CHAPTER TWO

Subgroups and Cosets

2A

What sorts of questions should we ask about a group G? What can we hope to answer? What do we need to know to claim that we "understand" G? In most cases, it would not be very practical (or interesting) to write down the multiplication table for the group, but we can get considerable insight into the "structure" of G by investigating its subgroups.

(2.1) DEFINITION. Let G be a group. A subset $H \subseteq G$ is a *subgroup* if H is closed under multiplication in G and forms a group with respect to this multiplication.

For instance, the permutation groups $G \subseteq \mathrm{Sym}(X)$ are precisely the subgroups of the full symmetric group $\mathrm{Sym}(X)$. For another example, view the integers $\mathbb{Z}$ as a group with respect to addition. Then, for each $n \in \mathbb{Z}$, the set $n\mathbb{Z}$ of all multiples of n is a subgroup of $\mathbb{Z}$. (In fact, these are all of the subgroups of $\mathbb{Z}$.) Of course, obvious examples of subgroups for any group G are G itself and the singleton subgroup $\{1\}$. We shall (in the hope that this will not cause confusion) write 1 in place of $\{1\}$ to denote this trivial subgroup of any group. Also, if G is a group and we write $H \subseteq G$, we generally intend this to mean that H is a subgroup of G unless we explicitly allow the possibility that H is merely a subset.

If $H \subseteq G$ is a subgroup, then H must contain some element e that acts as an identity element for H. In particular, $ee = e$. Since $e1 = e$ also (where 1 is the identity of G), we conclude that $1 = e$ by Lemma 1.5, and thus $1 \in H$. Now if $h \in H$, then there must exist $h' \in H$ with $hh' = 1$, and it follows that $h' = h^{-1}$ (where h^{-1} is the inverse of h in G). We have now shown that subgroups of a group G are closed under taking inverses (in G) as well as under multiplication.

Conversely, we have the following lemma.

(2.2) LEMMA. *Let G be a group and let $H \subseteq G$ be a nonempty subset. Suppose $xy^{-1} \in H$ for all $x, y \in H$. Then H is a subgroup of G. In particular, any nonempty subset of G closed under multiplication and taking inverses in G is a subgroup.*

Proof. Choose $h \in H$. Then $1 = hh^{-1} \in H$ by hypothesis. For $y \in H$, we have $y^{-1} = 1y^{-1} \in H$, and if also $x \in H$, then $xy = x(y^{-1})^{-1} \in H$. Therefore, the G-multiplication does define an operation on H and the associative property is inherited from G. Since $1 \in H$ and $y^{-1} \in H$ for all $y \in H$, we see that H has an identity and inverses and so is a group. ∎

(2.3) COROLLARY. *Suppose that $\mathcal{H}$ is a collection of subgroups of some group G and let*

$$D = \bigcap_{H \in \mathcal{H}} H .$$

Then D is a subgroup of G.

Proof. Since each $H \in \mathcal{H}$ contains 1, we have $1 \in D$ and, in particular, $D \neq \varnothing$. Now if $x, y \in D$, then $x, y \in H$ for all $H \in \mathcal{H}$ and so $xy^{-1} \in H$ for all such H. Thus, $xy^{-1} \in D$ and D is a subgroup. ∎

As a convenient notational shorthand, we will often write

$$\bigcap \mathcal{H} \quad \text{in place of} \quad \bigcap_{H \in \mathcal{H}} H .$$

How can we construct subgroups for a group? Much of group theory is concerned with variations on this question, but we will discuss a few such constructions now. Given any subset $X \subseteq G$, we can consider the family $\mathcal{H}$ of all subgroups $H \subseteq G$ such that $X \subseteq H$. (Note that $G \in \mathcal{H}$.) The subgroup $\bigcap \mathcal{H}$ is called the subgroup *generated* by X and is denoted $\langle X \rangle$. This subgroup is characterized by two properties:

1. $X \subseteq \langle X \rangle$.
2. If $X \subseteq H$ and H is a subgroup of G, then $\langle X \rangle \subseteq H$.

In other words, the group generated by X is the smallest subgroup of G that contains X (where the word "smallest" should be understood in the sense of containment). Note that if $X \subseteq G$ is itself a subgroup, then $\langle X \rangle = X$.

There is a more explicit (though somewhat less "clean") alternative construction of $\langle X \rangle$.

(2.4) LEMMA. *Let G be a group and suppose that $X \subseteq G$ is an arbitrary subset. Then $\langle X \rangle$ is the set of all finite products*

$$u_1 u_2 u_3 \cdots u_n$$

of elements $u_i \in G$ such that either u_i or $u_i^{-1} \in X$. (The "empty product" with $n = 0$ is understood to equal 1.)

Proof. Let S be the set of all finite products as in the statement of the lemma. Note that $1 \in S$ and so $S \neq \varnothing$ (even if $X = \varnothing$). Now S is clearly closed under multiplication, and since

$$(u_1 u_2 u_3 \cdots u_n)^{-1} = u_n^{-1} u_{n-1}^{-1} \cdots u_1^{-1} \in S,$$

it follows that S is a subgroup.

