First let us consider part (a). Since $e \cdot a = a$ for every $a \in G$, then, in particular, $e \cdot f = f$. But, on the other hand, since $b \cdot f = b$ for every $b \in G$, we must have that $e \cdot f = e$. Piecing these two bits of information together we obtain $f = e \cdot f = e$, and so $e = f$.

Rather than proving part (b), we shall prove something stronger which immediately will imply part (b) as a consequence. Suppose that for a in G, $a \cdot x = e$ and $a \cdot y = e$; then, obviously, $a \cdot x = a \cdot y$. Let us make this our starting point, that is, assume that $a \cdot x = a \cdot y$ for a, x, y in G. There is an element $b \in G$ such that $b \cdot a = e$ (as far as we know yet there may be several such b's). Thus $b \cdot (a \cdot x) = b \cdot (a \cdot y)$; using the associative law this leads to

$$x = e \cdot x = (b \cdot a) \cdot x = b \cdot (a \cdot x) = b \cdot (a \cdot y) = (b \cdot a) \cdot y = e \cdot y = y.$$

We have, in fact, proved that $a \cdot x = a \cdot y$ in a group G forces $x = y$. Similarly we can prove that $x \cdot a = y \cdot a$ implies that $x = y$. This says that we can cancel, from the same side, in equations in groups. A note of caution, however, for we cannot conclude that $a \cdot x = y \cdot a$ implies $x = y$ for we have no way of knowing whether $a \cdot x = x \cdot a$. This is illustrated in S_3 with $a = \phi$, $x = \psi$, $y = \psi^{-1}$.

Part (c) follows from this by noting that $a^{-1} \cdot (a^{-1})^{-1} = e = a^{-1} \cdot a$; canceling off the a^{-1} on the left leaves us with $(a^{-1})^{-1} = a$. This is the analog in general groups of the familiar result $-(-5) = 5$, say, in the group of real numbers under addition.

Part (d) is the most trivial of these, for

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot ((b \cdot b^{-1}) \cdot a^{-1}) = a \cdot (e \cdot a^{-1}) = a \cdot a^{-1} = e,$$

and so by the very definition of the inverse, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Certain results obtained in the proof just given are important enough to single out and we do so now in

LEMMA 2.3.2 *Given a, b in the group G, then the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions for x and y in G. In particular, the two cancellation laws,*

$$a \cdot u = a \cdot w \text{ implies } u = w$$

and

$$u \cdot a = w \cdot a \text{ implies } u = w$$

hold in G.

The few details needed for the proof of this lemma are left to the reader.

Problems

1. In the following determine whether the systems described are groups. If they are not, point out which of the group axioms fail to hold.
   (a) G = set of all integers, $a \cdot b \equiv a - b$.
   (b) G = set of all positive integers, $a \cdot b = ab$, the usual product of integers.
   (c) $G = a_0, a_1, \ldots, a_6$ where

$$a_i \cdot a_j = a_{i+j} \quad \text{if} \quad i + j < 7,$$

$$a_i \cdot a_j = a_{i+j-7} \quad \text{if} \quad i + j \geq 7$$

   (for instance, $a_5 \cdot a_4 = a_{5+4-7} = a_2$ since $5 + 4 = 9 > 7$).
   (d) G = set of all rational numbers with odd denominators, $a \cdot b \equiv a + b$, the usual addition of rational numbers.
2. Prove that if G is an abelian group, then for all $a, b \in G$ and all integers n, $(a \cdot b)^n = a^n \cdot b^n$.
3. If G is a group such that $(a \cdot b)^2 = a^2 \cdot b^2$ for all $a, b \in G$, show that G must be abelian.
*4. If G is a group in which $(a \cdot b)^i = a^i \cdot b^i$ for three consecutive integers i for all $a, b \in G$, show that G is abelian.
5. Show that the conclusion of Problem 4 does not follow if we assume the relation $(a \cdot b)^i = a^i \cdot b^i$ for just two consecutive integers.
6. In S_3 give an example of two elements x, y such that $(x \cdot y)^2 \neq x^2 \cdot y^2$.
7. In S_3 show that there are four elements satisfying $x^2 = e$ and three elements satisfying $y^3 = e$.
8. If G is a finite group, show that there exists a positive integer N such that $a^N = e$ for all $a \in G$.
9. (a) If the group G has three elements, show it must be abelian.
   (b) Do part (a) if G has four elements.
   (c) Do part (a) if G has five elements.
10. Show that if every element of the group G is its own inverse, then G is abelian.
11. If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.
12. Let G be a nonempty set closed under an associative product, which in addition satisfies:
   (a) There exists an $e \in G$ such that $a \cdot e = a$ for all $a \in G$.
   (b) Give $a \in G$, there exists an element $y(a) \in G$ such that $a \cdot y(a) = e$.
   Prove that G must be a group under this product.

