26. Give a one-sentence synopsis of the proof of the left cancellation law in Theorem 2.16.

27. Give at most a two-sentence synopsis of the proof in Theorem 2.17 that an equation $ax = b$ has a unique solution in a group.

Theory

28. An element $a \neq e$ in a group is said to have order 2 if $a * a = e$. Prove that if G is a group and $a \in G$ has order 2, then for any $b \in G$, $b' * a * b$ also has order 2.

29. Show that if G is a finite group with identity e and with an even number of elements, then there is $a \neq e$ in G such that $a * a = e$.

30. Let $\mathbb{R}^*$ be the set of all real numbers except 0. Define $*$ on $\mathbb{R}^*$ by letting $a * b = |a|b$.

a. Show that $*$ gives an associative binary operation on $\mathbb{R}^*$.

b. Show that there is a left identity for $*$ and a right inverse for each element in $\mathbb{R}^*$.

c. Is $\mathbb{R}^*$ with this binary operation a group?

d. Explain the significance of this exercise.

31. If $*$ is a binary operation on a set S, an element x of S is an **idempotent for** $*$ if $x * x = x$. Prove that a group has exactly one idempotent element. (You may use any theorems proved so far in the text.)

32. Show that every group G with identity e and such that $x * x = e$ for all $x \in G$ is abelian. [*Hint:* Consider $(a * b) * (a * b)$.]

33. Let G be an abelian group and let $c^n = c * c * \cdots * c$ for n factors c, where $c \in G$ and $n \in \mathbb{Z}^+$. Give a mathematical induction proof that $(a * b)^n = (a^n) * (b^n)$ for all $a, b \in G$.

34. Suppose that G is a group and $a, b \in G$ satisfy $a * b = b * a'$ where as usual, a' is the inverse for a. Prove that $b * a = a' * b$.

35. Suppose that G is a group and a and b are elements of G that satisfy $a * b = b * a^3$. Rewrite the element $(a * b)^2$ in the form $b^k a^r$. (See Exercise 33 for power notation.)

36. Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$. See Exercise 33 for the meaning of a^n. [*Hint:* Consider $e, a, a^2, a^3, \ldots, a^m$, where m is the number of elements in G, and use the cancellation laws.]

37. Show that if $(a * b)^2 = a^2 * b^2$ for a and b in a group G, then $a * b = b * a$. See Exercise 33 for the meaning of a^2.

38. Let G be a group and let $a, b \in G$. Show that $(a * b)' = a' * b'$ if and only if $a * b = b * a$.

39. Let G be a group and suppose that $a * b * c = e$ for $a, b, c \in G$. Show that $b * c * a = e$ also.

40. Prove that a set G, together with a binary operation $*$ on G satisfying the left axioms 1, 2, and 3 given after Corollary 2.19, is a group.

41. Prove that a nonempty set G, together with an associative binary operation $*$ on G such that

$$a * x = b \text{ and } y * a = b \text{ have solutions in } G \text{ for all } a, b \in G,$$

is a group. [*Hint:* Use Exercise 40.]

42. Let G be a group. Prove that $(a')' = a$.

43. Let $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ be an isometry of the plane.

a. Prove that ϕ is a one-to-one function.

b. Prove that ϕ maps onto $\mathbb{R}^2$.

44. Prove that if $f : G_1 \to G_2$ is a group isomorphism from the group $\langle G_1, *_1 \rangle$ to the group $\langle G_2, *_2 \rangle$, then $f^{-1} : G_2 \to G_1$ is also a group isomorphism.

45. Suppose that G is a group with n elements and $A \subseteq G$ has more than $\frac{n}{2}$ elements. Prove that for every $g \in G$, there exists $a, b \in A$ such that $a * b = g$. (This was Problem B-2 on the 1968 Putnam exam.)

SECTION 3 Abelian Examples

In this section we introduce two families of abelian groups and one special abelian group. These groups will be very useful in our study of groups in that they provide examples we can use to help understand concepts and test conjectures. Furthermore, we will see that some of them arise frequently in the study of groups.

We start by defining the set $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$, the first $n-1$ positive integers together with 0, which makes a total of n elements. To define an operation $+_n$ on $\mathbb{Z}_n$, we let $a, b \in \mathbb{Z}_n$. Then

$$a +_n b = \begin{cases} a+b & \text{if } a+b < n \\ a+b-n & \text{if } a+b \geq n \end{cases}.$$

Note that for any $a, b \in \mathbb{Z}_n$, $0 \leq a+b \leq 2n-2$, so $0 \leq a +_n b \leq n-1$ is an operation which we call **addition modulo *n***. Addition modulo n is clearly commutative: $a +_n b = b +_n a$ for any $a, b \in \mathbb{Z}_n$. The number 0 is an identity, the inverse of $a \in \mathbb{Z}_n$ is $n-a$ for $a \neq 0$, and the inverse of 0 is 0. To show that $\langle \mathbb{Z}_n, +_n \rangle$ is an abelian group, it only remains to show that $+_n$ is associative. Although it is not difficult to show directly that $+_n$ is associative, it is a little tedious, so we defer the proof until we develop the circle group and then use properties of that group to conclude that $\langle \mathbb{Z}_n, +_n \rangle$ is an abelian group.