Since $X \subseteq S$, we have $\langle X \rangle \subseteq S$. On the other hand, since $X \subseteq \langle X \rangle$ and $\langle X \rangle$ is closed under multiplication and inverses, it follows from the definition of S that $S \subseteq \langle X \rangle$. The proof is complete. ■

If X is given as an explicitly listed set, for instance, $X = \{a, b, c\}$, then it is customary to omit the braces and write $\langle a, b, c \rangle$ instead of $\langle \{a, b, c, \} \rangle$. An important case of this is when $|X| = 1$. A group G is said to be *cyclic* if there exists some $g \in G$ with $\langle g \rangle = G$. In general, for any element g of any group, the subgroup $\langle g \rangle$ is cyclic. The following result is immediate from Lemma 2.4. (Note that for negative integers n, the power g^n is defined as $(g^{-1})^{-n}$.)

(2.5) COROLLARY. *Let $g \in G$. Then $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.* ■

Cyclic groups are ubiquitous, since they occur as subgroups in every group. We shall therefore take the time to study them in some detail.

(2.6) LEMMA. *Let $G = \langle g \rangle$, so that G is cyclic. Let $H \subseteq G$ be a subgroup and suppose that $g^n \in H$, where n is the smallest positive integer that makes this true. Then*

a. *for $m \in \mathbb{Z}$, we have $g^m \in H$ iff n divides m and*
b. *$H = \langle g^n \rangle$.*

Note that if g has infinite order and $H = 1$, then there is no positive integer n such that $g^n \in H$. (Recall that $o(g) = \infty$ means that no positive power of g is 1.) In all other cases, if either $H > 1$ or $o(g) < \infty$, then there does exist a positive integer m with $g^m \in H$, and so the integer n of the lemma does exist. To see this, observe that if $o(g) < \infty$, we can take $m = o(g)$, and if $H > 1$, then if $1 \neq h \in H$, it follows that either h or h^{-1} will be of the form g^m for $m > 0$.

Proof of Lemma 2.6. If $n | m$ (n divides m), we write $m = nq$, with $q \in \mathbb{Z}$. Then $g^m = (g^n)^q \in H$. Conversely, suppose $g^m \in H$. Write $m = qn + r$ with $0 \leq r < n$. Then

$$g^r = g^m (g^n)^{-q} \in H,$$

and by the minimality of n, it follows that $r = 0$ and n divides m, as required.

Statement (b) follows, since certainly $\langle g^n \rangle \subseteq H$ and if h is any element of H, then $h = g^m$ for some m, and so by part (a), $m = qn$ and $h = (g^n)^q \in \langle g^n \rangle$. ■

(2.7) COROLLARY. *Every subgroup of a cyclic group is cyclic.* ■

(2.8) LEMMA. *Let $g \in G$ with $o(g) = n < \infty$. Then*

a. $g^m = 1$ *iff* $n | m$,
b. $g^m = g^l$ *iff* $m \equiv l$ *mod* n *and*
c. $|\langle g \rangle| = n$.

Proof. Apply Lemma 2.6(a) to the group $\langle g \rangle$ with $H = 1$. This yields part (a). Part (b) follows from (a) since $g^m = g^l$ iff $g^{m-l} = 1$. Finally, by part (b), the elements of $\langle g \rangle$ are in one-to-one correspondence with the residue classes of integers mod n, and there are exactly n of these. ■

Note that if $g \in G$ and $o(g) = \infty$, then all powers of g are distinct, since if $g^m = g^l$ with $m > l$, then $g^{m-l} = 1$ and g has finite order. We can thus write $|\langle g \rangle| = o(g)$ in all cases.

(2.9) THEOREM. *Let G be a finite cyclic group of order n. Then G has exactly one subgroup of order d for each divisor d of n, and G has no other subgroups.*

Proof. Write $G = \langle g \rangle$ so that $o(g) = n$ by Lemma 2.8(c). For each divisor d of n, we write $e = n/d$ and put $H_d = \langle g^e \rangle$. It is easy to see that $o(g^e) = d$ and thus $|H_d| = d$ by Lemma 2.8(c). What remains is to show that every subgroup $H \subseteq G$ is one of the H_d.

If $H \subseteq G$, then by Lemma 2.6, $H = \langle g^e \rangle$ for some integer e that divides every integer m such that $g^m \in H$. Since $g^n = 1 \in H$, we conclude that e divides n, and thus $H = H_d$, where $d = n/e$. ■

We mention that the additive groups of the integers and of the integers mod n are examples of cyclic groups. In fact, it is easy to prove (and we shall do so later) that every cyclic group is isomorphic to one of these.

To state our final results about cyclic groups in this chapter, we remind the reader that if a and b are integers that are not both zero, then their *greatest common divisor*, denoted $\gcd(a, b)$ is the largest integer that divides both a and b. Also, Euler's totient function $\varphi(n)$ is defined for positive integers n by $\varphi(n) = |U_n|$, where

$$U_n = \{r \in \mathbb{Z} \mid 0 \le r < n \text{ and } \gcd(r, n) = 1\}.$$

(2.10) THEOREM. *Let G be cyclic of finite order n. Then G contains precisely $\varphi(n)$ elements of order n, and these are the elements g^r for $r \in U_n$, where g is any element of order n in G.*

Proof. By Lemma 2.8(c), the elements $x \in G$ of order n are just those elements for which $\langle x \rangle = G$. Let g be any such element, so that the powers g^r for $0 \le r < n$ are the n distinct elements of G. We need to show that $o(g^r) = n$ iff $\gcd(r, n) = 1$.