13. Prove, by an example, that the conclusion of Problem 12 is false if we assume instead:
    (a′) There exists an $e \in G$ such that $a \cdot e = a$ for all $a \in G$.
    (b′) Given $a \in G$, there exists $y(a) \in G$ such that $y(a) \cdot a = e$.
14. Suppose a *finite* set G is closed under an associative product and that both cancellation laws hold in G. Prove that G must be a group.
15. (a) Using the result of Problem 14, prove that the nonzero integers modulo p, p a prime number, form a group under multiplication mod p.
    (b) Do part (a) for the nonzero integers relatively prime to n under multiplication mod n.
16. In Problem 14 show by an example that if one just assumed one of the cancellation laws, then the conclusion need not follow.
17. Prove that in Problem 14 infinite examples exist, satisfying the conditions, which are not groups.
18. For any $n > 2$ construct a non-abelian group of order $2n$. (*Hint:* imitate the relations in S_3.)
19. If S is a set closed under an associative operation, prove that no matter how you bracket $a_1 a_2 \cdots a_n$, retaining the order of the elements, you get the same element in S (e.g., $(a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = a_1 \cdot (a_2 \cdot (a_3 \cdot a_4))$; use induction on n).

#20. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $ad - bc \neq 0$ is a rational number. Prove that G forms a group under matrix multiplication.

#21. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ where $ad \neq 0$. Prove that G forms a group under matrix multiplication. Is G abelian?

#22. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ where $a \neq 0$. Prove that G is an abelian group under matrix multiplication.

#23. Construct in the G of Problem 21 a subgroup of order 4.

#24. Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo 2, such that $ad - bc \neq 0$. Using matrix multiplication as the operation in G, prove that G is a group of order 6.

#25. (a) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $ad - bc \neq 0$ and a, b, c, d are integers modulo 3, relative to matrix multiplication. Show that $o(G) = 48$.

(b) If we modify the example of G in part (a) by insisting that $ad - bc = 1$, then what is $o(G)$?

#*26. (a) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo p, p a prime number, such that $ad - bc \neq 0$. G forms a group relative to matrix multiplication. What is $o(G)$?

(b) Let H be the subgroup of the G of part (a) defined by

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid ad - bc = 1 \right\}.$$

What is $o(H)$?

2.4 Subgroups

Before turning to the study of groups we should like to change our notation slightly. It is cumbersome to keep using the $\cdot$ for the group operation; henceforth we shall drop it and instead of writing $a \cdot b$ for $a, b \in G$ we shall simply denote this product as ab.

In general we shall not be interested in arbitrary subsets of a group G for they do not reflect the fact that G has an algebraic structure imposed on it. Whatever subsets we do consider will be those endowed with algebraic properties derived from those of G. The most natural such subsets are introduced in the

DEFINITION A nonempty subset H of a group G is said to be a *subgroup* of G if, under the product in G, H itself forms a group.

The following remark is clear: if H is a subgroup of G and K is a subgroup of H, then K is a subgroup of G.

It would be useful to have some criterion for deciding whether a given subset of a group is a subgroup. This is the purpose of the next two lemmas.

LEMMA 2.4.1 *A nonempty subset H of the group G is a subgroup of G if and only if*

1. $a, b \in H$ *implies that* $ab \in H$.
2. $a \in H$ *implies that* $a^{-1} \in H$.

Proof. If H is a subgroup of G, then it is obvious that (1) and (2) must hold.

Suppose conversely that H is a subset of G for which (1) and (2) hold. In order to establish that H is a subgroup, all that is needed is to verify that $e \in H$ and that the associative law holds for elements of H. Since the associative law does hold for G, it holds all the more so for H, which is a

subset of G. If $a \in H$, by part 2, $a^{-1} \in H$ and so by part 1, $e = aa^{-1} \in H$. This completes the proof.

In the special case of a finite group the situation becomes even nicer for there we can dispense with part 2.

