subgroup and $h, h' \in H$, it follows that $h^{-1}h' \in H$. Hence, we have $h^{-1}h' \in H \cap K$, which implies that $h(H \cap K) = h'(H \cap K)$. Therefore, f is one to one. This yields this $|\mathcal{A}| \leq |\mathcal{B}|$, or equivalently $[H : H \cap K] \leq [G : K]$. ■

Exercises

1. If G is an infinite cyclic group and $\{e\} \neq H \leq G$, prove that $[G : H]$ is finite.
2. Show that the integers have infinite index in the additive group of rational numbers.
3. Suppose that G is a finite group and H, K are subgroups of G such that $K \subset H$ and $[G : K]$ is prime. Prove that $H = G$.
4. Determine the index of the following subgroups in the corresponding groups:
   (a) $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ in $\mathbb{Z}_{12}$;
   (b) $\mathbb{R}$ in $(\mathbb{C}, +)$;
   (c) $3\mathbb{Z}$ in $\mathbb{Z}$.

5. Show that if H is a subgroup of index 2 in a finite group G, then every left coset of H is also a right coset of H.
6. Two subgroups H and K of a group G are said to be *commensurable* if $H \cap K$ is of finite index in both H and K. Show that commensurability is an equivalence relation on the subgroups of G.

8.5 A Counting Principle and Double Cosets

Let A and B be two subsets of a group G. The set $AB = \{ab \mid a \in A,\ b \in B\}$ consisting of the products of elements $a \in A$ and $b \in B$ is said to be the *product* of A and B. The associative law of multiplication gives us $(AB)C = A(BC)$ for any three subsets A, B, and C. The product of two subgroups is not necessarily a subgroup. We have the following theorem.

Theorem 8.32 *Let H and K be two subgroups of a group G. Then, the following two conditions are equivalent:*

(1) The product HK is a subgroup of G;
(2) $HK = KH$.

Proof Suppose that HK is a subgroup of G. Then, for any $h \in H$ and $k \in K$, we have $h^{-1}k^{-1} \in HK$ and so $kh = (h^{-1}k^{-1})^{-1} \in HK$. Thus, $KH \subseteq HK$. Now, if x is any element of HK, then $x^{-1} = hk \in HK$, for some $h \in H$ and $k \in K$. So, we obtain $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$. This means that $HK \subseteq KH$. Thus, we conclude that $HK = KH$.

On the other hand, suppose that $HK = KH$, i.e., if $h \in H$ and $k \in K$, then $hk = k_1h_1$ for some $h_1 \in H$ and $k_1 \in K$. In order to prove that HK is a subgroup of G, we must verify that it is closed and every element in HK has its inverse in HK. Suppose that $x = hk \in HK$ and $y = h'k' \in HK$, where $h, h' \in H$ and $k, k' \in K$. Then, we have $xy = hkh'k'$, but since $kh' \in KH = HK$, it follows that $kh' = h_2k_2$ with $h_2 \in H$ and $k_2 \in K$. Hence, $xy = h(h_2k_2)k' = (hh_2)(k_2k') \in HK$. Clearly, $x^{-1} = k^{-1}h^{-1} \in KH = HK$. Consequently, HK is a subgroup of G. ■

Corollary 8.33 *If H and K are subgroups of the abelian group G, then HK is a subgroup of G.*

Theorem 8.34 *If H and K are finite subgroups of a group G, then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof Suppose that $A = H \cap K$, and let the index of A in H is n. Then, we can write $H = h_1A \cup h_2A \cup \cdots \cup h_nA$, in which $h_iA \cap h_jA = \emptyset$, for any $i \neq j$. On the other hand, we have $HK = h_1AK \cup h_2AK \cup \cdots \cup h_nAK$. Since $AK = K$, it follows that $HK = h_1K \cup h_2K \cup \cdots \cup h_nK$. We claim that $h_iK \cap h_jK = \emptyset$, for

any $i \neq j$. Indeed, if $h_iK = h_jK \neq \emptyset$, for some $i \neq j$, then there exist $k_1, k_2 \in K$ such that $h_ik_1 = h_jk_2$, and then $h_ih_j^{-1} = k_2k_1^{-1} \in A$. This implies that $h_iA = h_jA$, a contradiction. Therefore, we obtain $|HK| = n|K|$. Since $n = |H|/|A|$, it follows that $|HK| = |H||K|/|H \cap K|$. ■