Suppose first that $\gcd(r, n) > 1$. Then $d = n/\gcd(r, n) < n$ and n divides rd. It follows that $1 = (g^r)^d$ and so $o(g^r) \le d < n$, as required. Now suppose $\gcd(r, n) = 1$ and let e be the least positive integer such that $g^e \in \langle g^r \rangle$. By

Lemma 2.6(a), we see that e divides r and also (since $g^n = 1 \in \langle g^r\rangle$) e divides n. Thus, $e = 1$ and $g \in \langle g^r\rangle$. Therefore, $\langle g^r\rangle = G$ and $o(g^r) = n$. ■

(2.11) THEOREM. *Let B and C be cyclic of order $n < \infty$. Then $B \cong C$ and there are exactly $\varphi(n)$ different isomorphisms that map B to C.*

Proof. Fix $b \in B$ such that $B = \langle b\rangle$. If $\theta : B \to C$ is any isomorphism, write $\theta(b) = c$. Then $\theta(b^m) = c^m$ for all $m \in \mathbb{Z}$, and thus θ is completely determined on all of B once we are given $c = \theta(b)$. Also, since θ is surjective, every element of C must have the form c^m for some $m \in \mathbb{Z}$, and thus c is a generating element of C.

We have now constructed an injective map from the set of all isomorphisms $\theta : B \to C$ into the set of all generating elements c of C; this map carries θ to the generator $c = \theta(b)$ of C. Since the total number of generating elements of C is $\varphi(n)$ by Theorem 2.10, it suffices to show that for every choice of generator c, there exists an isomorphism $\theta : B \to C$ such that $\theta(b) = c$.

The isomorphism we seek will necessarily map b^m to c^m, and so we will define θ by $\theta(b^m) = c^m$ for $m \in \mathbb{Z}$. The problem with this is that the element b^m of B might also be called b^l for some other integer l. We need to show that the value of θ at this element is unambiguously defined. We need, in other words, to show that $c^m = c^l$. Since $o(b) = |B| = n$ by Lemma 2.8(c), the equation $b^m = b^l$ yields that $m \equiv l \pmod n$ by Lemma 2.8(b). Thus, $c^m = c^l$ by Lemma 2.8(b) and (c). We now know that θ is well defined, and what remains is to show that θ is an isomorphism.

Since every element of C has the form $c^m = \theta(b^m)$, we see that θ is surjective. It is thus necessarily injective, since $|B| = |C| < \infty$. Finally,

$$\theta(b^m b^l) = \theta(b^{m+l}) = c^{m+l} = c^m c^l = \theta(b^m)\theta(c^m),$$

and so θ really is an isomorphism. ■

2B

Recall that a group G is abelian if $xy = yx$ for all $x, y \in G$. (Note that cyclic groups are automatically abelian.) If G is nonabelian, we might wish to consider for some $g \in G$, the set

$$\mathbf{C}_G(g) = \{x \in G \mid xg = gx\}$$

of all elements that commute with g. This set is the *centralizer* of g in G, and what makes it especially useful is that it is a subgroup of G.

(2.12) LEMMA. *Let $g \in G$. Then $\mathbf{C}_G(g)$ is a subgroup of G.*

Proof. Since $1 \in \mathbf{C}_G(g)$, the centralizer is nonempty and it is easy to see that it is closed under multiplication. If $x \in \mathbf{C}_G(g)$, then $xg = gx$, and multiplying by x^{-1} from both the left and right yields $x^{-1}(xg)x^{-1} = x^{-1}(gx)x^{-1}$. Thus, $gx^{-1} = x^{-1}g$ and $x^{-1} \in \mathbf{C}_G(g)$, as required. ■

We can define the centralizer of an arbitrary subset $X \subseteq G$ by

$$\mathbf{C}_G(X) = \{y \in G \mid xy = yx \ \text{ for all } \ x \in X\}\,.$$

Thus,

$$\mathbf{C}_G(X) = \bigcap_{x \in X} \mathbf{C}_G(x)\,,$$

and so the centralizer of any subset of a group is a subgroup, by Corollary 2.3. In particular, taking $X = G$, we get the *center* of G, denoted $\mathbf{Z}(G)$. Thus

$$\mathbf{Z}(G) = \mathbf{C}_G(G) = \{y \in G \mid xy = yx \ \text{ for all } \ x \in G\}$$

is a subgroup.

Note that $\mathbf{Z}(G)$ is an abelian group and that G is abelian iff $G = \mathbf{Z}(G)$. Of course, it can happen (and often does) that the center of a group is trivial. For instance, for the dihedral groups,

$$|\mathbf{Z}(D_{2n})| = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 2 & \text{if } n \text{ is even.} \end{cases}$$

The rotation groups of the five regular polyhedra all have trivial centers, but the full groups of symmetries of four of these objects have centers of order 2. (Which one is the exception, and why?)

The following is an example that shows how one can use the fact that centralizers are not merely sets of elements but are subgroups.