3.1 Example For $n = 1$, $\mathbb{Z}_1 = \{0\}$, which is the trivial group with just one element. For $n = 2$, $\mathbb{Z}_2 = \{0, 1\}$, which as we saw in Section 2 is isomorphic with $\{1, -1\}$ under multiplication. It is important to note that completely different operations on sets can still define isomorphic groups. We also saw in Section 2 that any group with exactly three elements is isomorphic with any other group with exactly three elements. Therefore $\mathbb{Z}_3$ under addition modulo 3 is isomorphic with the group consisting of the three matrices

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \right\}$$

under matrix multiplication. Again we see that two groups can be isomorphic, but have completely different sets and operations. ▲

3.2 Example

Let us look more closely at the group table for $\mathbb{Z}_4$, Table 3.3. We see that the inverse for 0 is 0, the inverse for 1 is $4-1=3$, and the inverse for 2 is $4-2=2$. In Exercise 20 in Section 2, you were asked to show that there are two groups with exactly four elements. The other group is the **Klein 4-group** denoted V, which stands for Vier, German for "four." The group table for V is displayed as Table 3.4. How can we tell that the two groups $\mathbb{Z}_4$ and V are not isomorphic? We could try all possible one-to-one functions from $\mathbb{Z}_4$ onto K_4 to see if any of them make the table for $\mathbb{Z}_4$ look like the table for K_4. This is tedious, so instead we look for a sneaky method. Notice that the diagonal entries of the table for K_4 are all the identity. No matter how we relabel

3.3 Table

$\mathbb{Z}_4$:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

3.4 Table

V:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

the entries in the table for $\mathbb{Z}_4$, only two entries along the diagonal will be the same. Therefore $\mathbb{Z}_4$ and K_4 are not isomorphic. ▲

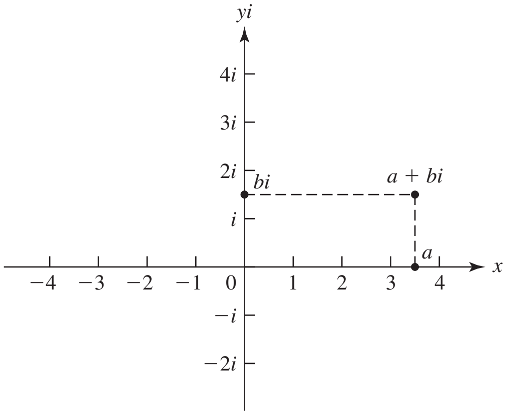
Looking back at the definition of $+_n$ there is no reason we had to restrict our set to integers a with $0 \le a < n$. In fact, the same formula defines an operation on all real numbers a with $0 \le a < n$. In general, let c be any positive real number and $a, b \in [0, c)$. We define $+_c$ by

$$a +_c b = \begin{cases} a + b & \text{if } a + b < c \\ a + b - c & \text{if } a + b \ge c \end{cases}.$$

This operation is called **addition modulo** c. It is easy to see that addition modulo c is an operation on $[0, c)$, it is commutative, 0 is an identity, the inverse of 0 is 0, and the inverse of any $a \in (0, c)$ is $c - a$. Instead of writing $[0, c)$ we will denote this set as $\mathbb{R}_c$. In order to show that $\langle \mathbb{R}_c, +_c \rangle$ is an abelian group, it remains to show that $+_c$ is associative. Again, we defer the proof until after we develop the circle group.

3.5 Example Let $c = 2\pi$. Then $\frac{2}{5}\pi +_{2\pi} \frac{6}{5}\pi = \frac{8}{5}\pi$ and $\frac{7}{5}\pi +_{2\pi} \frac{6}{5}\pi = \frac{3}{5}\pi$. The inverse of $\frac{\pi}{2}$ is $2\pi - \frac{\pi}{2} = \frac{3}{2}\pi$. ▲

In the group $\langle \mathbb{R}_{2\pi}, +_{2\pi} \rangle$, we are essentially equating 0 with 2π in the sense that if a and b add to give 2π, we know that $a +_{2\pi} b = 0$. Intuitively, we can think of this geometrically as taking a string of length 2π and attaching the ends together to form a circle of radius 1. Our next goal is to make this idea more precise by defining a group on the unit circle in the plane and showing that this group is isomorphic with $\mathbb{R}_{2\pi}$. To do this, we first review some facts about complex numbers.



3.6 Figure

Complex Numbers

A real number can be visualized geometrically as a point on a line that we often regard as an x-axis. A complex number can be regarded as a point in the Euclidean plane, as shown in Fig. 3.6. Note that we label the vertical axis as the yi-axis rather than just the y-axis, and label the point one unit above the origin with i rather than 1. The point with Cartesian coordinates (a, b) is labeled $a + bi$ in Fig. 3.6. The set $\mathbb{C}$ of **complex numbers** is defined by

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

We consider $\mathbb{R}$ to be a subset of the complex numbers by identifying a real number r with the complex number $r + 0i$. For example, we write $3 + 0i$ as 3 and $-\pi + 0i$ as $-\pi$ and $0 + 0i$ as 0. Similarly, we write $0 + 1i$ as i and $0 + si$ as si.