Corollary 8.35 *If H and K are finite subgroups of a group G such that* $\min\{|H|, |K|\} > \sqrt{|G|}$, *then $H \cap K \neq \{e\}$.*

Proof Since $HK \subseteq G$, it follows that $|HK| \leq G$. On the other hand, by Theorem 8.34, we have

$$|G| \geq |HK| = \frac{|H||K|}{|H \cap K|} > \frac{\sqrt{|G|}\sqrt{|G|}}{|H \cap K|} = \frac{|G|}{|H \cap K|}.$$

So, we conclude that $|H \cap K| > 1$. This yields that $H \cap K \neq \{e\}$. ■

Definition 8.36 Let G be a group and H, K be two subgroups of G and let $x \in G$. Then, the set $HxK = \{hxk \mid h \in H \text{ and } k \in K\}$ is called a *double coset* of H and K in G.

Lemma 8.37 *For any $x, y \in G$, two double cosets HxK and HyK are either disjoint or identical.*

Proof Suppose that $a \in HxK \cap HyK$. Then, $a = hxk = h'yk'$, for some $h, h' \in H$ and $k, k' \in K$. This implies that $x = h^{-1}h'yk'k^{-1}$ and $y = h'^{-1}hxkk'^{-1}$. Now, we show that $HxK = HyK$. Let $u \in HxK$ be an arbitrary element. Then, $u = h_1xk_1$, for some $h_1 \in H$ and $k_1 \in K$. Consequently, we obtain $u = h_1h^{-1}h'yk'k^{-1}k_1 \in HyK$. Conversely, if $v \in HyK$ is an arbitrary element, then $v = h_2yk_2$, for some $h_2 \in H$ and $k_2 \in K$. Thus, we have $v = h_2h'^{-1}hxkk'^{-1}k_2 \in HxK$. ■

Let $x, y \in G$ and define $x \sim y$ if and only if $x = hyk$, for some $h \in H$ and $k \in K$. It can be shown easily that $\sim$ is an equivalence relation and the equivalence class of x is HxK.

Lemma 8.38 *If H and K are subgroups of a finite group G and $x \in G$, then*

$$|HxK| = \frac{|H||K|}{|x^{-1}Hx \cap K|}.$$

Proof It is easy to see that the function $f : HxK \to x^{-1}HxK$ defined by $f(hxk) = x^{-1}hxk$, for all $h \in H$ and $k \in K$, is a one to one correspondence. Hence, we deduce that $|HxK| = |x^{-1}HxK| = |x^{-1}Hx||K|/|x^{-1}Hx \cap K|$. Since $|x^{-1}Hx| = |H|$, the result follows. ■

Theorem 8.39 *If H and K are subgroups of a finite group G, then*

$$|G| = \sum \frac{|H||K|}{|x^{-1}Hx \cap K|},$$

where summation on right side is taken over elements x chosen from disjoint double cosets HxK.

Proof For each $x \in G$, we have $x \in HxK$. In view of this, we conclude that $G = \bigcup_{x \in G} HxK$. If we write disjoint union, then we get $|G| = \sum |HxK|$. Hence, by Lemma 8.38, the result follows. ■

Lemma 8.40 *Let H and K be subgroups of a group G and $a \in G$. Then, the double coset HxK is a union of some right cosets of H in G, and also a union of some left cosets of K in G. Moreover, the number of distinct right cosets of H in HxK is $[K : K \cap x^{-1}Hx]$, and the number of distinct left cosets of K in HxK is $[H : H \cap x^{-1}Kx]$.*

Proof Clearly, we have

$$HxK = \bigcup_{k \in K} Hxk \text{ and } HxK = \bigcup_{h \in H} hxK.$$

Now, assume that $k, k' \in K$. Then, we have

$$\begin{aligned} Hxk = Hxk' &\Leftrightarrow (xk)(xk')^{-1} \in H \Leftrightarrow xkk'^{-1}x^{-1} \in H \\ &\Leftrightarrow kk'^{-1} \in x^{-1}Hx \Leftrightarrow kk'^{-1} \in K \cap x^{-1}Hx \text{ (since } k, k' \in K) \\ &\Leftrightarrow k(K \cap x^{-1}Hx) = k'(K \cap x^{-1}Hx). \end{aligned}$$