(2.13) LEMMA. *Let $X \subseteq G$ be a subset such that $xy = yx$ for all $x, y \in X$. Then $\langle X \rangle$ is abelian.*

Proof. This follows fairly easily from Lemma 2.4, but we prefer this argument. By hypothesis, $X \subseteq \mathbf{C}_G(X)$. Since $\mathbf{C}_G(X)$ is a subgroup, we conclude that $\langle X \rangle \subseteq \mathbf{C}_G(X)$ and so $X \subseteq \mathbf{C}_G(\langle X \rangle)$. As above, this yields $\langle X \rangle \subset \mathbf{C}_G(\langle X \rangle)$ and so $\langle X \rangle$ is abelian. ∎

If $\theta : G_1 \to G_2$ is an isomorphism, it should be clear that $\theta(\mathbf{Z}(G_1)) = \mathbf{Z}(G_2)$. Although this can be proved by a routine computation, we hope the reader will see that this has to be true because the center is a "group theoretic" object, and isomorphisms capture all group theoretic information.

An important special case is where $G_1 = G_2$. An isomorphism from a group G to itself is called an *automorphism* of G. (Note that the identity map on G is an automorphism, but most groups have many other automorphisms, too.) Since isomorphisms carry centers to centers, it follows that every automorphism of G maps $\mathbf{Z}(G)$ to itself. A subgroup $H \subseteq G$ with the property that $\theta(H) = H$ for every automorphism θ of G is said to be *characteristic* in G, and we write H char G.

Not only is the center of a group characteristic, but generally any subgroup uniquely defined by group theoretic properties and not dependent on arbitrary choices or on the names of elements is also characteristic. A good rule of thumb is that any subgroup described by the definite article "the" is characteristic. In Problem 2.7, for example, we shall define the "Frattini subgroup" of a group. Without referring to the definition, the reader should understand that the Frattini subgroup of any group is characteristic.

An important example of an automorphism of G is the *inner automorphism* θ_g induced by an element $g \in G$. This is the map

$$\theta_g(x) = g^{-1}xg.$$

(The reader should check that θ_g is really an automorphism.) A fairly standard notation that we shall adopt is

$$x^g = g^{-1}xg$$

for $x, g \in G$. The element x^g is said to be the *conjugate* of x with respect to g. In this language, the inner automorphism induced by g is the corresponding conjugation map. Observe that if x and g commute, then $x^g = x$, and thus in an abelian group, inner automorphisms are trivial. (As if to compensate for this, another type of automorphism exists only in abelian groups: this is the map $\theta(x) = x^{-1}$ for $x \in G$.)

The set Aut(G) of all automorphisms of G is a subgroup of Sym(G), and the set Inn(G) of inner automorphisms is a subgroup of Aut(G). (The reader should check these assertions.)

Let us go back to the situation of an isomorphism $\theta : G_1 \to G_2$. It should be clear that if $H \subseteq G_1$ is a subgroup, then $\theta(H)$ is a subgroup of G_2. In particular, automorphisms map subgroups to subgroups. The subgroup

$$H^g = \{h^g \mid h \in H\}$$

is a subgroup *conjugate* to H. It is, of course, the image of H under the inner automorphism induced by g.

Since characteristic subgroups are fixed by all automorphisms, they are surely fixed by inner automorphisms, and so if C char G, then $C = C^g$ for all $g \in G$. (Note that this is completely obvious in the case $C = \mathbf{Z}(G)$, since then $x^g = x$ for all $x \in C$. In general, the equation $C^g = C$ does not imply that $x^g = x$ for all $x \in C$.)

This leads us to the definition of what is certainly one of the most important concepts in group theory.

(2.14) DEFINITION. A subgroup $N \subseteq G$ is *normal* if $N^g = N$ for all $g \in G$. We write $N \triangleleft G$ in this situation.

In other words, the normal subgroups of a group are precisely those subgroups fixed by all inner automorphisms. All characteristic subgroups are normal and all subgroups of abelian groups are normal. Of course, the subgroups 1 and G are always normal in any group G.

(2.15) LEMMA. *Let $H \subseteq G$ be a subgroup. Then, $H \triangleleft G$ if $H^g \subseteq H$ for all $g \in G$.*

The reader should be warned that this lemma does not state that $H^g = H$ whenever $H^g \subseteq H$. Since the inner automorphism induced by the element g is a bijection, it is certainly true that $|H^g| = |H|$, and if H is finite, this equality of orders together with the containment $H^g \subseteq H$ certainly does imply that $H^g = H$. For infinite subgroups, however, this does not follow and is not generally true. (An example is given in the problems at the end of this chapter.)

Proof of Lemma 2.15. We must show that $H^g = H$ for all $g \in G$. Since $H^g \subseteq H$ for all elements g, it follows that

$$H = (H^g)^{g^{-1}} \subseteq H^{g^{-1}}$$

for all $g \in G$. Applying this result with the element g^{-1} in place of g, we obtain

$$H \subseteq H^{(g^{-1})^{-1}} = H^g$$

and thus $H = H^g$. ■

For example, consider the case $G = D_{2n}$, the dihedral group, and let H be the set of plane rotations in G. Since H is closed under multiplication, we have $H^g \subseteq H$ if $g \in H$. On the other hand, if $g \notin H$, then g is a "flip" that interchanges the front and back of the n-gon. In this case $g^{-1} = g$, and for $h \in H$ we have $h^g = ghg$, which does not interchange front and back. Thus, $h^g \in H$ for all $h \in H$, and it follows that $H \lhd G$.