LEMMA 2.4.2 *If H is a nonempty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.*

Proof. In light of Lemma 2.4.1 we need but show that whenever $a \in H$, then $a^{-1} \in H$. Suppose that $a \in H$; thus $a^2 = aa \in H$, $a^3 = a^2a \in H$, $\ldots$, $a^m \in H, \ldots$ since H is closed. Thus the infinite collection of elements $a, a^2, \ldots, a^m, \ldots$ must all fit into H, which is a finite subset of G. Thus there must be repetitions in this collection of elements; that is, for some integers r, s with $r > s > 0$, $a^r = a^s$. By the cancellation in G, $a^{r-s} = e$ (whence e is in H); since $r - s - 1 \geq 0$, $a^{r-s-1} \in H$ and $a^{-1} = a^{r-s-1}$ since $aa^{r-s-1} = a^{r-s} = e$. Thus $a^{-1} \in H$, completing the proof of the lemma.

The lemma tells us that to check whether a subset of a finite group is a subgroup we just see whether or not it is closed under multiplication.

We should, perhaps, now see some groups and some of their subgroups. G is always a subgroup of itself; likewise the set consisting of e is a subgroup of G. Neither is particularly interesting in the role of a subgroup, so we describe them as trivial subgroups. The subgroups between these two extremes we call nontrivial subgroups and it is in these we shall exhibit the most interest.

Example 2.4.1 Let G be the group of integers under addition, H the subset consisting of all the multiples of 5. The student should check that H is a subgroup.

In this example there is nothing extraordinary about 5; we could similarly define the subgroup H_n as the subset of G consisting of all the multiples of n. H_n is then a subgroup for every n. What can one say about $H_n \cap H_m$? It might be wise to try it for $H_6 \cap H_9$.

Example 2.4.2 Let S be any set, $A(S)$ the set of one-to-one mappings of S onto itself, made into a group under the composition of mappings. If $x_0 \in S$, let $H(x_0) = \{\phi \in A(S) \mid x_0\phi = x_0\}$. $H(x_0)$ is a subgroup of $A(S)$. If for $x_1 \neq x_0 \in S$ we similarly define $H(x_1)$, what is $H(x_0) \cap H(x_1)$?

Example 2.4.3 Let G be any group, $a \in G$. Let $(a) = \{a^i \mid i = 0, \pm 1, \pm 2, \ldots\}$. (a) is a subgroup of G (verify!); it is called the *cyclic subgroup generated by a*. This provides us with a ready means of producing subgroups

of G. If for some choice of a, $G = (a)$, then G is said to be a *cyclic group*. Such groups are very special but they play a very important role in the theory of groups, especially in that part which deals with abelian groups. Of course, cyclic groups are abelian, but the converse is false.

Example 2.4.4 Let G be a group, W a subset of G. Let (W) be the set of all elements of G representable as a product of elements of W raised to positive, zero, or negative integer exponents. (W) is the *subgroup of G generated by W* and is the smallest subgroup of G containing W. In fact, (W) is the intersection of all the subgroups of G which contain W (this intersection is not vacuous since G is a subgroup of G which contains W).

Example 2.4.5 Let G be the group of nonzero real numbers under multiplication, and let H be the subset of positive rational numbers. Then H is a subgroup of G.

Example 2.4.6 Let G be the group of all real numbers under addition, and let H be the set of all integers. Then H is a subgroup of G.

#Example 2.4.7 Let G be the group of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc \neq 0$ under matrix multiplication. Let

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \mid ad \neq 0 \right\}.$$

Then, as is easily verified, H is a subgroup of G.

#Example 2.4.8 Let H be the group of Example 2.4.7, and let $K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}$. Then K is a subgroup of H.

Example 2.4.9 Let G be the group of all nonzero complex numbers $a + bi$ (a, b real, not both 0) under multiplication, and let

$$H = \{a + bi \in G \mid a^2 + b^2 = 1\}.$$

Verify that H is a subgroup of G.

DEFINITION Let G be a group, H a subgroup of G; for $a, b \in G$ we say *a is congruent to b* mod H, written as $a \equiv b \bmod H$ if $ab^{-1} \in H$.

LEMMA 2.4.3 *The relation $a \equiv b \bmod H$ is an equivalence relation.*

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

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

Let's go through each of these in turn.

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

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

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

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

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

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

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

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

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

Suppose, now, that $x \in [a]$. Thus $ax^{-1} \in H$, so $(ax^{-1})^{-1} = xa^{-1}$ is