This shows that the number of distinct right cosets of H in HxK is $[K : K \cap x^{-1}Hx]$. The proof of the last part is similar. ■

Theorem 8.41 *Let H and K be subgroups of a group G. If $[G : H]$ is finite, then*

$$[G : H] = \sum_{x \in X} [K : K \cap x^{-1}Hx],$$

where X is the set of representatives of distinct double cosets. Similarly, if $[G : K]$ is finite, then

$$[G : K] = \sum_{x \in X} [H : H \cap x^{-1}Kx],$$

Proof We know that

$$G = \bigcup_{x \in X} Hxk.$$

By Lemma 8.40, for any $x \in X$, the number of distinct right cosets of H in HxK is $[K : K \cap x^{-1}Hx]$. Hence, the number of total distinct right cosets of H in G is

$$[G : H] = \sum_{x \in X} [K : K \cap x^{-1}Hx].$$

The proof of the second part is similar. ■

Exercises

1. Give an example of a group G and subgroups H and K such that HK is not a subgroup of G.
2. Let H, K, and N be subgroups of a group G such that $H \leq K$, $H \cap N = K \cap N$ and $HN = KN$. Show that $H = K$.
3. If A and B are non-empty finite subsets of a group G, prove that $G = AB$ or $|A| + |B| \leq |G|$.
4. (a) **(Dedekind's Modular Law).** Let H, K, and N be subgroups of a group G and assume that $K \leq N$. Prove that

$$(HK) \cap N = (H \cap N)K.$$

   (b) In particular, if H and K permute, prove that

$$\langle H, K \rangle \cap N = \langle H \cap N, K \rangle.$$

   (c) Can you give an example to show that $(HK) \cap N$ is not equal to $(H \cap N)(K \cap N)$?

- Find the number of left cosets of K which are contained in the double coset HxK.
- Let H, K be two subgroups of G. Prove that every subgroup of G containing both H and K contains the product sets HK and KH.

8.6 Worked-Out Problems

Problem 8.42 Let $G = \langle a \rangle$ be an infinite cyclic group and let $H = \langle a^k \rangle$, where k is a positive integer. Show that

$$H,\ aH,\ a^2H,\ \ldots,\ a^{k-1}H \tag{8.1}$$

is a complete list repetition free of the left (right) cosets of H in G.

Solution The problem is subdivided into proving that

(1) The list (8.1) is complete, i.e., every element of G belongs to one of the left cosets listed;
(2) The list (8.1) is repetition free.

(1) Suppose that x is an arbitrary element of G. Then, there exists positive integer n such that $x = a^n$. Now, by the Division algorithm, we can write $n = qk + r$, for some integers q and r with $0 \leq r < k$. So, we have $x = a^n = a^{qk+r} = a^r(a^k)^q \in a^rH$. Since $1 \leq r \leq k - 1$, it follows that a^rH is one of the left cosets in the list (8.1).

Therefore, every element of G lies in one of the left cosets in the list (8.1).

(2) Suppose (with a view to obtaining a contradiction) that $a^iH = a^jH$ with $0 \leq i < j \leq k-1$. Then, we get $(a^i)^{-1}a^j \in H$, or equivalently $a^{j-i} \in H$. Hence, we conclude that $a^{j-i} = a^{mk}$, for some integer m. Since a has infinite order, it follows that $j - i = mk$. This is a contradiction since $0 < j - i < k$. From this contradiction it follows that the list (8.1) is repetition free. ■

Problem 8.43 Let $d(G)$ be the smallest number of elements necessary to generate a finite group G. Prove that $|G| \geq 2^{d(G)}$. Note that by convention $d(G) = 0$ if $|G| = 1$.

Solution We do the proof by mathematical induction. If $d(G) = 1$, then $|G| > 2$, because each non-identity element has order of at least 2. Suppose that if a group is generated by $n-1$ elements, then its order is at least 2^{n-1}. Now, let $G = \langle a_1, a_2, \ldots, a_n \rangle$, i.e., G is generated by n elements. Then, the subgroup $H = \langle a_1, a_2, \ldots, a_{n-1} \rangle$ is a proper subgroup of G, and hence by assumption we have $|H| \geq 2^{n-1}$. Since $a_n \notin H$, it follows that $a_nH \cap H = \emptyset$. In addition, we have $a_nH \cup H \subseteq G$. Consequently, we obtain

$$|G| \geq |a_nH \cup H| = |a_nH| + |H| \geq 2|H| = 2 \cdot 2^{n-1} = 2^n,$$

and we are done. ■

Problem 8.44 Prove that a group has exactly three subgroups if and only if it is cyclic of order p^2, for some prime p.