Now H is cyclic of order n and it follows that each subgroup C of H is characteristic in H. This is so since if $\theta \in \mathrm{Aut}(H)$, then $\theta(C)$ is a subgroup of H such that $|C| = |\theta(C)|$. It follows by Theorem 2.9 that $C = \theta(C)$, as required. Thus, C char H and $H \lhd G$. The next result shows that $C \lhd G$.

(2.16) LEMMA. *Let $N \lhd G$ and suppose that C char N. Then $C \lhd G$.*

Proof. Let $g \in G$. Since $N \lhd G$, the conjugation map (inner automorphism) induced by g maps N to itself and, in fact, defines an automorphism of N. (Caution: It may not be an inner automorphism of N.) Since C is characteristic in N, this automorphism of N maps C to itself, and so $C^g = C$, as required. ■

In contrast with Lemma 2.16, it does not follow that $C \lhd G$ if all that is known is that $C \lhd N$ and $N \lhd G$ (or even that N char G).

We give one more example of a normal subgroup now.

(2.17) THEOREM. *Let G be any group. Then $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.*

Proof. Let $\theta \in \mathrm{Inn}(G)$ and $\sigma \in \mathrm{Aut}(G)$. By Lemma 2.15, it suffices to show that $\theta^\sigma \in \mathrm{Inn}(G)$ for any choice of θ and σ.

We can write $\theta = \theta_g$ (the conjugation map induced by $g \in G$). To compute θ^σ, we apply it to $x \in G$.

$$(x)\theta^\sigma = (x)\sigma^{-1}\theta_g\sigma = (g^{-1}(x\sigma^{-1})g)\sigma = (g^{-1})\sigma \cdot x \cdot (g)\sigma ,$$

where the last equality follows since σ is an automorphism. We have

$$(x)\theta^{\sigma} = (g\sigma)^{-1} \cdot x \cdot (g\sigma),$$

and so $\theta^{\sigma} = \theta_{(g)\sigma}$, the inner automorphism induced by $(g)\sigma \in G$. ■

2C

Let $X, Y \subseteq G$ be any two subsets. We write

$$XY = \{xy \mid x \in X, y \in Y\}.$$

Even if X and Y are both subgroups, it does not follow that XY is a subgroup.

(2.18) LEMMA. *Let $H, K \subseteq G$ be subgroups. Then HK is a subgroup iff $HK = KH$.*

Proof. Assume that HK is a subgroup. Since $1 \in H$, we have $K \subseteq HK$ and similarly $H \subseteq HK$. It follows that $KH \subseteq HK$ since HK is closed under multiplication. Also, if $x \in HK$, then $x^{-1} \in HK$, and we can write $x^{-1} = hk$ for some $h \in H$ and $k \in K$. It follows that

$$x = (hk)^{-1} = k^{-1}h^{-1} \in KH$$

and thus $HK \subseteq KH$. This proves that $HK = KH$.

Conversely, assume $HK = KH$. To prove that this set is a subgroup, let x and y be any two elements and write

$$x = h_1k_1 \qquad \text{and} \qquad y = k_2h_2$$

for $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$xy^{-1} = h_1k_1h_2^{-1}k_2^{-1}.$$

However, $k_1h_2^{-1} \in KH = HK$, and we can write $k_1h_2^{-1} = h_3k_3$ with $h_3 \in H$ and $k_3 \in K$. We now have

$$xy^{-1} = (h_1h_3)(k_3k_2^{-1}) \in HK$$

and thus HK is a subgroup. ■

In the case where $X = \{x\}$, we write xY or Yx instead of $\{x\}Y$ or $Y\{x\}$.

(2.19) DEFINITION. Let $H \subseteq G$ be a subgroup. If $g \in G$, then the sets

$$Hg = \{hg \mid h \in H\}$$

and

$$gH = \{gh \mid h \in H\}$$

are, respectively, the *right coset* and the *left coset* of H determined by g.

Note that if $g \notin H$, then also $g^{-1} \notin H$, and it follows that $1 \notin Hg$ and $1 \notin gH$. In particular, the cosets Hg and gH are not subgroups in this case. If $g \in H$, on the other hand, then $Hg = H = gH$, and thus the subgroup H is one of its own right cosets and left cosets. Also note that for any element $g \in G$, we have $g \in gH$ and $g \in Hg$. This shows that G is the union of all the right cosets and also of all the left cosets of any subgroup.

(2.20) LEMMA. *Let $H \subseteq G$ be a subgroup.*

a. *If $Hx \cap Hy \neq \varnothing$, then $Hx = Hy$.*
b. *If $xH \cap yH \neq \varnothing$, then $xH = yH$.*

Proof. First note that $Hh = H$ for $h \in H$. (This is really part of Lemma 1.5 applied to H.) Thus

$$H(hx) = (Hh)x = Hx\,,$$

and so if $g \in Hx \cap Hy$, we have

$$Hg = Hx \quad \text{and} \quad Hg = Hy\,,$$

so that $Hx = Hy$, as desired. Part (b) is proved similarly. ■

(2.21) COROLLARY. *Let $H \subseteq G$ be a subgroup. Then G is the disjoint union of the distinct right cosets of H. The analogous result also holds for left cosets.* ■

(2.22) LEMMA. *Let $H \subseteq G$ be a subgroup. For every $g \in G$, we have*

$$|gH| = |H| = |Hg|\,.$$

Proof. The map $\theta\colon H \to Hg$ defined by $(h)\theta = hg$ certainly maps onto Hg and it is injective by Lemma 1.5. It follows that $|H| = |Hg|$, and the other equality is proved similarly. ■

If $H \subseteq G$ is a subgroup, then the *index* of H in G, denoted $|G : H|$, is the number of distinct right cosets of H in G. As we shall see, the cardinality of the set of left cosets of H in G is equal to that of the right cosets, and so the index of a subgroup is, in fact, left-right symmetric.

In Theorem 2.9, we showed that if G is a finite cyclic group and $H \subseteq G$ is a subgroup, then $|H|$ divides $|G|$. We are now ready to prove this much more generally.

(2.23) THEOREM (Lagrange). *Suppose $H \subseteq G$ is a subgroup. Then $|G| = |H||G : H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and $|G|/|H| = |G : H|$.*

Proof. The group G is the disjoint union of $|G : H|$ right cosets, each of cardinality equal to $|H|$. ■

Note that we could as well have worked with left cosets and concluded that if G is finite, then the "left index" equals $|G|/|H|$ and therefore the left and right indices are equal for subgroups of finite groups. The proof of this fact for arbitrary groups is left to the problems at the end of the chapter.

An important consequence of Lagrange's theorem is the following corollary.

(2.24) COROLLARY. *Let G be finite and let $g \in G$. Then $o(g)$ divides $|G|$ and $g^{|G|} = 1$.*

Proof. We have $o(g) = |\langle g\rangle|$ by Lemma 2.8(c), and this divides $|G|$ by Theorem 2.23. The last assertion is immediate from Lemma 2.8(a). ∎

As an application of Corollary 2.24 we mention the number theoretic result of Euler that $a^{\varphi(n)} \equiv 1 \bmod n$ for positive integers a and n such that $\gcd(a, n) = 1$. The trick here is to observe that

$$U_n = \{r \in \mathbb{Z} \mid 0 \leq r < n \text{ and } \gcd(r, n) = 1\}$$

becomes a group under multiplication if we identify each element r with its residue class mod n. (A few things need to be checked, but we will not do so here.)

Observe that Euler's theorem is immediate by applying Corollary 2.24 to the group U_n.

2D

There is an important connection between the normality of a subgroup and the properties of its cosets.

(2.25) THEOREM. *Let $H \subseteq G$ be a subgroup. Then the following are equivalent:*

i. $H \triangleleft G$
ii. *$Hg = gH$ for all $g \in G$.*
iii. *Every left coset of H in G is a right coset.*
iv. *The set of right cosets of H in G is closed under set multiplication.*

Proof. First assume (i). Then $g^{-1}Hg = H$ for all $g \in G$, and multiplication by g on the left yields $Hg = gH$, proving (ii). That (ii) implies (iii) is obvious, so we assume (iii) and prove (iv).

If $x, y \in G$, we must show that $HxHy$ is a right coset. By (iii), however, $xH = Hg$ for some $g \in G$, and we have

$$HxHy = H(Hg)y = Hgy\,,$$

which is a right coset, as required.

Finally, assume (iv). Then $Hg^{-1}Hg$ is a right coset containing $g^{-1}g = 1$. Thus

$$g^{-1}Hg \subseteq Hg^{-1}Hg = H1 = H,$$

and H is normal by Lemma 2.15. ∎

Note that item (ii) of Theorem 2.25 is left-right symmetric. It follows that we can get two additional conditions equivalent to H being normal by exchanging the words "left" and "right" in (iii) and (iv).

(2.26) COROLLARY. *Let $H \subseteq G$ be a subgroup. Then the following are equivalent:*

i. $H \lhd G$.
ii. *Every right coset of H in G is a left coset.*
iii. *The set of left cosets of H in G is closed under set multiplication.* ∎

If $H \lhd G$, we use the notation G/H (read "G mod H") to denote $\{Hg \mid g \in G\}$. By Theorem 2.25, we know that G/H is closed under set multiplication.

(2.27) THEOREM. *If $H \lhd G$, then G/H is a group. The identity element of G/H is the coset H, and the inverse of the coset (Hx) in G/H is Hx^{-1}. Also*

$$(Hx)(Hy) = H(xy)$$

for all $x, y \in G$.

Proof. We have $H(Hx) = Hx$ and $(Hx)H = HxH = HHx = Hx$ since $xH = Hx$. Also, $xy \in (Hx)(Hy)$ and thus $(Hx)(Hy) = H(xy)$ by Lemma 2.20. In particular, $(Hx)(Hx^{-1}) = H = (Hx^{-1})(Hx)$. ∎

The group G/H is called the *quotient group* or *factor group* of G by H. For example, if $G = \mathbb{Z}$ (with respect to addition) and $H = n\mathbb{Z}$ (the multiples of n), then the (additive) coset $H + m$ is the residue class of m mod n and the factor group G/H is the additive group of residues mod n.