Solution Suppose that G is a cyclic group of order p^2. By Theorem 4.31, G has a unique subgroup H of order p. Therefore, the subgroups of G are $\{e\}$, H and G.

Conversely, assume that G is a group which has exactly three subgroups. Then, we conclude that there exists only one non-trivial proper subgroup H of G. Since H has no non-trivial subgroup, it follows that H is a group of order p, for some prime p. Let $H = \langle a \rangle$. Since $G \neq H$, it follows that there exists $b \in G - H$. Now, $\langle b \rangle$ is a subgroup of G different from H. Hence, we conclude that $\langle b \rangle = G$. This means that G is cyclic, and it has a subgroup of order p. Thus, G is finite and the only prime divisor of $|G|$ is p. Consequently, $|G|$ must be p^2, otherwise G has a subgroup from other divisors. ■

Problem 8.45 Let H and K be subgroups of a group G, and suppose that L is a left coset of H in G and R_1, R_2 are two right cosets of K in G. If $L \cap R_1 \neq \emptyset$ and $L \cap R_2 \neq \emptyset$, prove that $|L \cap R_1| = |L \cap R_2|$.

Solution Assume that $a \in L \cap R_1$ and $b \in L \cap R_2$. Then, we have $L = aH = bH$, $R_1 = Ka$ and $R_2 = Kb$. So, we obtain

$$\begin{aligned} L \cap R_1 &= aH \cap Ka = (aHa^{-1} \cap K)a, \\ L \cap R_2 &= bH \cap Kb = (bHb^{-1} \cap K)b. \end{aligned}$$

Since $aH = bH$, it follows that $a^{-1}b \in H$ or $b^{-1}a \in H$. This shows that $Ha^{-1} = Hb^{-1}$. Consequently, we can write $L \cap R_1 = (aHa^{-1} \cap K)a$ and $L \cap R_2 =$

$(aHa^{-1} \cap K)b$. Since $aHa^{-1} \cap K$ is a subgroup of G, it follows that $L \cap R_1$ and $L \cap R_2$ are right cosets of $aHa^{-1} \cap K$ in G. This forces $|L \cap R_1| = |L \cap R_2|$. ■

Problem 8.46 Let G be a group of order 100 that has a subgroup H of order 25. Prove that every element of G of order 5 is in H.

Solution Suppose that a is an element of G of order 5. Then, by Theorem 8.34, we can write

$$|\langle a \rangle H| = \frac{|\langle a \rangle||H|}{|\langle a \rangle \cap H|} = \frac{5 \cdot 25}{|\langle a \rangle \cap H|} = \frac{125}{|\langle a \rangle \cap H|}.$$

Since $\langle a \rangle H \subseteq G$, it follows that $|\langle a \rangle H| \leq 100$. This forces $|\langle a \rangle \cap H| > 1$. Since $|\langle a \rangle| = 5$ and $\langle a \rangle \cap H \subseteq \langle a \rangle$, it follows that $|\langle a \rangle H| = 5$. This yields that $|\langle a \rangle H| = \langle a \rangle$, and hence we conclude that $a \in H$. ■

Problem 8.47 Prove that if G is a finite group, the index of $Z(G)$ in G cannot be prime.

Solution Suppose that $[G : Z(G)] = p$, where p is a prime. Since $p > 1$, it follows that $G \neq Z(G)$, and so there exists $a \in G - Z(G)$. If $C_G(a)$ is the centralizer of a in G, then $Z(G)$ is a subgroup of $C_G(a)$. Since $a \in C_G(a)$ and $a \notin Z(G))$, it follows that $C_G(a) \neq Z(G)$. Hence, we conclude that

$$[C_G(a) : Z(G)] > 1. \tag{8.2}$$

On the other hand, by Theorem 8.29, we have

$$p = [G : Z(G)] = [G : C_G(a)][C_G(a) : Z(G)]. \tag{8.3}$$

Since p is prime, by (8.2) and (8.3), it follows that $[G : C_G(a)] = 1$ and $[C_G(a) : Z(G)] = p$. This shows that $G = C_G(a)$. It means that every element of G commutes with a, and it is a contradiction as $a \notin Z(G)$. Therefore, we conclude that $[G : Z(G)]$ cannot be prime. ■