Note that if G is finite and $H \lhd G$, then $|G/H| = |G : H| = |G|/|H|$ by Lagrange's theorem.

The following is another consequence of Theorem 2.25.

(2.28) COROLLARY. *Let $N \lhd G$ and let $H \subseteq G$ be any subgroup. Then $HN = NH$ is a subgroup and it is normal if $H \lhd G$.*

Proof. We have

$$HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH$$

by Theorem 2.25. It follows that HN is a subgroup by Lemma 2.18.

If $g \in G$, then since conjugation by g defines an automorphism of G, we have $(HN)^g = H^g N^g = H^g N$. If $H \lhd G$, then $H^g = H$ and the proof is complete. ∎

2E

Even if the subgroup $H \subseteq G$ is not normal, we may still be able to use some of our results about normality. The idea is to find some subgroup $K \subseteq G$ such that $H \lhd K$.

In fact, we shall see that for any subgroup $H \subseteq G$, there is a unique subgroup $K \supseteq H$ maximal with the property that $H \lhd K$.

It is convenient to work more generally and consider subsets that may not be subgroups. If $X \subseteq G$ is any subset, then we define the *normalizer* of X in G to be the set

$$\mathbf{N}_G(X) = \{g \in G \mid X^g = X\}.$$

(2.29) LEMMA. *The normalizer $\mathbf{N}_G(X)$ is a subgroup of G for every subset $X \subseteq G$. If X is a subgroup, then $X \subseteq \mathbf{N}_G(X)$.*

Proof. First, note that $X^1 = X$ and $(X^g)^h = X^{gh}$ for elements $g, h \in G$. It follows that $\mathbf{N}_G(X)$ is nonempty and that it is closed under multiplication. To see that it contains the inverse of each of its elements, suppose that $g \in \mathbf{N}_G(X)$. Then

$$X^{g^{-1}} = (X^g)^{g^{-1}} = X^{gg^{-1}} = X^1 = X$$

and thus $g^{-1} \in \mathbf{N}_G(X)$, as desired.

If X is a subgroup, then conjugation by any element $x \in X$ defines an automorphism of X and, in particular, the conjugation map is surjective. Thus $X^x = X$ for $x \in X$, and it follows that $X \subseteq \mathbf{N}_G(X)$, as required. ∎

(2.30) COROLLARY. *Suppose $H \subseteq G$ is a subgroup and write $N = \mathbf{N}_G(H)$. Then $H \lhd N$, and if $K \subseteq G$ is any subgroup containing H, then $H \lhd K$ iff $K \subseteq N$.* ∎

We saw in Corollary 2.28 that if $N \lhd G$, then $HN = NH$, and so NH is a subgroup of G. This can be generalized as follows.

(2.31) COROLLARY. *Let $H, K \subseteq G$ be subgroups. If $K \subseteq \mathbf{N}_G(H)$, then $HK = KH$ and HK is a subgroup of G.*

Proof. Since $H \lhd \mathbf{N}_G(H)$, we can apply Corollary 2.28 in the group $\mathbf{N}_G(H)$. ∎

The reader should note that although the condition $xH = Hx$ implies that $x \in \mathbf{N}_G(H)$, it does not follow from the equation $HK = KH$ that $K \subseteq \mathbf{N}_G(H)$.

Problems

2.1 Suppose $G = H \cup K$, where H and K are subgroups. Show that either $H = G$ or $K = G$.

2.2 Let G be a group with the property that there do not exist three elements $x, y, z \in G$, no two of which commute. Prove that G is abelian.

2.3 Suppose $\sigma \in \mathrm{Aut}(G)$.

a. If $x^\sigma = x^{-1}$ for all $x \in G$, show that G is abelian.

b. If $\sigma^2 = 1$ and $x^\sigma \neq x$ for $1 \neq x \in G$, show that if G is finite, it must be abelian.

HINT: For part (b), show that the set $\{x^{-1}x^{\sigma} \mid x \in G\}$ is the whole group G. To do this, consider the map $x \mapsto x^{-1}x^{\sigma}$ for $x \in G$.

2.4 Suppose G has precisely two subgroups. Show that G has prime order.

2.5 A proper subgroup $M < G$ is *maximal* if whenever $M \subseteq H \subseteq G$, we have $H = M$ or $H = G$. Suppose that G is finite and has only one maximal subgroup. Show that $|G|$ is a power of a prime.

2.6 Let $H \subseteq G$ with $|G : H| = 2$. Show that $H \lhd G$.

2.7 The *Frattini subgroup* $\Phi(G)$ is the intersection of all maximal subgroups of G. (If there are none, then $\Phi(G) = G$.) We say that an element $g \in G$ is a *nongenerator* if whenever $\langle X \cup \{g\}\rangle = G$, we have $\langle X \rangle = G$ for subsets $X \subseteq G$. If G is finite, show that $\Phi(G)$ is the set of nongenerators of G.