8.7 Supplementary Exercises

1. 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.
2. Let $n = n_1 + \cdots + n_r$ be a partition of the positive integer n. Use Lagrange's theorem to show that $n!$ is divisible by

$$\prod_{i=1}^{r} n_i!.$$

3. Let G be a finite abelian group and let m be the least common multiple of the orders of its elements. Prove that G contains an element of order m.
4. Let G be a finite group. Prove that the number of elements $x \in G$ such that $x^7 = e$ is odd.
5. If G is a finite group with precisely 2 conjugacy classes, prove $|G| = 2$.
6. If $\sigma \in S_n$ has order p, p is a prime, and $(n, p) = 1$, show that $r\sigma = r$, for some $1 \leq r \leq n$.
7. If in a group G of order n, for each positive integer $m|n$, the equation $x^m = e$ has less than $m + \varphi(m)$ solutions, then show G is cyclic.
8. In a cyclic group of order n, show that for each integer m that divides n there exist $\varphi(m)$ elements of order m.
9. Suppose that G is an abelian group with an odd number of elements. Show that the product of all of the elements of G is the identity.
10. Let G be a group such that $|G| < 200$. Suppose that G has subgroups of order 25 and 35. Find the order of G.
11. Let G be a group of order pqr, where p, q, and r are distinct primes. If H and K are subgroups of G with $|H| = pq$ and $|K| = qr$, prove that $|H \cap K| = q$.
12. Let G be the set of all matrices of the form

$$\begin{bmatrix} 2^k & p(x) \\ 0 & 1 \end{bmatrix},$$

where $k \in \mathbb{Z}$ and $p(x)$ is any polynomial with rational coefficients. Show that

(a) G is a group under matrix multiplication;
(b) There exists a subgroup H of G and an element $u \in G$ such that the left coset uH contains an infinite number of right cosets of H in G;
(c) The chain $H \subset uHu^{-1} \subset u^2Hu^{-2} \subset \cdots$ is an infinite proper ascending chain.

13. 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.
14. In Theorem 8.31, show that equality holds if and only if $G = HK$.
15. Let H be a subgroup of a group G such that $[G : H] = p$, where p is a prime number. If H is a subgroup of $Z(G)$, prove that G is abelian.
16. Let G be an abelian group of order n and $a_1, \ldots, a_n$ be elements of G. Let $x = a_1a_2 \ldots a_n$. Show that

(a) If G has exactly one element of order 2, then $x = b$;
(b) If G has more than one element of order 2, then $x = e$;
(c) If n is odd, then $x = e$.

17. Let H and K be subgroups of a finite group G. Show that

(a) $[H : H \cap K] \leq [H \vee K : K]$, where $H \vee K = \langle H \cup K \rangle$;
(b) If $[G : K] < 2[H : H \cap K]$, then $G = H \vee K$.

18. Let $n > 1$. Show that there exists a proper subgroup H of S_n such that $[S_n : H] \leq n$.
19. Using Lagrange's theorem, for any integers m and n, prove that

$$\frac{(mn)!}{(m!)^n} \text{ and } \frac{(mn)!}{(m!)^n n!}$$

are integers.
Hint: Consider the integers 1 to mn in a family of consecutive integers as follows: $\{1, \ldots, m\}, \{m+1, \ldots, 2m\}, \ldots, \{(n-1)m+1, \ldots, nm\}$. The elements of symmetric group S_{mn} that move each set within itself is a subgroup of S_{mn}.
20. Let G be a group and H be a subgroup of G. Prove that

$$\left| \bigcup_{a \in G} a^{-1} H a \right| \leq 1 + |G| - [G : H].$$

21. Suppose that G has exactly m subgroups of order p, where p is a prime number. Show that the total number of elements of order p in G is $m(p-1)$. Deduce the following results:

(a) A non-cyclic group of order 55 has at least one element of order 5;
(b) A non-cyclic group of order p^2 has altogether $p + 3$ subgroups.