2.8 If $H \subseteq G$, a *right transversal* for H in G is a subset $T \subseteq G$ such that each right coset of H in G contains exactly one element of T. Now let $H, K \subseteq G$ and let S be a right transversal for $H \cap K$ in K.

a. Show that there exists a right transversal T for H in G with $T \supseteq S$.
b. If T is as in part (a), show that $T = S$ iff $HK = G$.
c. If $|G : H| < \infty$, show that $|K : H \cap K| \leq |G : H|$ with equality iff $HK = G$.
d. If $|G| < \infty$ and $HK = G$, show that $|G| = |H||K|/|H \cap K|$.

2.9 (Dedekind's lemma) Let $H \subseteq K \subseteq G$ and $L \subseteq G$. Show that $K \cap HL = H(K \cap L)$.

2.10 Suppose G is finite and $G = H \cup K \cup L$ for proper subgroups H, K and L. Show that $|G : H| = |G : K| = |G : L| = 2$.

HINT: First get (say) $|G : H| = 2$ and then use Problem 2.8 to complete the proof.

2.11 Let G be finite and assume $H, K \subseteq G$ with $\gcd(|G : H|, |G : K|) = 1$. Show that $HK = G$.

HINT: If $U \subseteq V \subseteq G$, then $|G : U| = |G : V| \cdot |V : U|$. Compute $|G : H \cap K|$ and use Problem 2.8.

2.12 If $x, y \in G$, then the *commutator* of x and y, denoted $[x, y]$, is equal to $x^{-1}y^{-1}xy$. If also $z \in G$, then $[x, y, z]$ means $[[x, y], z]$. Note that $[x, y] = 1$ iff x and y commute. Prove the following commutator identities.

a. $[x, y][y, x] = 1$
b. $[xy, g] = [x, g]^y[y, g]$
c. $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$

NOTE: Part (c) was discovered by P. Hall.

2.13 Let $H, K \subseteq G$ be subgroups. Write $[H, K]$ to denote the subgroup of G generated by all commutators $[h, k]$ with $h \in H$ and $k \in K$.

a. Show that $H \subseteq \mathbf{C}_G(K)$ iff $[H, K] = 1$.
b. Show that $H \subseteq \mathbf{N}_G(K)$ iff $[H, K] \subseteq K$.
c. If $H, K \lhd G$ and $H \cap K = 1$, show that $H \subseteq \mathbf{C}_G(K)$.

2.14 Let $H, K \subseteq G$ be subgroups, and let $[H, K]$ be the subgroup defined in Problem 2.13.

a. Show that $[H, K] = [K, H]$.
b. Show that $H \subseteq \mathbf{N}_G([H, K])$.

HINT: For part (b), use Problem 2.12(b).

2.15 Let $H \subseteq G$ be a subgroup. Let $\mathcal{R}$ and $\mathcal{L}$ denote the sets of all right and left cosets of H in G, respectively.

a. Show that there is a bijection $\theta : \mathcal{R} \to \mathcal{L}$ such that $\theta(Hx) = x^{-1}H$ for all $x \in G$.
b. If there exists a bijection $\varphi : \mathcal{R} \to \mathcal{L}$ such that $\varphi(Hx) = xH$ for all $x \in G$, show that $H \lhd G$.

NOTE: Part (a) tells us that the "right index" and the "left index" of a subgroup are always equal.

2.16 Suppose $Z \subseteq \mathbf{Z}(G)$ and G/Z is cyclic. Show that G is abelian.

2.17 Let Q_8 be the group of Problem 1.9. Show that every subgroup of Q_8 is normal.

NOTE: It is a theorem that if $|G|$ is odd and every subgroup is normal, then G is abelian.

2.18 Let π be a set of prime numbers. A finite group is said to be a π-group if every prime that divides its order lies in π. If G is finite, show that G has a unique largest normal π-subgroup (which may be trivial and may be all of G).

NOTE: The largest normal π-subgroup of G is denoted $\mathbf{O}_\pi(G)$.

2.19 Let C be cyclic of order n. Show that Aut(C) is an abelian group of order $\varphi(n)$.

HINT: Take $B = C$ in Theorem 2.11.

NOTE: In fact, Aut(C) $\cong U_n$. If n is an odd prime power this is cyclic but observe that U_8 is not cyclic.

2.20 Given a positive integer n, show that

$$n = \sum_{d \mid n} \varphi(d) .$$

HINT: Let C be cyclic of order n. How many elements of order d are in C?

2.21 Suppose $A \lhd G$ is abelian and $AH = G$ for some subgroup H. Show that $A \cap H \lhd G$.

HINT: Show that $A \subseteq \mathbf{N}_G((A \cap H))$ and $H \subseteq \mathbf{N}_G((A \cap H))$.

NOTE: The computation of the normalizer of a subgroup is often a good way to prove normality.

2.22 Let G be the affine group of the line. (Recall that this is the set of all maps $\mathbb{R} \to \mathbb{R}$ of the form $x \mapsto ax + b$ with $a, b \in \mathbb{R}$ and $a \neq 0$. Show that G has a subgroup H such that H^g is a proper subgroup of H for some element $g \in G$.

HINT: Let H be the set of maps where $a = 1$ and $b \in \mathbb{Z}$.